NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.010.01.2018
P/18/006

01464518

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

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli Delegatura w Białymstoku

Kontrolerzy

Beata Palinowska – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/69/2018 z 29 maja 2018 r. (dowód: akta kontroli str. 1)

Jednostka kontrolowana

Urząd Miasta Brańsk, ul. Rynek 8, 17-120 Brańsk (dalej: „Urząd")

Kierownik jednostki kontrolowanej

Czesław Sokołowski – Burmistrz Miasta Brańsk[1] (dowód: akta kontroli str. 2)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Uzasadnienie oceny ogólnej

Najwyższa Izba Kontroli ocenia negatywnie przyjęte i wdrożone rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa informacji w Urzędzie[3]. Stwierdzono bowiem następujące nieprawidłowości:

- nie opracowano dokumentacji dotyczącej ochrony danych osobowych, wymaganej przepisami 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)[4];
- nie poddawano przeglądom i nie aktualizowano obowiązujących w Urzędzie dokumentów składających się na SZBI w związku z wejściem w życie przepisów RODO, co było niezgodne z § 20 ust. 2 pkt 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];
- nie posiadano pełnych i aktualnych danych dotyczących użytkowanego sprzętu i oprogramowania oraz jego konfiguracji, wymaganych § 20 ust. 2 pkt 2 rozporządzenia KRI;
- dziesięciu pracownikom nadano uprawnienia administratora, mimo że nie wynikało to z zadań ustalonych w ich zakresach obowiązków, czym naruszono przepis 20 ust. 2 pkt 4 rozporządzenia KRI;
- kopie zapasowe tworzone w Urzędzie nie były regularnie testowane, co było niezgodne z § 20 ust. 2 pkt 12 lit b i e rozporządzenia KRI;
- nie prowadzono rejestru czynności przetwarzania danych, wbrew wymogom art. 30 RODO;
- nie odebrano niezwłocznie dostępu do systemu, zawierającego dane osobowe, pracownikowi, z którym rozwiązano stosunek pracy, czym naruszono przepisy § 20 ust. 2 pkt 5 w związku z § 20 ust. 2 pkt 4 rozporządzenia KRI;
- w 2017 roku nie przeprowadzono okresowego audytu z zakresu bezpieczeństwa informacji, przewidzianego § 20 ust. 2 pkt 14 rozporządzenia KRI.

---

1 Funkcję Burmistrza Miasta Brańsk pełni od 10 grudnia 2010 r.
2 Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
3 Kontrolą objęto okres od 1 czerwca 2017 r. do zakończenia czynności kontrolnych.
4 Dz. Urz. UE L z 2016.119.1. Rozporządzenie zwane dalej: „RODO".
5 Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Urzędzie 9 maja 2017 r. wdrożono System Zarządzania Bezpieczeństwem Informacji[6], zgodnie z § 20 ust. 1 rozporządzenia KRI. Dokumentami składającymi się na SZBI były: [1] Polityka Bezpieczeństwa Informacji[7], [2] Polityka Bezpieczeństwa Przetwarzania Danych Osobowych, [3] Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych[8], [4] Regulamin Ochrony Danych Osobowych, [5] Procedura postępowania z kluczami, [6] Analiza poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka. SZBI został zakomunikowany pracownikom Urzędu.

Za ustanowienie, wdrożenie, monitorowanie, przeglądanie, utrzymywanie i doskonalenie SZBI, zgodnie z § 7 Polityki bezpieczeństwa informacji, odpowiadał Burmistrz, a osobami wspierającymi go w tych działaniach byli: Administrator Systemu Informatycznego (dalej: „ASI") oraz Sekretarz Miasta. Szczegółowe zadania nie były uwzględnione w zakresach obowiązków pracowników. (dowód: akta kontroli str. 3-78)

1.2. W Urzędzie nie opracowano nowej dokumentacji uwzględniającej wymogi RODO oraz nie dostosowano i nie zaktualizowano obowiązujących uregulowań, dotyczących ochrony danych osobowych, do wymogów tego rozporządzenia (szerzej nieprawidłowość w tym zakresie opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 239-241)

Na stronie internetowej Urzędu 25 maja 2018 r. opublikowano informację dla klientów o uprawnieniach wynikających z przepisów RODO, w szczególności o prawie przysługującym osobom, których dane są przetwarzane do sprostowania danych, usunięcia i ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody na przetwarzanie danych, jeżeli dane są przetwarzane na podstawie zgody niewynikającej z obowiązków nałożonych przez przepisy prawa.
(dowód: akta kontroli str. 113-114)

