NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.010.04.2018
P/18/006

01464818

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	Adrian Gosk – specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/77/2018 z 5 czerwca 2018 r. (dowód: akta kontroli str. 1)
Jednostka kontrolowana	Urząd Gminy w Nowych Piekutach, ul. Główna 8, 18-212 Nowe Piekuty (dalej: „Urząd")
Kierownik jednostki kontrolowanej	Marek Kaczyński – Wójt Gminy, od 4 lipca 1994 r. (dowód: akta kontroli str. 2)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, przyjęte oraz wdrożone rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji.

Uzasadnienie oceny ogólnej

W Urzędzie właściwie zorganizowano proces zabezpieczenia danych, w tym: opracowano i na bieżąco aktualizowano dokumentację bezpieczeństwa, do realizacji kluczowych zadań przydzielono właściwie przygotowany i wykwalifikowany personel, a pracownicy uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych zadań. Zadbano również o właściwe zabezpieczenia techniczne, w tym o pomieszczenia serwerowni. Poziom bezpieczeństwa podnosiły również systematyczne testy, analizy i wewnętrzne przeglądy. Prawidłowo zareagowano również w przypadku dwóch incydentów w zakresie bezpieczeństwa informacji.

Stwierdzone nieprawidłowości polegały na:

- nieopracowaniu rozwiązań technicznych i organizacyjnych uwzględniających ochronę danych w fazie projektowania oraz domyślną ochronę danych – wymaganych art. 25 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[3],
- nieopracowaniu planu przeglądów Systemu Zarządzania Bezpieczeństwem Informacji, wymaganego regulacjami wewnętrznymi Urzędu,
- nieposiadaniu pełnych i aktualnych danych dotyczących użytkowanego sprzętu i oprogramowania, co naruszało przepisy § 20 ust. 2 pkt 2 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[4],
- odebraniu z ponad miesięcznym opóźnieniem byłemu pracownikowi upoważnienia do przetwarzania danych, wbrew § 20 ust. 2 pkt 4 i 5 rozporządzenia w sprawie KRI,
- nieujęciu w umowie na świadczenie usług poczty elektronicznej zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym, mimo wymogu wynikającego z przepisu § 20 ust. 1 i ust. 2 pkt 7 i 10 rozporządzenia w sprawie KRI.

---

[1] Kontrolą objęto okres od 1 czerwca 2017 r. do 30 czerwca 2018 r.

[2] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

[3] Dz. Urz. UE L z 2016.119.1. Rozporządzenie zwane dalej: „RODO".

[4] Dz. U. 2017 r. poz.2247. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie KRI".

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Urzędzie opracowano i wdrożono System Zarzadzania Bezpieczeństwem Informacji („SZBI"), o którym mowa w § 20 ust. 1 rozporządzenia w sprawie KRI. Wójt Gminy wprowadził SZBI zarządzeniami z 26 lutego 2016 r.[5] oraz 25 maja 2018 r.[6], który obejmował: Politykę Bezpieczeństwa Danych Osobowych („PBDO"), Politykę Bezpieczeństwa Informacji („PBI"), Instrukcję Zarządzania Systemami Informatycznymi („IZSI") oraz Instrukcję postępowania w sytuacji naruszenia SZBI. Dokumenty te określały zasady i procedury bezpieczeństwa, a szczegółowe rozwiązania organizacyjno-techniczne zamieszczono w załącznikach do poszczególnych dokumentów. Wszyscy pracownicy Urzędu zostali przeszkoleni z zakresu bezpieczeństwa informacji i zapoznani z SZBI, co szerzej omówiono w pkt 3 niniejszego wystąpienia.

PBI (stanowiąca element SZBI) określała odpowiedzialność osób zaangażowanych w proces zabezpieczenia informacji w Urzędzie, w tym Administratora Bezpieczeństwa Informacji („ABI"), jako osobę odpowiedzialną za tworzenie, wdrażanie i nadzorowanie standardów bezpieczeństwa. Zadania ABI od 26 lutego 2016 r. do 24 maja 2018 r. sprawował pracownik podmiotu zewnętrznego. Ta sama osoba od 25 maja 2018 r. przejęła funkcję Inspektora Ochrony Danych („IOD"), a do jej zadań należał m.in. nadzór nad opracowaniem i aktualizacją dokumentacji bezpieczeństwa informacji.

