NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.11.2017
P/17/062

# WYSTĄPIENIE POKONTROLNE

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

# I. Dane identyfikacyjne kontroli

| | |
|---|---|
| *Numer i tytuł kontroli* | P/17/062 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim |
| *Jednostka przeprowadzająca kontrolę* | Najwyższa Izba Kontroli Delegatura w Białymstoku |
| *Kontrolerzy* | Wojciech Olszewski – doradca ekonomiczny, upoważnienie do kontroli nr LBI/164/2017 z 27 listopada 2017 r. (dowód: akta kontroli str. 1-2) |
| *Jednostka kontrolowana* | Urząd Miasta Bielsk Podlaski, ul. Kopernika 1, 17-100 Bielsk Podlaski (dalej „Urząd") |
| *Kierownik jednostki kontrolowanej* | Jarosław Borowski – Burmistrz Bielska Podlaskiego[1] (dowód: akta kontroli str. 3) |

# II. Ocena kontrolowanej działalności[2]

**Ocena ogólna**

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości zapewnienie przez Urząd[3] właściwej ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem.

Uzasadnienie oceny ogólnej

Pozytywna ocena wynika w szczególności z odpowiedniego poziomu wykonania zabezpieczeń odpowiadających za autoryzację dostępu do sieci, opracowania dokumentacji dotyczącej przetwarzania danych osobowych (Polityka bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym) i ich aktualizowania oraz przechowywania i zabezpieczenia danych w sposób odpowiadający przepisom i przyjętym procedurom.

Stwierdzone nieprawidłowości dotyczyły m.in.:

- braku skutecznego nadzoru nad działalnością poszczególnych użytkowników systemów informatycznych Urzędu zaangażowanych w proces przetwarzania informacji, w szczególności w zakresie korzystania z pamięci masowych,
- niezgodności ze stanem faktycznym zbiorów danych osobowych zgłoszonych Generalnemu Inspektorowi Ochrony Danych Osobowych (dalej „GIODO") oraz zakresów danych osobowych przetwarzanych w tych zbiorach,
- niepełnej realizację obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[4].

NIK zwraca również uwagę, że Administrator Bezpieczeństwa Informacji (dalej: „ABI") nie zakończył realizacji zadania dotyczącego weryfikacji zbiorów danych osobowych wymienionych w wykazach takich zbiorów i identyfikacji nowych zbiorów danych osobowych, co może wpłynąć w sposób istotny na konieczność aktualizacji dokumentacji dotyczącej przetwarzania danych osobowych i funkcjonowanie systemu zarządzania bezpieczeństwem informacji w Urzędzie.

---

1 Pan Jarosław Borowski burmistrzem jest od 1 grudnia 2014 r. (od 30 grudnia 2013 r. do 30 listopada 2014 r. pełnił funkcję Burmistrza Bielska Podlaskiego).

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

3 Kontrolą objęty został okres od 1 stycznia 2016 r. do zakończenia czynności kontrolnych oraz okres wcześniejszy jeśli miał wpływ na kontrolowaną działalność.

4 Dz. U. z 2016 r. poz. 922.

# III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

**1.1**. W Urzędzie do gromadzenia i przetwarzania danych wykorzystywano 13 systemów informatycznych, które zostały wymienione w pkt 4 niniejszego wystąpienia pokontrolnego. Przyjęto – zgodnie z § 6 ust. 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[5] – wysoki poziom zabezpieczeń, gdyż wszystkie stanowiska komputerowe, na których znajdowały się systemy służące do przetwarzania danych osobowych (poza przeznaczonymi do obsługi systemu „Źródło") posiadały dostęp do otwartego Internetu. (dowód: akta kontroli str. 4-53, 149)

Oględziny 32 stanowisk komputerowych (użytkowanych przez 28 pracowników Urzędu)[6] z 99 wykorzystywanych do przetwarzania danych osobowych wykazały, że żadnemu z użytkowników nie nadano uprawnień administratora umożliwiających instalowanie niewiadomego pochodzenia oprogramowania lub zmianę ustawień systemu operacyjnego bądź programów dziedzinowych, w tym ingerencję w rejestry zdarzeń. Każdy z komputerów poddanych oględzinom (poza urządzeniami z zainstalowaną aplikacją „Źródło" – sześć sztuk) posiadał dostęp do Internetu oraz możliwość podłączenia pamięci zewnętrznej lub zapisu na nośniku optycznym (także komputery z zainstalowaną aplikacją „Źródło"). Pracownicy zaangażowani w przetwarzanie danych w systemach informatycznych Urzędu posiadali własne loginy i hasła do systemu operacyjnego jednostek komputerowych oraz do systemów dziedzinowych. Złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych oraz Polityki bezpieczeństwa danych osobowych w Urzędzie Miasta Bielsk Podlaski (dalej „PB") i Instrukcji zarządzania systemem informatycznym do przetwarzania danych osobowych (dalej „IZSI"). Oględziny wykazały też m.in., że:

- Na każdym urządzeniu dostęp do systemu operacyjnego możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła.
- Comiesięczna zmiana hasła do systemu operacyjnego wymuszana była w sposób automatyczny, a wymuszanie haseł w systemach dziedzinowych było zależne od możliwości poszczególnych aplikacji.
- W 26 (z 32) komputerach zapewniono automatyczną aktualizację systemów operacyjnych. Wyjątkiem były komputery obsługujące aplikację „Źródło", które nie były podłączone do Internetu. Informatyk Urzędu wyjaśnił, że do automatycznej aktualizacji systemu operacyjnego potrzebne jest połączenie z Internetem, którego nie posiadają komputery obsługujące program „Źródło" (funkcjonują w wydzielonej sieci). Ręczna instalacja aktualizacji nie była przeprowadzana z obawy o poprawność działania programu „Źródło".
- Komputery do obsługi aplikacji „Źródło" miały zainstalowane oprogramowanie antywirusowe, lecz w trzech z nich program antywirusowy zakupiony przez Urząd i baza wirusów nie były aktualizowane, a w trzech kolejnych program antywirusowy zakupiony przez Ministerstwo Cyfryzacji do aplikacji „Źródło" aktualizował się przez wydzieloną sieć. W przypadku pozostałych 26 komputerów oprogramowanie antywirusowe było aktualizowane na bieżąco. Informatyk Urzędu wyjaśnił, że część komputerów miała zainstalowany program antywirusowy zakupiony przez Urząd, do którego aktualizacji potrzebne jest połączenie z Internetem, natomiast komputery z programem „Źródło" funkcjonują w wydzielonej sieci, bez takiego połączenia. Dodał, że w sierpniu 2017 roku, z forum dyskusyjnego na platformie „pl.id – platforma szkoleniowa" dowiedział się,

[5] Dz. U. Nr 100, poz. 1024 ze zm. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie dokumentacji i warunków technicznych".

[6] Liczba stanowisk komputerowych i liczba pracowników nie były tożsame. Spośród sześciu osób obsługujących sześć stanowisk komputerowych z zainstalowaną aplikacją „Źródło", cztery osoby posiadały dodatkowe stanowiska komputerowe z aplikacjami biurowymi i z dostępem do otwartego Internetu.

że istnieje możliwość instalacji oprogramowania antywirusowego dostarczonego przez Ministerstwo Cyfryzacji, które aktualizuje się również w sieci SRP. Te oprogramowanie antywirusowe zostało zainstalowane na części komputerów służących do obsługi programu „Źródło".

- We wszystkich jednostkach skonfigurowano wygaszacz ekranu, uruchamiany po upływie 15 minut (powrót do systemu operacyjnego wymagał podania loginu i hasła użytkownika), co było zgodne z regulacjami PB.
- Do wszystkich stacji roboczych była możliwość podłączenia zewnętrznych nośników danych (np. pendrive, CD, DVD).