1.3. Obowiązujące w Urzędzie dokumenty stanowiące SZBI, mimo obowiązku wynikającego z § 20 ust. 2 pkt 1 rozporządzenia KRI, nie były w okresie objętym kontrolą poddawane przeglądom i aktualizowane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości"). (dowód: akta kontroli str. 239-241)

1.4. W Urzędzie nie zostali wyznaczeni pracownicy odpowiedzialni za bezpieczeństwo informacji. Obowiązki ASI zostały powierzone firmie zewnętrznej świadczącej usługi z zakresu IT. Zgodnie z § 7 pkt 4 PBI, do obowiązków ASI należało w szczególności: zapewnienie bezpieczeństwa informacji w zakresie systemów i sieci teleinformatycznych; zarządzanie systemem informatycznym w Urzędzie; zabezpieczenie sieci komputerowej; wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem oraz utratą; opracowanie i aktualizacja procedur dotyczących systemów informatycznych. Kierowników referatów zobowiązano do zapewnienia, że podlegli im pracownicy posiadają odpowiedni poziom wiedzy o przepisach prawa i obowiązujących w Urzędzie zasadach dotyczących ochrony informacji oraz, że ich przestrzegają. (dowód: akta kontroli str. 48-52)

1.5. Burmistrz Brańska 10 maja 2018 r. zawarł z podmiotem zewnętrznym umowę w sprawie pełnienia funkcji IOD. Podpisano ją na czas określony, do 31 marca 2020 r. Zleceniobiorca zobowiązał się do pełnienia funkcji IOD, wymaganej art. 37 ust. 1 RODO. Osoba ta posiadała odpowiednie kwalifikacje do pełnienia tej funkcji (pełniła wcześniej obowiązki ABI, posiadała doświadczenie z zakresu informatyki, uczestniczyła w szkoleniu dla IOD). Do jej obowiązków, wynikających z umowy oraz art. 39 RODO należało m.in.: informowanie administratora, podmiotu przetwarzającego oraz pracowników o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii

[6] Dalej: „SZBI".
[7] Wprowadzona 9 maja 2017 r. Dalej: „PBI".
[8] Instrukcja zwana dalej: „Instrukcja zarządzania".

lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie; monitorowanie przestrzegania przepisów o ochronie danych; szkolenie personelu uczestniczącego w operacjach przetwarzania; udzielanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania; współpraca z organem nadzorczym; pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem. Ponadto zleceniobiorcę zobowiązano do sporządzania, sprawdzania i aktualizowania dokumentacji zgodnie z wymogami RODO. Umowa nie zawierała jednak harmonogramu realizacji poszczególnych zadań. W jej § 6 określono m.in., że w przypadku nienależytego wykonywania przez zleceniobiorcę obowiązków wynikających z umowy zostanie nałożona kara umowna, a w przypadku dłuższego (ponad 20 dni) niewykonywania obowiązków umowa może zostać rozwiązana. (dowód: akta kontroli str. 121-128)

1.6. IOD umożliwiono pełnienie obowiązków z sposób niezależny. Funkcję tę pełniła osoba wykonująca równocześnie zadania ASI. Powierzenie obowiązków IOD i ASI tej samej osobie mogło powodować konflikt interesów, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności".
(dowód: akta kontroli str. 3, 125-132, 245)

1.7. W Urzędzie opracowano regulacje wewnętrzne stanowiące szczegółowe dokumenty wykonawcze wymagane przez SZBI. Dokumenty te zostały wdrożone. Opracowano również inne dokumenty dotyczące bezpieczeństwa informacji: Wzór klauzuli poufności informacji, Rekomendacja odpowiedniej postawy osób posiadających upoważnienie do przetwarzania danych osobowych. (dowód: akta kontroli str. 48-76)

1.8. Regulacje wewnętrzne, stanowiące dokumenty wykonawcze, wymagane przez PBI były dostępne w formie papierowej wyłącznie dla osób odpowiedzialnych za realizację poszczególnych czynności wymaganych tymi dokumentami. Pracownicy potwierdzili zapoznanie się z dokumentacją wymaganą dla ich stanowisk. Zapoznano ich z PBI, Polityką ochrony danych osobowych, Instrukcją zarządzania, Regulaminem ochrony danych i Procedurą postępowania z kluczami. (dowód: akta kontroli str. 77-78, 239-241)