Poza SZBI w Urzędzie przyjęto inne dokumenty podwyższające poziom bezpieczeństwa informacji (zasobów), tj.: Plan ciągłości działania systemu informatycznego[7], Instrukcję w sprawie określenia procedury postępowania z kluczami[8] oraz Procedurę dokonywania przelewów[9]. Jak wyjaśnił IOD, pracownicy zapoznawani byli z tymi procedurami / instrukcjami „bez formalnego udokumentowania tego faktu".

(dowód: akta kontroli str. 3-229, 292-309, 363-365)

1.2. Zaktualizowany (w związku z wejściem w życie RODO) w dniu 25 maja 2018 r. SZBI obejmował m.in. procesy: ograniczenia przetwarzania (art. 18 RODO), powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO), rejestrowania czynności przetwarzania (art. 30 RODO), bezpieczeństwa przetwarzania (art. 32 RODO), zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO) oraz ocenę skutków dla ochrony danych osobowych (art. 35 RODO). Dokumentacja bezpieczeństwa Urzędu nie uwzględniała natomiast problematyki określonej w art. 25 RODO, tj. ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony danych, co opisano szerzej w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 85-217, 363-365)

1.3. W związku z obowiązkiem przewidzianym w § 20 ust. 2 pkt 1 rozporządzenia w sprawie KRI, w Urzędzie kolejno we wrześniu, listopadzie i grudniu 2017 roku przeprowadzono przeglądy aktualności SZBI. W wyniku przeglądu nie wystąpiła potrzeba aktualizacji SZBI. Plan sprawdzeń na 2018 rok zakładał, że kolejny przegląd nastąpi w III–IV kwartale 2018 roku. W związku z wejściem w życie RODO w dniu 25 maja 2018 r. dokonano kompleksowej aktualizacji dokumentacji SZBI. Zmianie uległy następujące dokumenty: PBDO, PBI, IZSI oraz Instrukcja postępowania w sytuacji naruszenia SZBI.

(dowód: akta kontroli str. 85, 244-262)

1.4. W okresie objętym kontrolą zadania związane z opieką informatyczną oraz zapewnieniem bezpieczeństwa informacji w Urzędzie realizował podmiot zewnętrzny, którego pracownicy pełnili funkcje: ABI, zastępcy ABI oraz administratora systemu

---

5 Zarządzenie Nr 41/2016 Wójta Gminy Nowe Piekuty z dnia 26 lutego 2016 r. w sprawie wprowadzenia dokumentacji w zakresie ochrony danych osobowych i bezpieczeństwa informacji.

6 Zarządzenie Nr 6/2018 Wójta Gminy Nowe Piekuty z dnia 25 maja 2018 r. w sprawie wprowadzenia dokumentacji w zakresie ochrony danych osobowych i bezpieczeństwa informacji.

7 Plan ciągłości działania systemu informatycznego w Urzędzie Gminy Nowe Piekuty, zatwierdzony przez Wójta Gminy 2 czerwca 2017 r.

8 Instrukcja w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń Urzędu Gminy Nowe Piekuty, zatwierdzona przez Wójta Gminy 1 czerwca 2017 r.

9 Procedura dokonywania przelewów w Urzędzie Gminy Nowe Piekuty, zatwierdzona przez Wójta Gminy 2 czerwca 2017 r.

informatycznego („ASI")[10]. Od 25 maja 2018 r. ten sam podmiot wykonywał obowiązki IOD, co szerzej omówiono w pkt 1.5. niniejszego wystąpienia, a Wójt Gminy w tym samym dniu wyznaczył jednego z pracowników do pełnienia funkcji pełnomocnika SZBI (osoba ta odpowiedzialna była m.in. za: komunikację w zakresie bezpieczeństwa informacji, zapewnienie wstępnego przeszkolenia nowych pracowników i zapoznanie ich z SZBI, a także zgłaszanie podejrzeń wystąpienia incydentów i aktywny udział w reagowaniu na incydenty). (dowód: akta kontroli str. 92-93, 276-319)