Nie stwierdzono przypadków wykorzystywania jednego konta użytkownika systemu operacyjnego przez więcej niż jedną osobę. (dowód: akta kontroli str. 55-78, 149)

**1.2.** Urząd wywiązywał się z obowiązku określonego w § 20 ust. 2 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7]. Obowiązek ten był realizowany w trakcie audytów zewnętrznych i w ramach kontroli zarządczej. W okresie objętym kontrolą (od 17 października do 20 listopada 2017 r.) w Urzędzie przeprowadzono sprawdzenie realizacji rekomendacji z zadania audytowego z 2015 roku dotyczącego skanowania i weryfikacji bezpieczeństwa sieci komputerowej Urzędu przy pomocy narzędzi informatycznych pod kątem ochrony danych osobowych zgodnie z rozporządzeniem KRI[8]. Ponadto w 2014 roku przeprowadzono audyt bezpieczeństwa informacji w zakresie przetwarzania danych osobowych, przeprowadzony zgodnie z § 20 rozporządzenia KRI. W przypadku obu audytów zalecone zostały rekomendacje. Skutkowały one:

- zmianą PB i IZSI, dokonaną 31 grudnia 2014 r. w wyniku rekomendacji Audytu z 2014 roku (w treści PB zmieniono załącznik nr 1, w którym określono wartości poszczególnych ryzyk i sposób reakcji na nie oraz dodano załącznik nr 8, w którym ustalono sposób przepływu danych osobowych pomiędzy poszczególnymi systemami; zapisy IZSI uzupełniono o procedurę postępowania z kluczami w budynku Urzędu),
- dodaniem w umowach z firmami zewnętrznymi dotyczących systemów informatycznych, w których przetwarzano dane osobowe, zapisów o postępowaniu z danymi osobowymi powierzonymi przez Administratora Danych Osobowych (dalej „ADO"),
- zaktualizowaniem zakresu czynności kierownika Referatu Organizacyjno-Gospodarczego i informatyków oraz przeglądem zakresów czynności pozostałych pracowników Urzędu,
- zmianą PB i IZSI, dokonana 26 sierpnia 2016 r., w wyniku rekomendacji Audytu z 2015 roku (m.in. w zakresie wyeliminowania nieścisłości i aktualizacji obu dokumentów, w tym określenia zasad postępowania z zewnętrznymi nośnikami danych),
- opracowaniem projektu Polityki Bezpieczeństwa Informacji, którą wprowadzono 12 stycznia 2018 r. (w trakcie niniejszej kontroli),
- określeniem przez kierowników poszczególnych referatów ważności i sposobu zabezpieczenia informacji, w tym zbiorów danych osobowych, przechowywanych w postaci elektronicznej w poszczególnych komórkach,
- ustaleniem procedury testowania UPS,
- wyodrębnieniem pomieszczenia serwerowni z drzwiami zamykanymi na klucz i przeniesieniem informatyka do pomieszczenia sąsiadującego z serwerownią oraz zamontowaniem w serwerowni czujników dymu i ognia podłączonych do instalacji przeciwpożarowej budynku),
- uruchomieniem automatycznych aktualizacji poprawek bezpieczeństwa na wszystkich komputerach,

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

[8] Oba audyty (w 2015 roku i 2017 roku) przeprowadziło konsorcjum osób fizycznych mających uprawnienia audytorów i wykształcenie informatyczne.

- wyeliminowaniem działających w sieci komputerów z systemem operacyjnym Windows XP,
- monitorowaniem oprogramowania pod kątem jego legalności,
- uzyskaniem z Urzędu Marszałkowskiego Województwa Podlaskiego hasła dostępu do routera od strony WAN oraz konfiguracją jego ustawień, co zapewniło możliwość administrowania tą siecią przez Urząd.

Nie została natomiast zrealizowana w pełni rekomendacja dotycząca podjęcia działań w celu monitorowania sieci komputerowej pod kątem używanych urządzeń i pamięci przenośnych. Wprawdzie wprowadzona, w trakcie niniejszej kontroli, Polityka Bezpieczeństwa Informacji z dokumentacją składającą się na System Zarządzania Bezpieczeństwem Informacji (dalej „SZBI") zawiera regulamin korzystania z pamięci zewnętrznych i urządzeń mobilnych, to nadal Urząd nie posiada narzędzi (oprogramowania) do monitorowania sieci w tym zakresie. Brak takiego monitoringu został stwierdzony podczas oględzin i przez biegłego powołanego przez NIK w trakcie niniejszej kontroli, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 55-78, 115-119, 120-136, 137-141 i 519-563)

W zamieszczonej w PB analizie ryzyka w zakresie przetwarzania danych osobowych wskazano 64 ryzyka. W przypadku 62 z nich prawdopodobieństwo wystąpienia zostało określone jako niskie, a w dwóch – jako średnie.

- W przypadku ryzyka dotyczącego identyfikacji i analizy ryzyka w zakresie przetwarzania i ochrony danych osobowych uznano, że sposobem reakcji na ryzyko były regulacje w sprawie kontroli zarządczej, w świetle których Referat Organizacyjno-Gospodarczy Urzędu został zobowiązany do szczegółowej analizy tego ryzyka. Ze sprawozdania Referatu na temat zarządzania ryzykiem w 2016 roku wynika, że realizowano zadania związane z ochroną i przetwarzaniem danych osobowych, w tym w systemach informatycznych. Takie zadanie zostało również ujęte w działaniach na 2017 rok.
- W przypadku ryzyka zapewnienia ciągłości przetwarzania i ochrony danych osobowych uznano, że sposobem reakcji na ryzyko było systematyczne (co najmniej raz w roku na etapie planowania budżetu) zabezpieczanie środków na zakup sprzętu i oprogramowania zapewniającego ciągłości przetwarzania danych osobowych.

(dowód: akta kontroli str. 4-53, 452-454, 455-456)

**1.3.** Z oględzin 32 stanowisk komputerowych obsługiwanych przez 28 pracowników wynika, że posiadali oni uprawnienia użytkownika systemu, nadane przez Informatyka Urzędu. Wszyscy posiadali własny login i hasło. Z wyników analizy 31 pracowników zatrudnianych w latach 2016 – 2017 (w tym jednego pracownika gospodarczego oraz dwóch stażystów zatrudnionych do pomocy technicznej) wynika, że wszyscy pracownicy merytoryczni (28) posiadali upoważnienia do przetwarzania danych osobowych, adekwatne do realizowanych zadań, określonych w zakresach czynności lub wynikających z powołania do organów funkcjonujących czasowo (na przykład zadnia związane z udziałem w Komisji ds. Budżetu Obywatelskiego)[9]. Poddani analizie pracownicy fizyczni i stażyści zatrudnieni w charakterze pomocy technicznej składali zaś oświadczenia zobowiązujące do nieujawniania podczas zatrudnienia oraz po jego ustaniu informacji dotyczących danych osobowych zawartych w zbiorach Urzędu[10]. (dowód: akta kontroli str. 4-53, 363-371, 372-382)

Upoważnienia do przetwarzania danych osobowych wydane 12 osobom, z którymi rozwiązano stosunek pracy, zostały odwołane lub ich ważność wygasła z chwilą rozwiązania stosunku pracy. Konta tych użytkowników w systemach Urzędu zostały zablokowane bezpośrednio po ustaniu stosunku pracy. (dowód: akta kontroli str. 372-382)

**1.4.** W Urzędzie nie prowadzono papierowej wersji rejestru dostępu do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych. Nie był również prowadzony zbiorczy rejestr dostępu do systemu w formie elektronicznej, co omówiono w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

[9] Wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem o zapoznaniu się z zasadami ochrony danych osobowych, obowiązującymi w Urzędzie, stanowił załącznik do PB.

[10] Wzór oświadczenia stanowił załącznik do PB.

Informacje w ograniczonym zakresie były gromadzone przez kontroler domeny (logi dotyczące logowania się użytkowników na poszczególnych komputerach oraz do zasobów sieciowych), przy czym – z uwagi na fabryczne ustawienia (50kB dla poszczególnych stacji roboczych) – logi te obejmowały kilka ostatnich dni. Pozostałe informacje o aktywności użytkowników gromadzone były na poszczególnych stanowiskach użytkowników przez system operacyjny oraz w siedmiu (z dziesięciu) aplikacjach / programach dziedzinowych związanych z przetwarzaniem danych osobowych w rejestrach lub w dziennikach zdarzeń. Pozostałe trzy nie posiadały możliwości technicznych pozwalających na gromadzenie takich danych – były to programy pozwalające jedynie na pogląd danych (w zakresie ewidencji gruntów i budynków) lub obsługiwane przez jedynego pracownika (program do obsługi kasy zapomogowo-pożyczkowej). (dowód: akta kontroli str. 4-53, 115-119, 441-444)

**1.5.** Zgodnie z § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI, zapewniono środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i urządzeń serwerowni, poprzez wymuszenie okresowej zmiany hasła. Sieć WI-FI była odseparowana fizycznie od sieci LAN i ograniczała się do sali konferencyjnej Urzędu. Dostęp do sieci WI-FI zabezpieczony był zmienianym okresowo hasłem, które było udostępniane wybranym osobom. (dowód: akta kontroli str. 115-119)

**1.6**. Regulacje wewnętrzne Urzędu nie dopuszczały możliwości pracy na urządzeniach prywatnych pracowników Urzędu. Konfiguracja sieciowa umożliwiała podłączenie do infrastruktury sieciowej Urzędu urządzeń do niego nie należących (laptopów, telefonów, tabletów itp.). Nie było jednak możliwe korzystanie na tych urządzeniach z zasobów informatycznych Urzędu. Nie został również przewidziany zdalny dostęp do zasobów sieci lokalnej Urzędu, a dostęp do danych osobowych za pomocą laptopów służbowych był możliwy wyłącznie w Urzędzie (zasoby te znajdowały się na serwerach).