1.9. W Urzędzie zidentyfikowano zbiory danych podlegające zabezpieczeniu, w tym zawierające dane osobowe. Prowadzony był rejestr zbiorów danych, stanowiący załącznik do Polityki ochrony danych osobowych. Składał się on z 35 zbiorów danych i zawierał: nazwę zbioru danych, sposób prowadzenia zbioru, sposób zabezpieczenia, system informatyczny służący do przetwarzania danych (w przypadku danych przetwarzanych w formie elektronicznej), lokalizację, zastosowane zabezpieczenia. Wobec wszystkich zbiorów danych przypisano i zastosowano odpowiedni (wysoki) poziom zabezpieczeń technicznych i organizacyjnych, zgodny z ich wagą. (dowód: akta kontroli str. 30-33)

1.10. Urząd, nie zapewnił aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, bowiem nie posiadał systemu do zarządzania zasobami IT, służącego do tego celu. Było to niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI. Ponadto, 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, przez co możliwe będzie odtworzenie po katastrofie lub innym zdarzeniu losowym. Szerzej nieprawidłowość w tym zakresie opisano poniżej, w sekcji „Ustalone nieprawidłowości".

Na dzień 31 grudnia 2017 r. przeprowadzono inwentaryzację do celów rachunkowości. Wówczas posiadane zasoby informatyczne zostały przypisane do osób odpowiedzialnych za dany sprzęt. (dowód: akta kontroli str. 158, 239-241)

Ustalone nieprawidłowości

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

1. Urząd nie posiadał dokumentacji dotyczącej ochrony danych osobowych uwzględniającej wymogi RODO, mimo że powinna być ona opracowana do 25 maja 2018 r., tj. do dnia wejścia w życie RODO. Jednym z powodów było nieustalenie w umowie dotyczącej pełnienia funkcji IOD terminów realizacji poszczególnych zadań powierzonych IOD (szerzej na ten temat w pkt 1.5. niniejszego wystąpienia).

Burmistrz Brańska wyjaśnił, że: *„Wobec niejasności części przepisów RODO, od początku tego roku poszukiwaliśmy firmy, która mogłaby nam pomóc sprostaniu wymogom. Większość oferowała „gotową" dokumentację za opłatą i pomoc „zdalną". […] Ostatecznie po rozmowach, 10 maja 2018 r. podpisaliśmy umowę z firmą w obowiązkach której jest także dokumentacja. Staraliśmy się osiągnąć gotowość na 25 maja uznając, że rozporządzenie RODO jest fundamentem, który posłuży do ustawowych zmian w polskim prawie. Obecnie nasza dokumentacja jest opracowywana […]".* (dowód: akta kontroli str. 3-76, 239-241, 244-248)

2. Obowiązujące w Urzędzie dokumenty składające się na SZBI, wbrew wymogom § 20 ust. 2 pkt 1 rozporządzania KRI, nie były (w okresie objętym kontrolą) poddawane przeglądom i aktualizowane, mimo takiej konieczności, wynikającej m.in. ze zmiany przepisów o ochronie danych osobowych. Nie opracowano również planu ciągłości działania.

   Burmistrz Brańska wyjaśnił, że: *„Uznaliśmy, że dokumentacja, którą posiadamy jest wystarczająca. Zmiany w dokumentacji zaplanowano na wiosnę 2018 r. Dopiero od 25 maja 2018 r. obowiązuje nowa ustawa o ochronie danych osobowych. W związku z tym cała dokumentacja zostanie dostosowana do jej wymogów z uwzględnieniem RODO i innych zmian w przepisach, które właśnie następują".*
   (dowód: akta kontroli str. 3-76, 239-241, 244-248)

3. Urząd, wbrew § 20 ust. 2 pkt 2 rozporządzenia KRI, nie posiadał aktualnych informacji o posiadanych zasobach informatycznych, obejmujących ich rodzaj i konfigurację. Ponadto spis aktywów informatycznych powinien być sporządzany i aktualizowany w sposób umożliwiający odtworzenie infrastruktury informatycznej po katastrofie lub innym zdarzeniu losowym (pkt 8.1.1 normy PN-ISO/IEC 27002:2014-12).

   Burmistrz Brańska wyjaśnił, że: *„Rejestru bieżącego zasobów informatycznych nie prowadzono ze względu na koszty programu komputerowego, który dla małego Urzędu jest stosunkowo drogi. […] nie zanotowano w Urzędzie żadnych zdarzeń losowych, które spowodowałyby utratę danych lub sprzętu poza fizycznym zużywaniem się.* (dowód: akta kontroli str. 239-241, 244-248)

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że równoczesne pełnienie funkcji IOD oraz ASI przez tą samą osobę może powodować konflikt interesów. IOD uczestniczy bowiem w ustanawianiu zasad i sposobów przetwarzania informacji, natomiast ASI odpowiada za ich wprowadzenie w systemach informatycznych. Burmistrz wyjaśnił, że powierzając obowiązki IOD tej samej osobie kierował się dotychczasową dobrą współpracą, znajomością podmiotu. Ponadto wyjaśnił, że firma obsługująca znała system, a wprowadzenie dodatkowego podmiotu z dostępem do baz danych mogło wpłynąć na osłabienie ochrony informacji w Urzędzie.
(dowód: akta kontroli str. 3, 125-132, 245)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie organizację systemu bezpieczeństwa informacji w Urzędzie.