1.5. Wójt Gminy 25 maja 2018 r. zawarł z podmiotem zewnętrznym umowę w sprawie powierzenia funkcji IOD. Podpisano ją na czas określony, do 31 grudnia 2018 r. Zgodnie z umową zleceniobiorca zobowiązał się do opracowania i wdrożenia aktualizacji SZBI oraz pełnienia funkcji IOD, wymaganej art. 37 ust. 1 RODO. W umowie wskazano zadania IOD, określone w art. 39 ust. 1 RODO, w szczególności: informowane administratora i pracowników Urzędu o obowiązkach spoczywających na RODO, monitorowanie przestrzegania przepisów w tym zakresie, udzielanie zaleceń do oceny skutków dla ochrony danych, współpraca z organem nadzorczym, a także pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych. Osoba wyznaczona do pełnienia funkcji IOD posiadała kwalifikacje do pełnienia tej funkcji, wskazane w art. 37 ust. 5 RODO. (dowód: akta kontroli str. 279-309)

1.6. Warunki współpracy określone w umowie „outsourcingu IOD", zawartej z podmiotem zewnętrznym, gwarantowały wykonywanie funkcji IOD w sposób niezależny, stosownie do wymogów art. 38 ust. 3 RODO. (dowód: akta kontroli str. 301-309, 364)

1.7. W Urzędzie sporządzono większość dokumentów wykonawczych wymaganych przez PBI, w tym: deklarację Polityki SZBI, Plan postępowania z ryzykiem, protokoły z audytu i przeglądów zarządzania. Do końca I połowy 2018 roku nie opracowano natomiast planu przeglądów SZBI, wymaganego pkt 4 z rozdziału siódmego PBI z 25 maja 2018 r., co opisano szerzej w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 141-145, 245-274, 320-337, 364)

1.8. Szczegółową dokumentację bezpieczeństwa (przede wszystkim listę zastosowanych zabezpieczeń) ujęto w załącznikach do SZBI i według IOD nie udostępniono jej wszystkim pracownikom. (dowód: akta kontroli str. 85-217, 363-365, 402-410)

1.9. W Urzędzie zidentyfikowano 46 zbiorów danych podlegających zabezpieczeniu, które ujęto w wykazie zbiorów danych osobowych. Do 24 maja 2018 r. ABI prowadził także rejestr zbiorów danych osobowych, wymagany art. 36a ust. 2 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[11].
(dowód: akta kontroli str. 320-337, 345-359, 363-365)

1.10. Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI, zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu służącego do przetwarzania informacji, a zgodnie z normą PN-ISO/IEC 27002:2014-12, pkt 8.1.1, wszystkie aktywa powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany spis wszystkich aktywów informatycznych. Aktualna inwentaryzacja sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, co umożliwia odtworzenie zasobów informatycznych po zdarzeniu losowym.

W Urzędzie prowadzono inwentaryzację sprzętu w formie elektronicznej[12]. W trakcie oględzin 15 urządzeń (10 komputerów stacjonarnych, dwóch laptopów, jednego serwera, routera oraz drukarki) konfrontowano dane uzyskane z poszczególnych jednostek sprzętu informatycznego takie, jak: [1] nazwę jednostki oraz jej typ i model, [2] system operacyjny, [3] zainstalowane oprogramowanie, [4] rodzaj procesora, [5] klucz instalacyjny, [6] aktualny użytkownik oraz [7] lokalizacja urządzenia w Urzędzie. W wyniku oględzin stwierdzono, że dla trzynastu jednostek sprzętu komputerowego (dziewięciu komputerów stacjonarnych, dwóch laptopów, serwera oraz rutera) dysponowano wszystkimi informacjami, o których mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI. Dla jednego komputera stacjonarnego oraz

[10] Urząd na podstawie umowy zawartej 2 stycznia 2017 r. współpracował także z innym podmiotem zewnętrznym zajmującym się obsługą serwisową jednego z systemów dziedzinowych.
[11] Dz.U. 2016 poz. 922, ze zm. Ustawa uchylona z dniem 25 maja 2018 r.
[12] Inwentaryzację sprzętu i oprogramowania prowadzono z wykorzystaniem programu MS Access.

drukarki nie dysponowano kompletem danych dotyczących konfiguracji i oprogramowania, co opisano szerzej poniżej, w sekcji „Ustalone nieprawidłowości".