(dowód: akta kontroli str. 4-53,115-119)

Regulacje wewnętrzne[11] dotyczące komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych zobowiązywały użytkowników do stosowania procedur przewidzianych dla pracy na komputerach stacjonarnych oraz do bezwzględnego zakazu udostępniania komputerów innym osobom, a także ochrony ich przed uszkodzeniem, kradzieżą i zachowania szczególnej ostrożności podczas transportu.

(dowód: akta kontroli str. 4-53)

**1.7.** W latach 2016 – 2017 (do 28 listopada) wystąpił jeden incydent (15 lipca 2016 r.) wskazujący na możliwość nieautoryzowanego dostępu do zasobów informatycznych. Jeden z pracowników zgłosił ABI i informatykowi naruszenie lub podejrzenie naruszenia bezpieczeństwa systemu informatycznego, polegające na niemożności zalogowania się do stacji roboczej, po powrocie pracownika z urlopu (brak reakcji systemu na hasło użytkownika). ABI dokonał sprawdzenia doraźnego zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. W jego wyniku ustalono, że nastąpiła zmiana hasła na komputerze pracownika (podczas urlopu) przez informatyka, w celu umożliwienia innemu pracownikowi dostępu do wzoru umowy. Z wyjaśnień informatyka złożonych podczas sprawdzenia wynikało, że nie nastąpił dostęp do danych osób trzecich (z komputera pobrano wzór umowy oraz wzór porozumienia z operatorem usług telekomunikacyjnych). Z podjętych działań ABI sporządził notatkę (którą podpisała osoba zgłaszająca zdarzenie) i sprawozdanie ze sprawdzenia doraźnego. Oba dokumenty przekazano ADO. W sprawozdaniu zaznaczono, że obowiązująca w Urzędzie IZSI nie przewiduje procedur na wypadek pozyskania danych z komputera użytkownika podczas jego nieobecności. W związku z tym zaproponował wprowadzenie takiej procedury do IZSI. W nowej IZSI (wprowadzonej 26 sierpnia 2016 r.) procedura taka została dodana[12].

(dowód: akta kontroli str. 262-267)

[11] Określone w § 6 IZSI z sierpnia 2016 roku.

[12] § 5 pkt. 12 IZSI, stanowiącej załącznik nr 2 do zarządzenia Nr 269/16 Burmistrza z dnia 26 sierpnia 2016 r.

**1.8.** Jak opisano w pkt. 1.6. niniejszego wystąpienia pokontrolnego, poza siedzibą Urzędu nie ma możliwości pracy na jego systemach.

**1.9.** We wszystkich trzech umowach dotyczących obsługi serwisowej zakupionego przez Urząd oprogramowania, wykorzystywanego do przetwarzania danych osobowych (FISKUS, ELUD, WYB+, NDM+, WF-GANG) zawarte były zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Było to zgodne z § 20 ust. 2 pkt. 10 rozporządzenia KRI. Przykładowe treści tego rodzaju postanowień do umów zwarto również w PB.

(dowód: akta kontroli str. 82-93)

**1.10**. Ochronę systemów informatycznych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, realizowano poprzez funkcjonowanie stanowisk komputerowych w sieci wewnętrznej, połączonej pośrednio z siecią publiczną (poza stanowiskami komputerowymi przeznaczonymi do obsługi aplikacji „Źródło", przeznaczonej do obsługi Systemu Rejestrów Państwowych, które funkcjonowały w wyodrębnionej sieci – na oddzielnym łączu internetowym i z odrębnym serwerem). Dostęp do sieci publicznej z poszczególnych jednostek sieci wewnętrznej Urzędu był chroniony sprzętowo (firewallem), a na serwerach i stacjach roboczych stosowano oprogramowanie antywirusowe

(dowód: akta kontroli str.4-53, 55-78 i 115-119)

**1.11.** W okresie objętym kontrolą Urząd wykupił usługę dostępu do Internetu, z pakietem hostingowym (strona internetowa, domena internetowa, poczta elektroniczna). W umowie zawarto postanowienia dotyczące powierzenia danych osobowych na platformie hostingowej, w których dostawca usługi zobowiązał się do przechowywania danych zgodnie z umową i ustawą o ochronie danych osobowych oraz zachowania w tajemnicy danych osobowych i informacji dotyczących przechowywania takich danych zarówno w trakcie trwania umowy, jak i po jej ustaniu (§ 9 umowy). Poczta elektroniczna była zlokalizowana na serwerze dostawcy. Dostęp do niej był możliwy za pomocą aplikacji Mozilla Thunderbird. W umowie dostawca zagwarantował podstawowy pakiet bezpieczeństwa sieciowego.

(dowód: akta kontroli str. 55-78, 94-102)

**1.12.** W PB oraz IZSI uregulowano wykonywanie kopii bezpieczeństwa komputerowych zbiorów danych, zasady ich przechowywania i weryfikacji. Procedury w tym zakresie były przestrzegane. W serwerowni znajdowało się dwudyskowe urządzenie do robienia backupów. Kopie bezpieczeństwa baz danych programów wykorzystywanych w Urzędzie oraz folderów sieciowych użytkowników były wykonywane raz dziennie. Zapisywano je na dyskach przenośnych i przechowywano poza serwerownią, w zabezpieczonej szafie.

W okresie objętym kontrolą wystąpił w Urzędzie jeden przypadek konieczności odtworzenia danych z kopii zapasowej. Dotyczyło to awarii serwera z bazą danych programu „Płatnik" po zainstalowaniu najnowszej aktualizacji sytemu. Po wycofaniu aktualizacji baza danych programu „Płatnik" nie nadawała się do użytku. Baza została odtworzona z kopii zapasowej z dnia poprzedniego. (dowód: akta kontroli str. 4-53, 105-106, 115-119, 441-444)

**1.13.** Pracownicy Urzędu dysponowali możliwością ściągania aplikacji i plików wykonalnych. Nie posiadali natomiast uprawnień do instalowania ich na stacjach komputerowych, do których mieli dostęp. Uprawnienia do konfiguracji systemów operacyjnych komputerów działających w sieci LAN posiadał tylko administrator. Informatyk prowadził ewidencję sprzętu komputerowego, w której ujęto m.in. informacje o systemach operacyjnych zainstalowanych na poszczególnych stacjach roboczych.