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

Opis stanu faktycznego

2.1. Na wszystkich dziesięciu – objętych oględzinami – komputerach[9] użytkownicy posiadali uprawnienia administratora. Nie ograniczono im możliwości zainstalowania nieautoryzowanego oprogramowania, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 232-238)

2.2. Analiza uprawnień do systemów informatycznych służących do przetwarzania danych nadanych 15 (z 25) pracownikom Urzędu (w tym czterem zatrudnionym na stanowiskach kierowniczych), zaangażowanym w proces przetwarzania informacji wykazała, że były one adekwatne do zadań i obowiązków realizowanych przez te osoby. Tym samym wypełniono obowiązek wynikający z § 20 ust. 2 pkt 4 rozporządzenia KRI.
(dowód: akta kontroli str. 160-165, 232-236, 242)

[9] Trzy komputery przenośne i siedem stacjonarnych.

W okresie objętym kontrolą żaden pracownik nie zmienił stanowiska pracy bądź komórki organizacyjnej. Stosownie do § 9 Instrukcji Zarządzania, za nadawanie, modyfikowanie i odbieranie uprawnień odpowiadał ASI, który realizował te zadania na pisemne zlecenie Burmistrza Brańska. Pracownicy, którym nadawane były uprawnienia dostępu do systemu informatycznego byli zapoznawani z obowiązującymi w Urzędzie zasadami bezpieczeństwa przetwarzania danych oraz zobowiązani do zachowania poufności.

(dowód: akta kontroli str. 14-26, 159)

2.3. W okresie objętym kontrolą żaden pracownik nie zakończył zatrudnienia w Urzędzie. Jednemu pracownikowi zablokowano dostęp do systemu informatycznego 18 czerwca 2018 r. (w trakcie kontroli), tj. po ponad 11 latach od ustania zatrudnienia (27 kwietnia 2007 r.). Szerzej wymienioną nieprawidłowość opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 159, 202)

2.4. Na podstawie oględzin trzech systemów informatycznych służących do przetwarzania danych[10] przez Urząd stwierdzono, że – w myśl przepisów § 20 ust. 2 pkt 7 rozporządzenia KRI – zapewniono ochronę przetwarzanych informacji przed nieuprawnionym dostępem, poprzez zastosowanie indywidualnych haseł dostępu. Wymogi w zakresie odpowiedniej złożoności i długości hasła, a także okresu ważności zostały określone w § 10 Instrukcji zarządzania. Oględziny dziesięciu stanowisk komputerowych wykazały, że użytkownicy, logując się do systemów operacyjnych tych komputerów, wprowadzali hasła o wymaganej liczbie znaków.

(dowód: akta kontroli str. 14-26, 207-209, 232-236)

2.5. Dane wyświetlane na ekranie pięciu komputerów, na których realizowane były zadania związane z obsługą klientów Urzędu, tj. w Urzędzie Stanu Cywilnego, w Sekretariacie oraz w Referacie Finansowo-Budżetowym, nie były widoczne dla osób nieuprawnionych. Spełnione tym samym zostały wymogi określone w § 20 ust. 2 pkt 7 rozporządzenia KRI. (dowód: akta kontroli str. 230)

2.6. W Instrukcji zarządzania ustalono następujące zasady użytkowania sprzętu i oprogramowania poza siedzibą Urzędu: [1] w przypadku przetwarzania zbioru danych wykonywanie regularnej lub automatycznej kopii bezpieczeństwa, [2] zabezpieczenie dostępu hasłem. Sekretarz Miasta wyjaśnił, że brak innych procedur w tym zakresie wynika z tego, że komputery przenośne są użytkowane wyłącznie w siedzibie Urzędu.

(dowód: akta kontroli str. 14-26)

2.7. W Urzędzie były wykorzystywane trzy komputery przenośne (laptopy). Nie posiadały one oprogramowania odpowiedzialnego za szyfrowanie danych na dyskach twardych, gdyż – jak wyjaśnił IOD – wykorzystywano je wyłącznie w Urzędzie (co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności").