Objęte oględzinami urządzenia informatyczne przydzielono pod opiekę (przypisano) poszczególnym pracownikom. (dowód: akta kontroli str. 366-378)

Ustalone nieprawidłowości

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

1. W przyjętym 25 maja 2018 r. SZBI nie uwzględniono problematyki ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony danych przewidzianej w art. 25 RODO. Jak wyjaśnił IOD, nie wprowadzano nowych rozwiązań technicznych (systemów informatycznych) oraz zmian do funkcjonującego oprogramowania bądź sieci informatycznej, a w momencie tworzenia SZBI nie było jasnych wskazówek w jaki sposób można spełnić powyższe wymogi (na przykład wprowadzić zatwierdzony mechanizm certyfikacji, przewidziany w art. 42 w związku z art. 25 RODO), stąd uznano, że w dokumentacji bezpieczeństwa nie należy ujmować rozwiązań, które nie posiadają rekomendacji właściwych w tym zakresie instytucji.
(dowód: akta kontroli str. 85-217, 363-365)

2. Do końca I połowy 2018 roku w Urzędzie nie przyjęto planu przeglądów SZBI, zawierającego m.in.: przedmiot, zakres oraz termin poszczególnych przeglądów, wymaganego pkt 4 rozdziału siódmego PBI z 25 maja 2018 r. IOD wyjaśnił, że powodem tego była nieodległa data wejścia w życie znowelizowanego SZBI (zadeklarował jego opracowanie w III kwartale 2018 roku). (dowód: akta kontroli str. 141-142, 364)

3. W Urzędzie, wbrew wymogom wynikającym z § 20 ust. 2 pkt 2 rozporządzenia KRI, nie utrzymywano aktualności inwentaryzacji sprzętu i oprogramowania, obejmującej ich rodzaj i konfigurację. W prowadzonej w Urzędzie ewidencji sprzętu informatycznego nie ujęto żadnej posiadanej drukarki oraz systemu informatycznego zainstalowanego lokalnie na jednym z komputerów stacjonarnych (spośród 10 analizowanych). ASI wyjaśnił, że w ewidencji IT zapisano wszystkie komputery i inne istotne urządzenia z punktu widzenia sieci lokalnej (serwery, routery itp.), a Urząd nie posiadał do tej pory dużych drukarek sieciowych z pamięcią wymagających przypisania użytkowników oraz ich skonfigurowania, a jedynie „proste urządzenia drukujące przypisane dla pojedynczych użytkowników". Z kolei systemu informatycznego nie odnotowano w ewidencji IT, ponieważ nie był on użytkowany do bieżącej pracy i stanowi jedynie bazę danych archiwalnych. (dowód: akta kontroli str. 366-378)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości organizację systemu bezpieczeństwa informacji w Urzędzie. 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. Urząd zabezpieczył się przed możliwością zainstalowania nieautoryzowanego oprogramowania, ograniczając uprawnienia poszczególnych użytkowników do instalacji dowolnego oprogramowania. Potwierdziły to oględziny dziesięciu wykorzystywanych w Urzędzie komputerów (sześciu stacjonarnych i czterech przenośnych). Było to zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, w myśl którego 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.
(dowód: akta kontroli str. 366-377)

2.2. Wszyscy pracownicy Urzędu (18 osób) posiadali uprawnienia do systemów informatycznych i zbiorów danych zgodne z ich zakresami obowiązków, czym wypełniono obowiązek wskazany w § 20 ust. 2 pkt 4 rozporządzenia KRI.
(dowód: akta kontroli str. 3-217, 366-377)

2.3. W okresie objętym kontrolą zatrudnienie w Urzędzie zakończyło czterech pracowników. W trzech przypadkach upoważnienia do przetwarzania danych osobowych i uprawnienia w systemach informatycznych odebrane zostały niezwłocznie (dostęp do systemów zablokowano w dniu zakończenia pracy), a dla jednej osoby wnioski o odebranie upoważnienia oraz uprawnienia – wbrew § 20 ust. 2 pkt 4–5 rozporządzenia w sprawie KRI – złożone zostały do ABI i ASI po ponad miesiącu od dnia odejścia z pracy, co opisano szerzej w dalszej części wystąpienia, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 360-380)

2.4. Stosownie do wymogów § 20 ust. 2 pkt 7 lit. c rozporządzenia w sprawie KRI, na wykorzystywanych stacjach roboczych i w poszczególnych systemach informatycznych[13] stosowano zabezpieczenia wymagane przez SZBI, m.in. mechanizm centralnego zarządzania uprawnieniami oraz hasła dostępu o odpowiedniej złożoności.