(dowód: akta kontroli str. 115-119, 150-160)

**1.14.** W Urzędzie, zgodnie z § 20 ust. 2 pkt 12 lit. a rozporządzenia KRI, zadbano o aktualizację systemów operacyjnych oraz aplikacji bezpieczeństwa Były one aktualizowane automatycznie (poza zainstalowanymi na komputerach służących do obsługi systemu Źródło). (dowód: akta kontroli str. 55-78, 115-119)

**1.15.** W Urzędzie nie opracowano odrębnych procedur związanych z płatnościami realizowanymi drogą elektroniczną, poza uprawnieniem części pracowników do wykonywania przelewów drogą elektroniczną. Do dokonywania przelewów wydzielono komputer stacjonarny w Referacie Finansowo-Budżetowym Urzędu, na którym był dostęp

do aplikacji banków, w których Urząd posiadał konta. Po sprawdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym oraz zatwierdzeniu go do wypłaty / przelewu, wyznaczony pracownik sporządzał szablon przelewu, który był zatwierdzany przez uprawnione osoby. (dowód: akta kontroli str. 55-78, 142-148)

Trzy podmioty serwisujące oprogramowanie Urzędu posiadały możliwość zdalnego dostępu do zasobów sieciowych za pomocą aplikacji TeamViewer, niewymagającej autoryzacji od użytkownika. Informatyk wyjaśnił, że usterki i nieprawidłowości w działaniu oprogramowania zgłasza się administratorowi systemu, który – jeśli problemu nie rozwiąże sam – kontaktuje się z podmiotem serwisującym oprogramowanie i ustala sposób usunięcia usterki. Jeśli w tym celu konieczne jest połączenie zdalne, administrator systemu uruchamia oprogramowanie wskazane przez podmiot serwisujący i nadzoruje czynności wykonywane przez ten podmiot. Problem ten przedstawiono poniżej, w sekcji „Ustalone nieprawidłowości. (dowód: akta kontroli str. 115-119, 441-444)

Ustalone nieprawidłowości

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

1. Nie rejestrowano elektronicznie (w sposób zbiorczy) wszystkich działań użytkowników systemów. Rejestrowano logowania poszczególnych użytkowników do stacji roboczych i do zasobów sieciowych, lecz informacje na ten temat przechowywano tylko przez kilka dni. Nie było m.in. możliwość rejestracji korzystania przez użytkowników z pamięci zewnętrznych. Informatyk Urzędu wyjaśnił, że informacje o logowaniu użytkowników do systemów operacyjnych oraz o dostępie użytkowników do zasobów sieciowych były zapisywane w logach serwera SAMBA w ograniczonym zakresie – wielkość pliku z logiem dla pojedynczego użytkownika była ograniczona do 50 kB. Informacje takie, jak dziennik podłączeń urządzeń przenośnych USB, z uwagi na brak poważniejszych incydentów w przeszłości, nie były gromadzone i weryfikowane.
2. Trzy podmioty serwisujące oprogramowanie Urzędu posiadały możliwość zdalnego dostępu do zasobów sieciowych za pomocą aplikacji TeamViewer, niewymagającej autoryzacji od podmiotu serwisującego (połączenie realizowano na konto użytkownika lub administratora Urzędu). Taki sposób uniemożliwia zidentyfikowanie działań podmiotu serwisującego w administrowanych systemach, mimo zapewnienia nadzoru ze strony informatyka nad czynnościami wykonywanymi przez ten podmiot.

Zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji jest – stosownie do § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI – jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

(dowód: akta kontroli str. 55-78, 115-119, 441-444)

**Ocena cząstkowa**

NIK ocenia pozytywnie mimo stwierdzonych nieprawidłowości skuteczność przyjętych rozwiązań dotyczących zabezpieczenia dostępu do poszczególnych systemów informatycznych i usług sieciowych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem danych.

### 2. Dokumentacja i procedury dotyczące ochrony danych

Opis stanu faktycznego

**2.1.** Według stanu na 28 listopada 2017 r., Urząd od 27 listopada 1999 r. do 4 marca 2015 r. zgłosił GIODO do zarejestrowania 21 zbiorów danych, z których 17 zostało zarejestrowanych. Po powołaniu ABI (w czerwcu 2015 roku i zgłoszeniu tego faktu GIODO) Urząd nie dokonywał rejestracji kolejnych zbiorów danych osobowych. Żaden ze zbiorów danych zgłoszonych GIODO nie był aktualizowany ani wykreślany.

(dowód: akta kontroli str. 161, 162-181, 474-518)

W Urzędzie, wg. stanu na 28 listopada 2017 r., wykazywano prowadzenie 33 zbiorów danych osobowych. Wykaz tych zbiorów i zakres danych osobowych w nich przetwarzanych został ujęty w PB i w jawnym rejestrze zbiorów danych osobowych przetwarzanych w Urzędzie. Analiza zbiorów danych zgłoszonych do GIODO oraz zbiorów danych ujętych w PB i rejestrze wskazała, że: [1] do GIODO zgłoszono zbiory danych nieujęte w wykazach PB i rejestrze; [2] zakres danych w zbiorach zgłoszonych do GIODO różnił się od zakresu

tych zbiorów zawartych w wykazach PB i rejestrze, co szerzej omówiono w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 4-53, 161, 162-181, 184-190, 191-226, 474-518)

Z działań podjętych przez ABI w okresie objętym kontrolą wynika, że w Urzędzie może funkcjonować więcej zbiorów danych osobowych, niż zostało ujętych w wykazach zawartych w PB i w wymienionym wyżej rejestrze prowadzonym przez ABI.

ABI w planie sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych na 2016 rok założył bowiem m.in. aktualizację wykazu zbiorów danych osobowych poprzez sprawdzenie istniejących i identyfikację nowych zbiorów danych. Realizację tego zadania ustalono na okres od 16 sierpnia do 31 października 2016 r. Faktyczna realizacja tego zadania przez ABI została rozpoczęta w marcu 2017 roku i do dnia rozpoczęcie kontroli NIK (tj. 28 listopada 2017 r.) nie została zakończona. W marcu 2017 roku ABI wystąpił do kierowników poszczególnych referatów Urzędu o informacje o faktycznie przetwarzanych zbiorach danych w odniesieniu do wykazów zawartych w PB[13], rodzaju przetwarzanych danych osobowych, formie i podstawach prawnych przetwarzania oraz o lokalizacji zbiorów i miejscach ich przetwarzania.

Z uzyskanych od 9 marca do 13 czerwca 2017 r. przez ABI informacji wynika m.in., że:

- wystąpiły przypadki rozbieżności pomiędzy danymi faktycznie przetwarzanymi a zakresem określonym w zbiorach danych ujętych w PB i w rejestrze (odnosiło się to głównie do zbiorów danych dotyczących spraw obronności i kwalifikacji wojskowej, sprzedaży lokali komunalnych, naboru pracowników, rejestru mieszkańców i rejestru zamieszkania cudzoziemców),
- kierownicy referatów zgłosili propozycje ujęcia w PB 43 nowych zbiorów danych osobowych, w tym ewidencję zbiorników bezodpływowych, rejestry wniosków o: Kartę Dużej Rodziny, awans zawodowy nauczycieli, stypendia udzielane przez samorząd Miasta, wypoczynek dzieci w kraju i za granicą.

Do dnia rozpoczęcia kontroli NIK nie dokonano uzupełnienia i weryfikacji zbiorów danych osobowych znajdujących się w Urzędzie w oparciu o uzyskane informacje.

(dowód: akta kontroli str. 184-190, 227-228, 229-256)

ABI wyjaśnił, że ze względu na obowiązki służbowe związane z pracą w Referacie Inwestycji i Zamówień Publicznych (konieczność rozliczenia do końca 2016 roku inwestycji dofinansowywanej ze środków krajowych oraz przygotowywanie wniosków aplikacyjnych w związku z naborami do końca 2016 roku i końca lutego 2017 roku) rozpoczęcie sprawdzenia było możliwe w marcu 2017 roku. Po otrzymaniu informacji z referatów Urzędu okazało się, że konieczne jest doprecyzowanie części informacji, związanych z danymi osobowymi przetwarzanymi na poszczególnych stanowiskach. Sprawdzenie zostanie zakończone w możliwie najszybszym czasie. (dowód: akta kontroli str.437-440)

**2.2.** ADO w Urzędzie był Burmistrz Bielska Podlaskiego. W okresie objętym kontrolą ABI, o którym mowa w art. 36a ust. 1 ustawy o ochronie danych osobowych, był inspektor zatrudniony w Urzędzie. Powołany został on przez ADO 29 czerwca 2015 r.[14] Fakt ten, zgodnie z art. 46b ust. 1 i 2 powołanej ustawy[15], został następnego dnia zgłoszony do rejestracji GIODO, na wymaganym formularzu i w zakresie wymaganych danych.

(dowód: akta kontroli str. 110-112)

**2.3.** Zadania ABI, wynikające z art. 36a ust. 2 ustawy o ochronie danych, zostały określone w PB, w tym: sprawowanie nadzoru nad przestrzeganiem zasad przetwarzania i ochrony danych osobowych w imieniu i na rzecz ADO, w szczególności poprzez:

- prowadzenie i aktualizację PB i IZSI, tj. dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych (w przypadku PB przegląd pod względem jej aktualności i stosowalności powinien być przeprowadzony nie rzadziej niż raz w roku,

[13] Określających: nazwę zbioru, program zastosowany do przetwarzania / formę zbioru, jego lokalizację, miejsce przetwarzania i jego strukturę.