(dowód: akta kontroli str. 232-236, 249-252)

2.8. W serwerowni Urzędu, stosownie do przepisów § 20 ust. 2 pkt 9 rozporządzenia KRI, zastosowano odpowiednie rozwiązania umożliwiające zabezpieczenie informacji przed nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem. Dostęp do niej miał ASI oraz upoważniony pracownik. Serwerownia znajdowała się w nieoznakowanym pomieszczeniu, wyposażonym w klimatyzator. Wyposażona została w oddzielne połączenie z siecią elektryczną. Serwery (trzy) podłączone były do urządzeń UPS.

(dowód: akta kontroli str. 229)

2.9. W czterech umowach serwisowych obowiązujących w okresie objętym kontrolą, które zawarte zostały z firmami zewnętrznymi i dotyczyły: [1] serwisu oprogramowania (dwie umowy); [2] pełnienia funkcji IOD; [3] serwisu sprzętu komputerowego ujęto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Wykonawców, zgodnie z wymogiem określonym w § 20 ust. 2 pkt 10 rozporządzenia KRI, zobowiązano do zachowania w tajemnicy informacji, do których uzyskali dostęp w związku z realizacją tych umów. (dowód: akta kontroli str. 125-129, 142, 146-150)

[10] Elektroniczne Zarządzanie Dokumentacją, Gospodarowanie odpadami, Obsługa finansowo-księgowa Urzędu.

2.10. Procedury dotyczące przekazywania urządzeń informatycznych na zewnątrz Urzędu zawarte zostały w Instrukcji zarządzania. Użytkowników zobowiązano do niezwłocznego i trwałego usuwania / kasowania danych z nośników uszkodzonych (i z tego powodu podlegających likwidacji) oraz takich, dla których ustał powód przechowywania. Przestarzałe nośniki powinny być niszczone komisyjnie, a nośniki zamontowane w sprzęcie IT – wymontowane lub wyczyszczone specjalistycznym oprogramowaniem przed przekazaniem poza Urząd (Sekretarz Miasta wyjaśnił, że w okresie objętym kontrolą nie były przekazywane poza Urząd nośniki danych, a zatem nie było konieczności zastosowania ustalonych regulacji). (dowód: akta kontroli str. 14-26, 239-241)

2.11. W Urzędzie nie były użytkowane komputery wykorzystujące systemy operacyjne nieobjęte wsparciem producenta[11]. Na podstawie oględzin dziesięciu (z 19) stanowisk komputerowych stwierdzono, że w myśl § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI, systemy operacyjne posiadały zainstalowane bieżące aktualizacje.

(dowód: akta kontroli str. 232-236)

2.12. Kopie zapasowe danych w systemach informatycznych były wykonywane codziennie (w dni robocze) i przechowywane, z ostatnich pięciu dni, na serwerach znajdujących się w serwerowni. Dodatkowo, zgodnie z § 12 Instrukcji zarządzania, kopie zapasowe były raz w miesiącu zapisywane na nośnikach danych (płytach CD), które przechowywano w pomieszczeniu innym niż serwerownia, w metalowej, zamykanej na klucz szafie. W wyniku oględzin stwierdzono, że sposób przechowywania kopii zapasowych spełniał wymogi określone w § 20 ust. 2 pkt 7 rozporządzenia KRI.

Urząd nie prowadził jednak testów sporządzonych kopii zapasowych, co było niezgodne z § 20 ust. 2 pkt 12 lit. b i e rozporządzenia KRI. Zagadnienie to szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 14-26, 231, 239-241)

2.13. Na wszystkich 10 poddanych oględzinom stanowiskach komputerowych zainstalowane było oprogramowanie antywirusowe z aktualną bazą wirusów. Spełniono tym samym wymóg określony w § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI.

(dowód: akta kontroli str. 232-236)

2.14. ASI monitorował doraźnie pojemność pamięci masowych (dysków twardych) wykorzystywanych w serwerach. Były one wykorzystane w 22%, 47% i 54%.

(dowód: akta kontroli str. 231)

2.15. W Urzędzie nie przyjęto procedur / instrukcji wprowadzania zmian w oprogramowaniu wykorzystywanym w Urzędzie. ASI wyjaśnił, że przyjęty sposób wdrażania zmian umożliwiał poprawne ich funkcjonowanie, miał charakter usystematyzowanych działań i ograniczał ryzyko wystąpienia problemów w działaniu systemów informatycznych w związku z wprowadzonymi zmianami. Składał się on z następujących etapów: [1] identyfikowanie i rejestrowanie znaczących zmian w zakresie oprogramowania wykorzystywanego w Urzędzie; [2] planowanie i testowanie zmian; [3] szacowanie potencjalnego wpływu wprowadzanych zmian na działanie środowiska informatycznego, także ich wpływu na bezpieczeństwo informacji; [4] formalne zatwierdzanie proponowanych zmian; [5] przekazanie informacji o zmianach wszystkim zainteresowanym pracownikom; [6] procedury przywracania, w tym procedury na wypadek niepomyślnych zmian lub nieprzewidzianych zdarzeń.