(dowód: akta kontroli str. 366-371)

2.5. Oględziny wszystkich (18) stanowisk pracy w Urzędzie wykazały, że monitory usytuowano w sposób uniemożliwiający bezpośredni wgląd do danych przez osoby nieuprawnione. Było to zgodne z wymogami § 20 ust. 2 pkt 7 rozporządzenia w sprawie KRI. (dowód: akta kontroli str. 366-371)

2.6. W Urzędzie ustanowiono zasady gwarantujące bezpieczną pracę przy mobilnym przetwarzaniu danych (poza siedzibą Urzędu), stosownie do wymogu § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI. SZBI przewidywał m.in., że wymiana informacji odbywa się w postaci zaszyfrowanej z wykorzystaniem mechanizmów kryptograficznych, a każdy zdalny dostęp użytkownika do zasobów informacyjnych jest automatycznie rejestrowany. W okresie objętym kontrolą zgodę na mobilne przetwarzanie danych (łączenie się z zasobami Urzędu) posiadał jeden pracownik Urzędu. Procedury nie wymagały obowiązku okresowego podłączania użytkowanego przez tą osobę komputera przenośnego do lokalnej sieci informatycznej. (dowód: akta kontroli str. 179-181, 190, 230, 378-380)

2.7. Do rozpoczęcia niniejszej kontroli, w Urzędzie nie stosowano rozwiązań polegających na szyfrowaniu danych zgromadzonych na dyskach twardych komputerów przenośnych, co opisano szerzej w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". (dowód: akta kontroli str. 230, 378-380)

2.8. Realizując wymóg § 20 ust. 2 pkt 9 rozporządzenia w sprawie KRI, pomieszczenie serwerowni Urzędu zostało właściwie zlokalizowane, zabezpieczone i wyposażone, a dostęp do niego został ograniczony i na bieżąco ewidencjonowany. Klimatyzowana serwerownia znajdowała się w nieoznakowanym pomieszczeniu, wyposażonym m.in. w czujnik ruchu. Posiadała także oddzielne zasilanie elektryczne, a na wypadek przerw w dostawach energii serwer podłączono do urządzeń podtrzymujących zasilanie.

(dowód: akta kontroli str. 366-369)

2.9. W okresie objętym kontrolą obowiązywały m.in. cztery umowy dotyczące: sprawowania od 2 stycznia 2017 r. opieki informatycznej oraz zapewnienia bezpieczeństwa informacji i obsługi serwisowej jednego z systemów dziedzinowych, a także podłączenia i świadczenia od 3 lipca 2017 r. usług internetowych. Analiza tych umów wykazała, że ujęto w nich odpowiednie zapisy bezpieczeństwa, a podmioty zewnętrzne zobowiązały się do zachowania zasad poufności i właściwej ochrony informacji.

Z kolei w umowie na świadczenie usług poczty elektronicznej[14] nie ujęto zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający ujawnienie osobom nieuprawnionym, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 286-317, 378-380, 394-400)

2.10. SZBI obejmował procedurę zabezpieczenia danych przy przekazywaniu na zewnątrz sprzętu IT, w której przewidziano m.in.: wymontowywanie nośników danych bądź trwałe usuwanie danych osobowych. ASI prawidłowo nadzorował ten proces. W okresie objętym kontrolą zużyty i pozbawiony nośników sprzęt Urząd przekazywał za pokwitowaniem

[13] W trakcie oględzin weryfikacją objęto trzy wybrane systemy informatyczne.
[14] Umowa hostingu z „Nazwa.pl".

wyłącznie podmiotowi zatrudniającemu ASI, a drobne naprawy wykonywał osobiście lub przy pomocy współpracowników (nie zlecano ich na zewnątrz).
(dowód: akta kontroli str. 380, 382-393)

2.11. W Urzędzie korzystano wyłącznie z komputerów z systemami operacyjnymi z zainstalowanymi bieżącymi aktualizacjami. Jedyne urządzenie z oprogramowaniem nieposiadającym wsparcia producenta (komputer stacjonarny z systemem operacyjnym Windows XP) zostało wyłączone z eksploatacji i – jak wyjaśnił ASI – pozostawało na stanie Urzędu do momentu zutylizowania. Było to zgodne z wymogami określonymi w § 20 ust. 2 pkt 12 lit. a i f rozporządzenia w sprawie KRI. (dowód: akta kontroli str. 376-377, 379)