[14] Poprzednio ABI (od 2007 roku) był informatyk Urzędu.

[15] Data wysłania zgłoszenia: 30 czerwca 2015 r.

a PB powinna podlegać aktualizacji m.in. każdorazowo w przypadku likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru),

- nadzorowanie i przestrzeganie zasad określonych w PB i IZSI,
- szkolenie osób dopuszczonych do przetwarzania danych osobowych,
- nadzorowanie udostępniania danych osobowych odbiorcom tych danych,
- nadzorowanie zamieszczania zapisów dotyczących ochrony danych osobowych w umowach z użytkownikami upoważnionymi do przetwarzania danych osobowych lub konserwacji urządzeń, oprogramowania,
- nadzorowanie wdrożenia adekwatnych do zagrożeń środków fizycznych, a także organizacyjnych i technicznych służących zapewnieniu bezpieczeństwa,
- nadzorowanie obiegu oraz przechowywania dokumentów zawierających dane osobowe w zakresie związanym z bezpieczeństwem tych danych,
- przeprowadzanie sprawdzeń wynikających z ustawy o ochronie danych osobowych oraz prowadzenie szczegółowej dokumentacji z kontroli dotyczących: przestrzegania przepisów o ochronie danych osobowych, stwierdzonych naruszeń bezpieczeństwa danych osobowych,
- podejmowanie lub wnioskowania o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego.

(dowód: akta kontroli str. 4-53)

W okresie objętym kontrolą ABI w ograniczonym zakresie realizował nałożone obowiązki, m.in.:

- rozpoczął planowane sprawdzenie z zakresu przestrzegania zasad ochrony danych osobowych dotyczących aktualizacji wykazu zbiorów danych osobowych, które nie zostało zakończone,
- nie dokonał zaplanowanych na 2016 rok sprawdzeń realizacji procedur wdrożonych przez ADO w zakresie ochrony danych osobowych dotyczących sprawdzenia czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia, czy odwołano upoważnienia osób, które nie powinny mieć już prawa dostępu do danych osobowych oraz ewidencji wydanych upoważnień,
- podjął działania w związku z możliwością wystąpienia nieautoryzowanego dostępu do zasobów informatycznych zgłoszoną przez pracownika Urzędu,
- przedłożył (w grudniu 2015 roku) ADO uaktualnienie polityki bezpieczeństwa, będące wynikiem realizacji zaleceń / rekomendacji audytu wewnętrznego prowadzonego w 2015 roku w Urzędzie,
- przeprowadzał szkolenia osób, którym w okresie objętym kontrolą wydawano upoważnienia do dostępu do danych osobowych,
- prowadził rejestr zbiorów danych, o którym mowa w art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych, zawierający wykaz – 33 ujętych w PB – zbiorów danych osobowych przetwarzanych w Urzędzie,
- uczestniczył w opracowaniu projektu Polityki Bezpieczeństwa Informacji.

Nierealizowanie przez ABI części obowiązków szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności”

(dowód: akta kontroli str. 137-141, 227-228 229-256, 268-286, 372-382, 457-461)

**2.4.** W Urzędzie, w myśl przepisu art. 39 ust. 1 ustawy o ochronie danych osobowych, prowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych. Zawierała ona elementy określone w art. 39 ust 1 pkt 1-3 powołanej ustawy, tj.: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych i identyfikator. Według stanu na 28 listopada 2017 r. w ewidencji osób upoważnionych ujęto upoważnienia dotyczące dostępu do systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie i do pozostałych zasobów zawierających dane osobowe.

Analiza zakresów obowiązków 28 pracowników merytorycznych Urzędu i wydanych przez Burmistrza upoważnień do przetwarzania danych osobowych wykazała, że pracownicy mieli upoważnienia do przetwarzania danych osobowych, zgodne z zakresem ich czynności, co omówiono szerzej w pkt. 1.3. niniejszego wystąpienia pokontrolnego. Upoważnienia tych pracowników były ujęte w ewidencji osób upoważnionych do przetwarzania danych osobowych. (dowód: akta kontroli str. 372-382, 383-385)

Burmistrz posiadał imienne upoważnienie do przetwarzania danych w Systemie Rejestrów Państwowych, wydane w 2014 roku przez Ministra Spraw Wewnętrznych i Administracji. Na podstawie tego upoważnienia Burmistrz udzielił upoważnień pracownikom do przetwarzania danych w Systemie Rejestrów Państwowych korzystających z aplikacji „Źródło" oraz informatykowi Urzędu. (dowód: akta kontroli str. 303, 372-382, 386-391)

**2.5**. W Urzędzie do 28 listopada 2017 r. prowadzono aktualizacje wewnętrznych aktów prawnych, procedur, instrukcji lub poleceń dotyczących sposobu gromadzenia i przetwarzania zasobów informacyjnych. PB i IZSI wprowadzono w Urzędzie w 2011 roku[16]. Od momentu przyjęcia tych dokumentów były one przedmiotem aktualizacji, które wynikały głównie z zaleceń / rekomendacji przedstawionych przez audytorów zewnętrznych w latach 2014 i 2015 oraz kontroli NIK z 2016 roku. Aktualizacje PB i IZSI miały miejsce w grudniu 2014 roku i w sierpniu 2016 roku, co omówiono w pkt. 1.2. i 2.9. niniejszego wystąpienia pokontrolnego.

Ponadto w związku z zaleceniami / rekomendacjami audytu w Urzędzie trwały prace nad Polityką Bezpieczeństwa Informacji. Urząd dysponował na dzień rozpoczęcia niniejszej kontroli (28 listopada 2018 r.) projektem Polityki Bezpieczeństwa Informacji, na którą miały się składać: [1] Polityka bezpieczeństwa danych osobowych, [2] Instrukcja zarządzania systemem informatycznym, [3] Procedura nadawania, zarządzania i użytkowania uprawnieniami do systemów informatycznych, [4] Procedura oceny i zarządzania ryzykiem w obszarze ochrony informacji, [5] Ogólne zasady związane z zapewnieniem bezpieczeństwa informacji przy wykonywaniu obowiązków służbowych, [6] Procedura postępowania z kluczami i alarmami, [7] Standard stacji roboczej, [8] Procedura testowania i wymiany akumulatorów w urządzeniach UPS, [9] Regulamin korzystania z pamięci zewnętrznych i urządzeń mobilnych.
(dowód: akta kontroli str. 4-53, 120-136, 137-141, 316-362, 457-461,519-563)

**2.6.** Administrowanie systemami informatycznymi powierzono informatykowi zatrudnionemu w Urzędzie na umowę o pracę. Do czerwca 2015 roku osoba ta pełniła również obowiązki ABI (bez zgłoszenia do GIODO). Zakres zadań informatyka, jako administratora systemów informatycznych, wynikał z zakresu czynności i regulacji zwartych w PB, w której wskazano, że informatyk to osoba odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych w Urzędzie, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach. Do jego obowiązków należało też m.in. zarządzanie i bieżący nadzór nad systemem informatycznym. Informatyk dysponował stosownymi upoważnieniami ADO do przetwarzania danych osobowych. (dowód: akta kontroli str. 4-53, 294-307)

**2.7.** Prowadzenie w Urzędzie audytów z zakresu bezpieczeństwa informacji oraz ich wykorzystanie omówiono w pkt 1 niniejszego wystąpienia pokontrolnego.