(dowód: akta kontroli str. 3-76, 249-252)

2.16. W Urzędzie nie był prowadzony rejestr czynności przetwarzania danych osobowych, określony w art. 30 RODO, co szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 239-241, 244-248, 253-255)

Ustalone nieprawidłowości

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

1. Użytkownicy dziesięciu poddanych oględzinom stanowisk komputerowych posiadali uprawnienia administratora, mimo że nie byli administratorami systemów

[11] Windows XP lub wcześniejsze wersje tego systemu.

informatycznych. Pracownikom tym – wbrew wymogom § 20 ust. 2 pkt 4 rozporządzenia KRI – umożliwiono zatem instalowanie dowolnego oprogramowania (w trakcie kontroli nieprawidłowość została usunięta).

ASI wyjaśnił, że 23 czerwca 2018 r. przeprowadził kontrolę i zmodyfikował ustawienia systemów operacyjnych na stacjach roboczych użytkowanych przez pracowników Urzędu. (dowód: akta kontroli str. 232-238, 253-255)

2. Pracownikowi, z którym 27 kwietnia 2007 r. rozwiązano stosunek pracy, odebrano uprawnienia do systemu informatycznego 18 czerwca 2018 r. (w trakcie kontroli NIK), tj. po upływie ponad 11 lat. Naruszono tym samym postanowienia § 20 ust. 2 pkt 5 rozporządzenia KRI w związku z § 20 ust. 2 pkt 4 tego rozporządzenia oraz § 9 Instrukcji zarządzania.

   ASI wyjaśnił, że: *„Służby informatyczne nie miały informacji na temat odebrania uprawnień logowania do dziedzinowego oprogramowania dla użytkownika* [...]".

   Burmistrz Brańska wyjaśnił, że: *„Pani [...] zakończyła pracę w Urzędzie w 2007 r. Wówczas od razu nie zablokowano jej dostępu do programu. Ten błąd mógł wynikać z przeoczenia i pozostawał niezauważony. [...] Po zauważeniu tego błędu został on naprawiony"*. (dowód: akta kontroli str. 159, 202, 244-248, 253-255)

3. W Urzędzie nie sprawdzano kopii zapasowych pod kątem prawidłowości ich odtworzenia (testowanie), co było niezgodne z § 20 ust. 2 pkt 12 lit. b i e rozporządzenia KRI, w myśl którego zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polega w szczególności na dbałości o aktualizację oprogramowania oraz minimalizowaniu ryzyka utraty informacji w wyniku awarii.

   ASI wyjaśnił, że *„Służby informatyczne traktują obowiązek tworzenia kopii jako priorytetowy i wymagający należytego postępowania. Kopia baz danych znajdujących się na serwerze odbywa się codziennie. Na serwerze jest zainstalowany system do tworzenia kopii. Ponadto są przechowywane kopie baz danych w katalogu na dysku twardym. Jakość kopii była potwierdzana poprzez odtwarzanie wcześniej utworzonych kopii baz danych. Sprawdzanie, jakości kopii nie ma charakteru okresowego, ale odbywa się wybiórczo od przypadku do przypadku"*.

   (dowód: akta kontroli str. 14-26, 231, 239-241)

4. W Urzędzie – wbrew wymogom określonym w art. 30 RODO – nie prowadzono rejestru czynności przetwarzania danych osobowych.

   Burmistrz Miasta wyjaśnił, że: *„Rozporządzenie RODO nie jest jasne, początkowo obowiązek z artykułu 30 rozpatrywaliśmy w kontekście ust. 5, co okazało się niewłaściwe. Oczekiwaliśmy na dodatkowe krajowe unormowania prawne, licząc na uściślenia i komentarze. Niestety te zaczęły się ukazywać z dużym opóźnieniem (dopiero od 25 maja tego roku). Dlatego, w celu wywiązania się z obowiązku w dniu 10 maja 2018 r. zawarliśmy umowę z podmiotem zewnętrznym, który jako IOD zobowiązał się do sporządzania, sprawdzania oraz aktualizowania dokumentacji zgodnie z wymogami RODO. Na dzień dzisiejszy rejestr czynności nadal jest opracowywany. Polecono przyśpieszenia prac nad zakończeniem opracowywania i wdrożeniem tego dokumentu"*.