2.12. W procesie archiwizacji danych nie korzystano z mobilnych nośników danych. Kopie zapasowe wykonywano w Urzędzie w cyklu dziennym i tygodniowym (na oddzielnej partycji serwera głównego) oraz miesięcznym (na niezależnym serwerze znajdującym się innym pomieszczeniu niż główny serwer). W procesie archiwizacji i testowania danych korzystano ze specjalistycznego oprogramowania. Działania te wypełniały obowiązki wskazane w § 20 ust. 2 pkt 12 lit. b i e oraz § 20 ust. 2 pkt 7 rozporządzenia KRI.
(dowód: akta kontroli str. 366-380)

2.13. Wszystkie 10 komputerów (w tym cztery laptopy) poddanych oględzinom posiadało zainstalowane aktualne bazy oprogramowania antywirusowego, czym wypełniono wymagania § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI. (dowód: akta kontroli str. 366-371)

2.14. Monitorowanie pojemności nośników pamięci, zgodnie z postanowieniami SZBI, należało do zadań ASI, który nie korzystał w tym zakresie ze specjalistycznego oprogramowania i – jak wyjaśnił – weryfikował to w trakcie wykonywania miesięcznych kopii i testów bezpieczeństwa. W przypadku kończącej się pojemności, pamięć rozbudowywano, co po raz ostatni miało miejsce w lipcu 2016 roku. Na dzień oględzin Urząd dysponował dostateczną ilością wolnej przestrzeni na obu serwerach (zajęte było 66,2% i 59,2% przestrzeni). (dowód: akta kontroli str. 3-217, 366-380, 411-417)

2.15. SZBI oraz Plan ciągłości działania systemu informatycznego określały zasady i procedury związane z wdrażaniem zmian oprogramowania w Urzędzie, obejmujące m.in.: identyfikację, szacowanie, rejestrowanie i testowanie zmian, proces zatwierdzania proponowanych zmian, a także przywracanie prawidłowego funkcjonowania systemów. ASI wyjaśnił, że w momencie kiedy zachodziła potrzebna zmiany lub aktualizacji oprogramowania, wykorzystywał rozwiązanie oparte o tzw. maszynę wirtualną, które pozwalało na przywrócenie oprogramowania do stanu pierwotnego, gdy po aktualizacji oprogramowanie nie działało prawidłowo. (dowód: akta kontroli str. 3-222, 380)

2.16. Od 25 maja 2018 r. w Urzędzie prowadzono rejestr czynności przetwarzania danych, zawierający wszystkie elementy wymagane art. 30 ust. 1 RODO. Rejestr ten stanowił załącznik do PBDO z 25 maja 2018 r. i prowadzony był przez IDO w formie elektronicznej. Analogicznie do wcześniejszego okresu zawierał on 46 zidentyfikowanych zbiorów danych podlegających zabezpieczeniu. (dowód: akta kontroli str. 353-359)

Ustalone nieprawidłowości

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

1. Wnioski o odebranie upoważnienia do przetwarzania danych osobowych oraz uprawnienia dostępu w systemach informatycznych w przypadku jednego byłego pracownika złożone zostały do ABI oraz ASI po ponad miesiącu od dnia odejścia tej osoby z pracy (31 marca 2018 r.). Zgodnie z § 20 ust. 2 pkt 4–5 rozporządzenia w sprawie KRI, anulowanie upoważnienia i uprawnienia powinno nastąpić bezzwłocznie. Przygotowująca oba wnioski w tej sprawie Z-ca Kierownika USC wyjaśniła, że opóźnienie wynikało z jej przeoczenia, na skutek natłoku bieżących zadań. Według ASI, faktyczne cofnięcie uprawnień w systemach informatycznych dla tej osoby nastąpiło niezwłocznie, tj. po telefonicznym zgłoszeniu 2 kwietnia 2018 r. (ASI załączył także wydruk wskazujący na brak logowań tej osoby w kwietniu 2018 roku), a jedynie ze względu na pomyłkę pracownika Urzędu pisemne zgłoszenie (zgodne z procedurą SZBI) nastąpiło 2 maja 2018 r. Z kolei według IOD (do 24 maja 2018 r. pełniącego

funkcję ABI), cofnięcie upoważnienia do przetwarzania danych osobowych nastąpiło w dniu otrzymania wniosku (2 maja 2018 r.). (dowód: akta kontroli str. 360-380, 401)