**2.8.** W latach 2016 – 2017 (do 28 listopada) ABI uczestniczył w trzech szkoleniach zewnętrznych związanych z ochroną danych osobowych, w tym dwóch dotyczących nowych zadań ABI i ADO w związku ze zmianami ustawy o ochronie danych osobowych. Jednorazowo w tym okresie w takich szkoleniach uczestniczyli: Sekretarz Miasta, informatyk oraz kierownik Referatu Zarządzania Kryzysowego. Wcześniej, w 2015 roku ABI był na dwóch zewnętrznych szkoleniach dotyczących nowelizacji ustawy o ochronie danych oraz nowych zadań ABI, a informatyk Urzędu był na jednym szkoleniu zewnętrznym

[16] Zarządzeniem Nr 98/11 Burmistrza z 21 czerwca 2011 r. w sprawie wprowadzenia w życie „Polityki bezpieczeństwa danych osobowych w Urzędzie Miasta Bielsk Podlaski" oraz w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Bielsk Podlaski". Dokumenty te zastąpiły Instrukcję o ochronie danych osobowych i Instrukcję bezpieczeństwa danych z 5 marca 2007 r.

dotyczącym nowych zadań ABI. Pozostali pracownicy Urzędu w okresie objętym kontrolą nie byli szkoleni w zakresie ochrony danych osobowych, poza szkoleniami indywidualnymi prowadzonymi przez ABI w związku z nadaniem pracownikom nowych upoważnień do przetwarzania danych osobowych[17]. Wcześniej (w 2015 roku) 30 pracowników Urzędu uczestniczyło w szkoleniu zewnętrznym w zakresie dokumentów elektronicznych w administracji, co było związane z wdrażaniem w Urzędzie systemu EDZ. Niezapewnienie szkoleń dla pozostałej części pracowników z zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 372-382, 394-436)

**2.9.** Od 1 stycznia 2016 r. do 28 listopada 2017 r. jedyną kontrolą dotyczącą bezpieczeństwa danych osobowych była kontrola NIK (wystąpienie pokontrolne z 14 lipca 2016 r.) dotycząca Systemów Rejestrów Państwowych – bezpieczeństwo, funkcjonowanie i użyteczność, w wyniku której oceniono prawidłowo realizację zadań z wykorzystaniem Systemu Rejestrów Państwowych[18]. W wyniku kontroli wnioskowano o opracowanie i wdrożenie całościowego systemu zarządzania bezpieczeństwem informacji oraz uaktualnienie PB i IZSI. W odpowiedzi Burmistrz wskazał, że zostały przygotowane uaktualnienia PB i IZSI oraz, że trwają pracę nad Systemem Zarządzania Bezpieczeństwem Informacji (SZBI). Z ustaleń obecnej kontroli wynika, że PB i IZSI zostały uaktualnione w sierpniu 2016 roku, a Urząd dysponował projektami dokumentów składającymi się na SZBI, które podczas niniejszej kontroli zostały wprowadzone[19]. W ww. okresie nie wpłynęły do Urzędu skargi dotyczące przypadków związanych z ujawnieniem danych osobowych lub naruszeniem przepisów związanych z ich ochroną.

(dowód: akta kontroli str. 4-53, 54, 392, 519-563)

**2.10.** Jak wspominano w pkt. 2.5., dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania tych danych wdrożono w 2011 roku. Ostatnia aktualizacja tej dokumentacji nastąpiła w sierpniu 2016 roku. PB zawierała elementy określone w § 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, tj.:

- wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie – z przeprowadzonych oględzin pomieszczeń oraz lokalizacji 32 stanowisk komputerowych wynika, że lokalizacja zakresu przetwarzanych danych w poszczególnych pomieszczenia była zgodna z tym wykazem,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania – wykaz ten nie obejmował wszystkich zbiorów danych funkcjonujących w Urzędzie, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości",
- opis struktury przetwarzanych zbiorów danych osobowych – zakres tych zbiorów nie był w pełni zgodny z zakresem zbiorów wskazanym GIODO lub ich obecną strukturą, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości",
- sposób przepływu danych pomiędzy poszczególnymi systemami Urzędu,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

PB zawierała również: [1] analizę ryzyka i sposoby ich ograniczenia w zakresie przetwarzania danych osobowych; [2] przykładową treść zapisów w umowach z użytkownikami upoważnionymi do przetwarzania danych osobowych, firmami, którym powierzono przetwarzanie danych osobowych lub konserwacje urządzeń służących do przetwarzania danych oraz pracownikami tych firm; [3] wzór upoważnienia do przetwarzania danych osobowych wraz ze wzorem oświadczenia w sprawie

[17] W okresie objętym kontrolą, a szczególnie w 2016 roku, większości pracowników Urzędu nadano uprawnienia do przetwarzania danych osobowych w związku z dostępem do EZD – przetwarzania danych w rejestrze kontrahentów.

[18] Kontrola P/16/006 nr. LBI.410.014.01.2016.

[19] Zarządzeniem Nr 482/18 Burmistrza Miasta Bielsk Podlaski z dnia 12 stycznia 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji dla Urzędu Miasta Bielsk Podlaski.

przeszkolenia przed przystąpieniem do przetwarzania danych oraz oświadczeniem w sprawie zapoznania się i zrozumienia zasad dotyczących ochrony danych osobowych zawartych w PB i IZSI; [4] wzór oświadczenia o zachowaniu w poufności danych przez inne osoby zatrudnione w Urzędzie (personel sprzątający, pomoc techniczna).

(dowód: akta kontroli str. 4-53)

IZSI zawierała elementy określone w § 5 rozporządzenia w sprawie dokumentacji i warunków technicznych, w tym: [1] procedurę nadawania, zarządzania i użytkowania uprawnień do przetwarzania danych osobowych, stosowane metody i środki uwierzytelniania oraz związane z ich zarządzaniem i użytkowaniem; [2] procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego; [3] procedury tworzenia, przechowywania i niszczenia kopii zapasowych; [4] procedury używania, przechowywania i niszczenia elektronicznych nośników informacji zawierających dane osobowe; [5] sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego; [6] procedury wykonywania przeglądów, konserwacji i naprawy systemów oraz elektronicznych nośników informacji służących do przetwarzania danych.

Ponadto IZSI zawierała: procedurę postępowania z kluczami do pomieszczeń w budynku Urzędu, kontrolę nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych, procedurę postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego. (dowód: akta kontroli str. 4-53)

W IZSI określono (zgodnie z § 6 ust. 4 rozporządzenia w sprawie dokumentacji i warunków technicznych) wymóg stosowania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych, z uwagi na dostęp urządzeń informatycznych Urzędu do sieci publicznej. W związku z tym wyodrębniono również w Urzędzie dwie strefy bezpieczeństwa i sposoby ich zabezpieczenia oraz dostępu do nich. (dowód: akta kontroli str. 4-53)

Ustalone nieprawidłowości

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

1. Wykazy zbiorów danych, stanowiące element PB z sierpnia 2016 roku i rejestru zbiorów danych, były prowadzone w sposób nierzetelny. Nie ujęto w nich bowiem informacji o pięciu zbiorach danych osobowych prowadzonych w Urzędzie, które zostały zgłoszone do GIODO. Dotyczyło to zbiorów danych osobowych: Skargi, Rejestry korespondencji przychodzącej i wychodzącej, Oświadczenia majątkowe radnych Rady Miasta, Oświadczenia majątkowe lub inne oświadczenia osób zatrudnionych. Ponadto zakresy danych gromadzonych w pięciu zbiorach zgłoszonych do GIODO różniły się od zakresu danych wykazywanych w PB i w rejestrze zbiorów danych. Dotyczyło to: Ewidencji Ludności i Dowodów Osobistych; wykazów i rejestrów przedpoborowych, poborowych oraz formacji obrony cywilnej i osób zobowiązanych do świadczeń na rzecz obrony; rejestru wniosków o leczenie odwykowe; dodatków mieszkaniowych; opłat adiacenckich. Zakres danych zgłoszonych do GIODO był w przypadku tych zbiorów szerszy niż ujęty w wykazach zbiorów PB i w rejestrze zbiorów danych (na przykład w przypadku Ewidencji Ludności i Dowodów Osobistych do GIODO zgłoszono dodatkowo: miejsce pracy, zawód, wykształcenie, serię i nr dowodu osobistego).

   (dowód: akta kontroli str. 4-53, 161, 162-181, 191-226, 474-518)

   ABI wyjaśnił, że do różnic i rozbieżności wymienionych wyżej doszło w wyniku przeoczenia. W związku z występującymi różnicami pomiędzy zbiorami danych osobowych zawartymi w PB a zgłoszonymi przez Urząd do GIODO, podjęte zostaną kroki w celu zlikwidowania ww. różnic. Niezwłocznie zostaną podjęte również działania w celu zlikwidowania rozbieżności, które występują w strukturach poszczególnych zbiorów danych osobowych zgłoszonych do GIODO i w strukturach zbiorów zamieszczonych w PB (dowód: akta kontroli str. 437-440)

   Podobnej treści wyjaśnienia złożył ADO. (dowód: akta kontroli str. 445-446)

2. W okresie objętym kontrolą nie organizowano grupowych szkoleń dla pracowników Urzędu w zakresie bezpieczeństwa informacji, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI, mimo że w sierpniu 2016 roku zaktualizowana została PB i IZSI.