   IOD wyjaśnił, że: *„Umowa na świadczenie usługi Inspektora Ochrony Danych została podpisana pomiędzy stronami 10 maja 2018 r. Strony ustaliły, że dokumentacja, która jest potrzebna do wdrożenia RODO będzie sukcesywnie tworzona i wdrażana"*.

   (dowód: akta kontroli str. 239-241, 244-248, 253-255)

Uwagi dotyczące badanej działalności

W Urzędzie nie stosowano rozwiązania polegającego na szyfrowaniu dysków komputerów przenośnych. ASI wyjaśnił, że nie wykonywano pracy na odległość i przy przetwarzaniu mobilnym nie było potrzeby używania oprogramowania do szyfrowania danych. NIK zauważa, 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. (dowód: akta kontroli str. 251)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie wdrożenie i wykorzystywanie rozwiązań technicznych oraz stosowanie i egzekwowanie rozwiązań organizacyjnych związanych z zapewnieniem bezpieczeństwa informacji w Urzędzie.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Urzędzie 9 maja 2017 r. przeprowadzono analizę ryzyka utraty integralności, poufności lub dostępności informacji, wymaganą § 20 ust. 2 pkt 3 rozporządzenia KRI, oraz podjęto działania naprawcze związane z wynikami tej analizy. Zidentyfikowano następujące zagrożenia związane z fizycznymi zabezpieczeniami zasobów: odcięcie zasilania, kradzież, awaria sprzętu. W celu zmniejszenia zagrożeń, podjęto działania minimalizujące możliwość wystąpienia zidentyfikowanych zagrożeń.

W 2018 roku nie przeprowadzono analizy ryzyka. Burmistrz Brańska wyjaśnił, że: *„Założyliśmy, że analizy ryzyka utraty integralności, poufności lub dostępności będziemy dokonywali raz w roku. Ostatnia odbyła się w maju 2017 r. Ze względu na kontrolę kolejna miała odbyć się w czerwcu, ale przeprowadzona zostanie w lipcu. Praktyka wykazała, że Urząd na dzień dzisiejszy odnotowuje pojedyncze drobne incydenty, w postaci próby przesłania w korespondencji mailowej dołączonego złośliwego oprogramowania (trojany, rookity i wirusy), z którymi radzimy sobie, jak dotychczas bez problemów. W tym zakresie pracownicy zostali poinformowani i wiedzą jak reagować na takie przypadki*".

(dowód: akta kontroli str. 53-74, 239-241)

3.2. W Urzędzie umożliwiono pracownikom bezzwłoczne zgłaszanie incydentów dotyczących bezpieczeństwa informacji i danych osobowych, zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI. W myśl z Instrukcji alarmowej, będącej elementem *Polityki ochrony danych*, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych pracownicy Urzędu zobowiązani są do poinformowania o tym fakcie bezpośredniego przełożonego lub ADO. W przypadku stwierdzenia incydentu, ADO prowadzi udokumentowane postępowanie wyjaśniające: [1] ustala czas wystąpienia, zakres, przyczyny, skutki oraz zaistniałe szkody; [2] zabezpiecza dowody; [3] podejmuje działania naprawcze; [4] inicjuje działania dyscyplinarne; [5] wyciąga wnioski oraz rekomenduje działania korygujące. Zdarzenia kwalifikowane jako incydenty bezpieczeństwa zostały opisane w pkt 3 ww. Instrukcji. W okresie objętym kontrolą wystąpiło sześć incydentów, polegających na skierowaniu do Urzędu e-maili zawierających szkodliwe oprogramowanie. Podjęto działania zaradcze, polegające na usunięciu e-maili zawierających szkodliwe oprogramowanie. (dowód: akta kontroli str. 14-26, 115-116)

3.3. Pracownicy zaangażowani w proces przetwarzania informacji nie uczestniczyli w cyklicznych szkoleniach z zakresu bezpieczeństwa informacji, obejmujących zagadnienia o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów naruszenia bezpieczeństwa informacji. Problematyka ta została 21 listopada 2017 r. omówiona przez Sekretarza Miasta podczas wewnętrznego szkolenia z zakresu ochrony danych osobowych (incydenty związane z naruszeniem bezpieczeństwa informacji i reagowanie na nie, ryzyka związane z przetwarzaniem danych osobowych, ustawienie monitora, hasła, nośniki informacji). (dowód: akta kontroli str. 77-78, 139-141)

3.4. W Urzędzie 24 maja 2018 r. przeprowadzono audyt wewnętrzny z zakresu bezpieczeństwa informacji, wymagany § 20 ust. 2 pkt 14 rozporządzenia KRI. Obejmował on w szczególności sprawdzenie obowiązującej w Urzędzie dokumentacji dotyczącej ochrony danych osobowych, przestrzeganie przez pracowników regulacji wewnętrznych oraz wynikających z przepisów prawa (m.in. stosowanie zabezpieczeń, sporządzanie kopii zapasowych, reagowanie na incydenty dotyczące naruszenia bezpieczeństwa informacji, ochrona i zmiana hasła dostępu do systemów informatycznych, blokowanie dostępu do komputera oraz kończenie pracy, postępowanie w przypadku awarii), zastosowanie zabezpieczenia komputerów przed zagrożeniami pochodzącymi z sieci publicznej, środki ochrony zastosowane do uwierzytelniania przesyłanych danych.