2. W umowie na świadczenie usług poczty elektronicznej[15], 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 ujawnienie osobom nieuprawnionym. ASI wyjaśnił, że Urząd używał kont pocztowych podmiotu, który nie chciał podpisywać pisemnych umów w tym zakresie, a zawarcie umowy odbywało się poprzez akceptację regulaminu świadczenia usług, uruchomienie usługi i jej późniejsze opłacenie. We wspomnianym regulaminie nie było jednak zapisów zobowiązujących usługodawcę do zachowania poufności informacji związanych ze świadczeniem ww. usług. (dowód: akta kontroli str. 378-380, 394-400)

Uwagi dotyczące badanej działalności

W Urzędzie nie stosowano rozwiązania polegającego na szyfrowaniu dysków komputerów przenośnych, gdyż – według ASI – nie było takiej potrzeby, ze względu na korzystanie z większości tych urządzeń (czterech laptopów) wyłącznie w siedzibie Urzędu oraz utworzenie bezpiecznego połączenia dla osoby przetwarzającej dane poza siedzibą. Zdaniem NIK warto jednak 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. (dowód: akta kontroli str. 230, 366-371, 378-380)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości wdrożenie i wykorzystywanie rozwiązań technicznych oraz stosowanie i egzekwowanie rozwiązań organizacyjnych związanych z zapewnieniem bezpieczeństwa informacji.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W grudniu 2017 roku ABI wspólnie z ADO przeprowadzili – wymaganą § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI – okresową analizę ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie i sporządzili plan postępowania z ryzykiem (w ramach ochrony zasobów zidentyfikowano 84 zagrożenia i dla każdego z nich zaplanowano odpowiednie działania zapobiegawcze). Zdaniem IOD, poza sporządzonym w grudniu 2017 roku planem postępowania z ryzykiem ww. analiza oraz działania minimalizujące ryzyko były w Urzędzie prowadzone na bieżąco i obejmowały przede wszystkim: aktualizację dokumentacji (procedur) bezpieczeństwa, szkolenia pracowników, a także monitoring zasobów informatycznych (dokumentowany w dzienniku ASI). Na prawidłowość działań w tym zakresie – według IOD – wskazuje niezmaterializowanie się zagrożeń (poza dwoma incydentami). Dodał, że na koniec 2018 roku zaplanowano aktualizację planu postępowania z ryzykiem. (dowód: akta kontroli str. 320-337, 364)

3.2. Urząd opracował i wdrożył procedury postępowania z incydentami naruszenia bezpieczeństwa informacji, które stanowiły element SZBI. Obie instrukcje postępowania w tym zakresie (z 26 lutego 2016 r. i 25 maja 2018 r.) przewidywały m.in.: obowiązek niezwłocznego zgłaszania incydentów, wdrożenie działań minimalizujących szkody, przeprowadzanie postępowań wyjaśniających, a także dokumentowanie poszczególnych czynności.

W okresie objętym kontrolą w Urzędzie odnotowano dwa incydenty związane z naruszeniem bezpieczeństwa informacji (w czerwcu 2017 roku i w marcu 2018 roku). W obu przypadkach, niezwłocznie po zgłoszeniu (w dniu zgłoszenia lub w kolejnym dniu), wszczęto tzw. sprawdzenia doraźne (mające na celu ustalenie przyczyn, zakresu oraz skutków zgłoszonych incydentów). Nie stwierdzono winy pracowników Urzędu i naruszenia przepisów o ochronie danych osobowych, a także podjęto odpowiednie działania korygujące. (dowód: akta kontroli str. 81-84, 207-217, 231-243, 364)

3.3. Bezpośrednio po wejściu w życie SZBI (w marcu – kwietniu 2016 roku) wszystkich ówczesnych pracowników Urzędu przeszkolono z zakresu ochrony danych osobowych i bezpieczeństwa informacji (szkolenie obejmowało m.in.: zagrożenia bezpieczeństwa informacji i ich konsekwencje, zasady i środki zapewniające bezpieczeństwo, a także