   ABI wyjaśnił, że każda osoba, która ma zostać upoważniona do przetwarzania danych osobowych jest zapoznawana z zasadami opisanymi w PB i IZSI. W latach 2015 – 2017 nie prowadzono odrębnych wewnętrznych szkoleń dla grup pracowników Urzędu. Wymienione wyżej działania wydawały się wystarczające, aby pracownicy mieli świadomość jak postępować z danymi osobowymi, z którymi mają styczność. W świetle zbliżającego się wejścia w życie (25 maja 2018 r.) nowego rozporządzenia dotyczącego ochrony danych osobowych, konieczne będzie przeprowadzenie w bieżącym roku szkolenia pracowników pod tym kątem. (dowód: akta kontroli str. 372-382, 394-436, 466)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że do dnia rozpoczęcia kontroli NIK nie zostało zakończone rozpoczęte przez ABI w marcu 2017 roku sprawdzenie w zakresie aktualizacji wykazu zbiorów danych osobowych, chociaż na jego realizację założono trzy miesiące a przedłożone przez referaty merytoryczne uwagi do wykazanych w PB zbiorów i zgłoszone potencjalne nowe zbiorów danych osobowych mogą w istotnych sposób zmienić informacje na temat przetwarzanych w Urzędzie zbiorów danych osobowych. Podobnie nie zostało zrealizowane sprawdzenie dotyczące wydawania, odwoływania i ewidencjonowania upoważnień do przetwarzania danych osobowych. ABI wyjaśnił, że przeprowadzenie sprawdzenia upoważnień do przetwarzania danych osobowych pracownikom Urzędu związane jest z weryfikacją aktualności zbiorów danych osobowych i nie zostało jeszcze zakończone. Sprawdzenie zostanie zakończone w możliwie najkrótszym czasie, a sprawozdanie ze sprawdzenia przestawione zostanie ADO. (dowód: akta kontroli str. 465)

**Ocena cząstkowa**

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości opracowanie oraz wdrożenie dokumentacji i procedur wymaganych przepisami ustawy o ochronie danych osobowych.

### 3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

**3.1**. Z wykazywanych przez Urząd (w PB i rejestrze zbiorów danych) 33 zbiorów danych osobowych, 17 prowadzono z wykorzystaniem systemów elektronicznych, a pozostałe papierowo. IZSI ustalała dla Urzędu wysoki poziom bezpieczeństwa. Wyodrębniono w niej dwie strefy bezpieczeństwa. Pierwsza obejmowała serwerownię, kasę, pomieszczenia przetwarzania danych o ewidencji ludności i ewidencji dowodów osobistych oraz pomieszczenia, w których przechowywano kopie zapasowe elektronicznych zbiorów danych. Druga zaś obejmowała pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych, ujęte w wykazie budynków i pomieszczeń tworzących obszar, w którym przetwarzano dane osobowe. Dla obu stref określono zabezpieczenia fizyczne i organizacyjne, m.in.: w strefie pierwszej ochrona pomieszczeń systemem antywłamaniowym, zakratowane okna, dostęp do pomieszczeń dla osób upoważnionych do przetwarzania danych. Osoby trzecie mogły przebywać w tych pomieszczeniach tylko w obecności osób mających tam stałe miejsce pracy. W procedurze postępowania z kluczami do pomieszczeń Urzędu ustalono m.in., że pobieranie i zdawanie kluczy odbywa się w biurze podawczym. Wydawane są one wyłączenie pracownikom wykonującym zadania w danych pomieszczeniach, a wydanie i zwrot kluczy odnotowuje się w rejestrze. Pracownicy przetwarzający dane osobowe zobowiązani byli po zakończeniu pracy do chowania akt, dokumentów i wydruków zawierających dane osobowe w zamykanych na klucz szafach oraz do niszczenia niepotrzebnych dokumentów w sposób uniemożliwiający ich odtworzenie (np. w niszczarce). W PB ujęto regulacje minimalizujące ryzyko utraty danych przetwarzanych w Urzędzie: na rzecz osób trzecich mających dostęp do tych danych (serwisantów, usługodawców), poprzez wprowadzenie do umów zapisów o powierzeniu przetwarzania danych osobowych oraz na rzecz innych osób nieuprawnionych (konserwatorzy, osoby sprzątające), poprzez zobowiązanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

(dowód: akta kontroli str. 4-53, 107-109)

Oględziny pomieszczeń, w których przetwarzane były zbiory danych osobowych wykazały, że zgodnie z postanowieniami PB: [1] przetwarzanie danych odbywało się w miejscach do tego wyznaczonych; [2] w Urzędzie zainstalowano monitoring wizyjny wejść do budynku oraz system alarmowy i przeciwpożarowy; [3] dane sensytywne (określone w art. 27 ustawy o ochronie danych osobowych) przechowywane były w zamykanych szafach; [4] pomieszczenia I strefy bezpieczeństwa były okratowane; [5] pomieszczenie serwerowni posiadało zabezpieczenia w postaci: systemu alarmowego, systemu przeciwpożarowego, systemu klimatyzacji, przy czym drzwi do tego pomieszczenia (z korytarza i z pokoju informatyka) były drzwiami standardowymi takimi, jak pozostałe drzwi do pomieszczeń Urzędu (poza archiwum zakładowym, które było zabezpieczone drzwiami ognioodpornymi oraz wyposażone w czujki systemu alarmowego i przeciwpożarowego, z kratami w oknach). (dowód: akta kontroli str. 105-106)

Kopie zapasowe baz danych, zgodnie z postanowieniami § 7 ust. 5 IZSI, znajdowały się w szafie pancernej w innym pomieszczeniu, niż to, w którym umiejscowiono urządzenia z danymi podlegającymi procesowi tworzenia kopii. (dowód: akta kontroli str. 105-106)

**3.2.** W Urzędzie gromadzono na bieżąco dane, o których mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI. Oprócz ewidencji środków trwałych prowadzonych przez Referat Finansowo-Budżetowy, ewidencję oprogramowania, sprzętu i urządzeń prowadził informatyk. (dowód: akta kontroli str. 150-160)

**3.3.** W latach 2016 – 2017 (do 28 listopada) w Urzędzie przeprowadzono jedną likwidację sprzętu komputerowego, w tym 43 dysków twardych. Likwidację przeprowadziła firma zajmująca się likwidacją tego rodzaju urządzeń. Wydała ona potwierdzenie fizycznej likwidacji dysków twardych. (dowód: akta kontroli str. 447-450)

**3.4.** Niszczenie niepotrzebnych dokumentów / wydruków zawierających dane osobowe prowadzono w niszczarkach, które znajdowały się w pomieszczeniach do przetwarzania danych osobowych. Regulację w tym zakresie zawarto w IZSI.
(dowód: akta kontroli str. 4-53)

**3.5.** W § 6 ust. 14 IZSI określono, że osoby użytkujące komputery przenośne, które są wykorzystywane do przetwarzania danych osobowych, zobowiązane są do przestrzegania procedur pracy takich, jakie obowiązują na stacjach roboczych. Ponadto obowiązywał zakaz używania tych komputerów przez inne osoby oraz obowiązek ochrony ich przed uszkodzeniem i kradzieżą. Z przeprowadzonych oględzin trzech (z 10) wykorzystywanych przez pracowników laptopów wynika, że były one wykorzystywane w siedzibie Urzędu. Nie było możliwości dostępu do zasobów sieciowych Urzędu poza jego siedzibą. (dowód: akta kontroli str. 55-78, 115-119, 149, 150-160)

**3.6.** Sprzątanie pomieszczeń zostało uregulowane w IZSI. W pierwszej strefie bezpieczeństwa przetwarzania danych osobowych (określonej w IZSI) sprzątanie pomieszczeń mogło się odbywać podczas obecności osób pracujących w tych pomieszczeniach, a w strefie drugiej sprzątanie odbywało się po godzinach pracy, przez obsługę upoważnioną do przebywania w tych pomieszczeniach. Pracownicy sprzątający złożyli oświadczenia, o których mowa w pkt. 1.3. niniejszego wystąpienia pokontrolnego.
(dowód: akta kontroli str. 4-53)