W wyniku audytu sformułowano rekomendacje w zakresie wprowadzenia Polityki kluczy, odpowiedniej do potrzeb Urzędu, modernizacji wyposażenia (szaf i zamków) oraz przeprowadzenia rozmów z pracownikami, dotyczących bezpieczeństwa informacji (bezpiecznego używania sprzętu, stref przetwarzania danych osobowych, możliwych zagrożeń).

W 2017 roku w Urzędzie został przeprowadzony audyt z zakresu bezpieczeństwa informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 91-112, 139-141)

3.5. W związku z art. 32 ust. 1 RODO, w Urzędzie przeprowadzono 18 maja 2018 r. kontrolę dotyczącą przetwarzania danych osobowych (w tym danych wrażliwych), a 24 maja 2018 r. – audyt wewnętrzny, obejmujący zagadnienia z zakresu przetwarzania danych osobowych oraz dokonano oceny stopnia zapewnienia ich bezpieczeństwa. Podejmowane czynności w ramach ww. działań obejmowały w szczególności zabezpieczenia techniczne i organizacyjne, tj. podjęcie działań w celu opracowania procedur korzystania z Internetu i poczty elektronicznej, przeprowadzenie profilaktycznych rozmów z pracownikami dotyczących bezpieczeństwa informacji na wszystkich stanowiskach pracy, uzupełnienie zabezpieczeń w szafach. (dowód: akta kontroli str. 80-111)

3.6. Dwóch pracowników (z 19) Urzędu uczestniczyło w 2017 roku i 2018 roku w trzech szkoleniach, dotyczących zagadnień związanych z wejściem w życie przepisów RODO. Obejmowały one m.in. zmiany w zakresie danych osobowych kandydatów do pacy i pracowników oraz nowe zasady przetwarzania danych osobowych. W Urzędzie 21 listopada 2017 r. przeprowadzono wewnętrzne szkolenie z zakresu danych osobowych, w którym uczestniczyli wszyscy pracownicy. Szkolenie obejmowało zagadnienia związane ze zmianą przepisów dotyczących ochrony danych osobowych (kluczowe wymagania z zakresu ochrony danych osobowych, bezpośrednia odpowiedzialność osób przetwarzających dane, zgłaszanie naruszeń, nowe prawa obywateli, incydenty i reagowanie na nie, ryzyka związane z przetwarzaniem danych osobowych, dokumentacja ochrony danych osobowych w Urzędzie i obowiązek jej stosowania).
(dowód: akta kontroli str. 77-78)

Ustalone nieprawidłowości

W działalności jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na nieprzeprowadzeniu w 2017 roku okresowego audytu z zakresu bezpieczeństwa informacji, wymaganego przepisami § 20 ust. 2 pkt 14 rozporządzenia KRI.

Burmistrz Brańska wyjaśnił, że ze względu na niewielkie rozmiary Urzędu oraz koszty z tym związane audyty nie były przeprowadzane. (dowód: akta kontroli str. 139-141, 244-248)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie podjęte przez Urząd działania w celu 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[12], wnosi o:

1. Ustalenie harmonogramu (terminów i częstotliwości) realizacji zadań IOD, powierzonych podmiotowi zewnętrznemu, w szczególności w zakresie opracowania dokumentacji uwzględniającej wymogi RODO.
2. Dostosowanie obowiązującej w Urzędzie dokumentacji do wymogów RODO oraz poddawanie przeglądom i aktualizowanie dokumentacji składającej się na SZBI.
3. Przeprowadzenie kompletnej inwentaryzacji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.
4. Regularne testowanie kopii zapasowych sporządzanych w Urzędzie.
5. Prowadzenie rejestru czynności przetwarzania danych osobowych wymaganego art. 30 RODO.

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

6. Przeprowadzanie w Urzędzie, co najmniej raz w roku, audytu w zakresie bezpieczeństwa informacji.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Białystok, dnia 17 lipca 2018 r.

Kontroler
Beata Palinowska
starszy inspektor kontroli państwowej

Palinowska Beata
podpis

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

podpis