[15] Umowa hostingu z „Nazwa.pl".

odpowiedzialność prawną z tym związaną), zapoznano z SZBI i zobowiązano do jego stosowania. Według IOD, w trakcie ww. szkolenia omówiono wszystkie cztery dokumenty składające się na SZBI, jednak bez upubliczniania treści załączników (zawierających m.in. listę zastosowanych zabezpieczeń) do tych dokumentów. Kolejne przeszkolenie przeprowadzone w kwietniu 2018 roku miało na celu przygotowanie kadry Urzędu do wejścia w życie nowych przepisów o ochronie danych osobowych (przede wszystkim RODO), a także zapoznanie z zaplanowaną zmianą regulacji wewnętrznych w tym zakresie (szerzej zagadnienie omówiono w pkt 3.6. niniejszego wystąpienia).

(dowód: akta kontroli str. 338-344, 363-365)

3.4. W grudniu 2017 roku ASI przeprowadził audyt wewnętrzny z zakresu bezpieczeństwa informacji, co stanowiło realizację wymogu § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI. W jego wyniku nie stwierdzono nieprawidłowości oraz potwierdzono wdrożenie wszystkich rekomendacji z poprzedniego audytu (z lutego 2017 roku). Zarekomendowano usprawnienie przepływu informacji oraz ciągłe monitorowanie przestrzegania zasad bezpieczeństwa, a w razie potrzeby aktualizację regulacji wewnętrznych. ASI zalecił także przyspieszenie prac wdrożeniowych systemu EZD. IOD wyjaśnił, że do końca I połowy 2018 roku zarówno on, jak i ASI nie weryfikowali wykonania ww. zalecenia, jednak po konsultacjach z pracownikami ocenił, że poziom wykorzystania tego narzędzia systematycznie rośnie. Dodał, że zalecenie jest realizowane.

(dowód: akta kontroli str. 250-274, 363-365)

3.5. W związku z wejściem w życie RODO, w Urzędzie przeprowadzono analizę prowadzonych procesów przetwarzania danych osobowych i dokonano oceny stopnia zapewnienia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk. Opracowano i zaktualizowano SZBI. (dowód: akta kontroli str. 85-217, 338-344, 363-365)

3.6. W związku z wejściem w życie RODO, 9 kwietnia 2018 r. IOD przeszkolił 12 pracowników Urzędu w tym zakresie. W ramach szkolenia omówiono m.in.: analizę ryzyka wiążącego się z przetwarzaniem danych osobowych, przesłanki legalności przetwarzania danych, problematykę umów powierzenia, podstawowe zabezpieczenia fizyczne, organizacyjne i informatyczne, ocenę skutków dla ochrony danych, rolę IOD, sposób postępowania w przypadku naruszenia ochrony danych, a także odpowiedzialność cywilną, karną i administracyjną z tym związaną. IOD 13 czerwca 2018 r. w tym samym zakresie przeszkolił kolejnego pracownika Urzędu. W czerwcu 2018 roku wszyscy pracownicy Urzędu potwierdzili zapoznanie się z SZBI, obowiązującym od 25 maja 2018 r.

(dowód: akta kontroli. str. 338-344)

Ustalone nieprawidłowości

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

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działania Urzędu w zakresie zapobiegania incydentom bezpieczeństwa informacji.

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[16], wnosi o:

1. Wdrożenie rozwiązań technicznych i organizacyjnych uwzględniających wymogi art. 25 RODO.
2. Opracowanie planu przeglądów Systemu Zarządzania Bezpieczeństwem Informacji, przewidzianego w Polityce Bezpieczeństwa Informacji.
3. Prowadzenie aktualnej i kompletnej inwentaryzacji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.
4. Bezzwłoczne odbieranie byłym pracownikom upoważnień do przetwarzania danych osobowych i uprawnień w systemach informatycznych.

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

5. Zawarcie w umowie na świadczenie usług poczty elektronicznej zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji oraz ich zabezpieczenia w sposób uniemożliwiający nieuprawnionym osobom ich ujawnienie.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 ustawy o NIK, kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Białymstoku.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Białystok, dnia 17 lipca 2018 r.

Kontroler
Adrian Gosk
specjalista kontroli państwowej

.....
podpis

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

.....
podpis