**3.7.** Procedury dotyczące przeglądów i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych osobowych, zostały określone w § 11 IZSI. Określono w nich m.in., że informatyk dokonuje doraźnych przeglądów i konserwacji oraz drobnych napraw i zmian systemu informatycznego oraz serwerów i stacji roboczych. Pozostałe konserwacje przeglądy i naprawy są dokonywane przez serwisanta lub podmioty zewnętrzne, pod nadzorem informatyka. Nie określono częstotliwości tych przeglądów i konserwacji. (dowód: akta kontroli str. 4-53)

**3.8.** W Urzędzie nie opracowano procedur na wypadek wystąpienia sytuacji nadzwyczajnych, w tym długotrwałego braku zasilania, dotyczących przywracania systemów po awarii oraz planu ciągłości działania, umożliwiającego kontynuację wykonywania zadań publicznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". Możliwość podtrzymania

pracy serwerowni wynosiła ok 25 minut. Urząd posiadał od 2016 roku agregat prądotwórczy umożliwiający zasilenie całego budynku, jednak nie było regulacji w zakresie konieczności uruchomienia awaryjnego zasilania. (dowód: akta kontroli str. 105-106, 393)

Burmistrz wyjaśnił, że system reakcji na działania nadzwyczajne nie został formalnie stworzony z następujących przyczyn:

1. Na podstawie wcześniejszych doświadczeń dotyczących braku zasilania stwierdzono, że brak sygnalizowania awarii zasilania w nocy nie zagraża bezpieczeństwu informacji. Po wyłączeniu serwerów nie następuje utrata danych zapisanych na serwerach. Dodatkowo systematycznie wykonywane są kopie zapasowe, które są przechowywane w oddzielnym pomieszczeniu, w szafie metalowej. Od czasu zakończenia remontu budynku w 2013 roku takie zdarzenia nie miały miejsca. Zaplanowano środki na zakup w 2018 roku serwera do przechowywania kopii zapasowych.
2. W Urzędzie zatrudniony jest konserwator posiadający świadectwo kwalifikacyjne do wykonywania prac w zakresie obsługi, konserwacji urządzeń, instalacji i sieci elektrycznych do 1kV.
3. Jeśli awaria zasilania nastąpi w godzinach pracy Urzędu, osoby odpowiadające za zapewnienie ciągłości pracy podejmują odpowiednie działania. Jeśli awaria dotyczy instalacji elektrycznej w budynku Urzędu, konserwator podejmuje odpowiednie kroki w celu wyeliminowania usterki. Jeśli awaria wynikła z przyczyn dostawcy energii, to – na podstawie informacji uzyskanych od dostawcy energii o długotrwałości przerw zasilania – burmistrz lub zastępca podejmują decyzję o wykorzystaniu przenośnego agregatu prądotwórczego do zasilania budynku. Do obsługi agregatu są wyznaczeni przeszkoleni pracownicy posiadających odpowiednie upoważnienia Burmistrza. Do tej pory takie zdarzenia nie miały miejsca.
4. W bieżącym roku upływa termin obowiązywania umowy na świadczenie usług telekomunikacyjnych. W ramach postępowania na wyłonienie nowego dostawcy planuje się uwzględnić zapewnienie możliwości dodatkowego źródła Internetu.
5. Na wypadek nieprzewidzianych sytuacji dodatkowo w szafie metalowej przechowywane są loginy i hasła administratora do systemów teleinformatycznych wykorzystywanych w Urzędzie.
6. Na wypadek pożaru w pomieszczeniach budynku Urzędu umieszczone są czujniki ognia i dymu mające bezpośrednie połączenie z systemem monitoringu firmy zewnętrznej.
7. Z przepisów zewnętrznych nie wynika wprost posiadanie procedur dotyczących przywracania systemów po awarii oraz planu ciągłości działania. Dotychczasowe regulacje i przedsięwzięte środki ochrony wystarczały do zapewnienia ciągłości pracy Urzędu. (dowód: akta kontroli str. 467-469)

**3.9.** W IZSI przewidziano (§ 7 ust. 4) testowanie przez informatyka wybranej kopii danych. Informatyk wyjaśnił, że sprawdzenie przydatności kopii danych odbywa się raz w miesiącu. Poza koniecznością odtworzenia danych do Płatnika, co omówiono w pkt. 1.12. niniejszego wystąpienia pokontrolnego, w Urzędzie nie wystąpił inny przypadek utraty danych.
(dowód: akta kontroli str. 4-53, 441-444)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

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

**Ocena cząstkowa**

Najwyższa Izba Kontroli ocenia pozytywnie przestrzeganie przez Urząd przyjętych procedur dotyczących przechowywania i zabezpieczenia danych oraz zapewnienia im właściwej ochrony.

## 4. Zakres przetwarzanych zasobów informacyjnych

Opis stanu faktycznego

**4.1.** Urząd w swojej dokumentacji wykazywał prowadzenie 33 zbiorów danych osobowych, z tego 16 wyłącznie w formie papierowej oraz 17 w formie elektronicznej lub elektronicznej i papierowej. Do prowadzenia zbiorów danych osobowych w wersji elektronicznej wykorzystywanych było 13 systemów informatycznych, tj.: SmartDOC (rejestr kontrahentów), Źródło (System Rejestrów Państwowych, akty stanu cywilnego), ELUD (rejestr mieszkańców, rejestr zamieszkania cudzoziemców), NDM+ (dodatki mieszkaniowe i energetyczne), WYB+ (rejestr mieszkańców), EwOpis i EwMapa (ewidencja gruntów i budynków), MIENIE (ewidencja nieruchomości miejskich), EMUiA (rejestr numerów porządkowych), WF-GANG i KADRY-PŁACE (systemy kadrowo-płacowe) PKZP (kasa zapomogowo-pożyczkowa pracowników Urzędu i pracowników oświaty), FISKUS (podatki lokalne, ewidencja opłat za odpady komunalne). (dowód: akta kontroli str. 4-53)

**4.2.** Zbiory danych zgłoszone do GIODO nie były aktualizowane. Jak podano w pkt. 2 niniejszego wystąpienia pokontrolnego, występowały rozbieżności pomiędzy zbiorami zgłoszonymi do GIODO a wykazywanymi w dokumentacji przetwarzania danych osobowych Urzędu. Trwała też, prowadzona przez ABI, weryfikacja zbiorów danych i zakresu danych w nich prowadzonych. Przedstawione przez poszczególne referaty Urzędu informacje w tym zakresie wskazują na rozbieżności w zakresie przetwarzanych danych w poszczególnych zbiorach i na konieczności zidentyfikowania nowych zbiorów danych.
(dowód: akta kontroli str. 161, 162-181, 227-228, 229-256,474-518)

**4.3.** Z danych gromadzonych przez Urząd w systemie FISKUS (obsługującego podatki lokalne i ewidencję opłat za odpady komunalne) wynika, że dane gromadzone przez jednostkę były niezbędne do realizacji zadań w tych obszarach.
(dowód: akta kontroli str. 257-261)

Nie w pełni natomiast Urząd wywiązywał się z obowiązku informacyjnego w przypadku naboru kandydatów do pracy, co szerzej omówiono w sekcji „Ustalone nieprawidłowości".

**4.4.** Urząd posiadał dostęp do zewnętrznych zbiorów danych, dla których ADO nie był administratorem. Dotyczyło to systemów: Źródło (System Rejestrów Państwowych), CEIDEG (Centralna Ewidencja i Informacja o Działalności Gospodarczej), EMUiA (Rejestr numerów porządkowych), KDR (Rejestr Wniosków o Kartę Dużej Rodziny). W przypadku wszystkich wymienionych wyżej baz danych uzyskano dostęp dla pracowników Urzędu od administratorów tych zbiorów danych. W przypadku dostępu do Systemu Rejestrów Państwowych (Źródło) Urząd spełnił warunki dostępu, gdyż osiem stanowisk do obsługi aplikacji Źródło nie miało dostępu do Internetu, a pracownicy mieli stosowne upoważnienia.
(dowód: akta kontroli str. 149, 182-183, 363-382)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niespełnieniu w pełnym zakresie obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, wobec kandydatów do pracy. W ogłoszeniu o naborze określono adres administratora danych i cel zbierania danych – podając ustawę o pracownikach samorządowych. Nie poinformowano natomiast kandydatów o prawie dostępu do swoich danych oraz ich poprawiania, dobrowolności lub obowiązku podania danych, tj. w zakresie art. 24 ust. 1 pkt 3 i 4 ww. ustawy. (dowód: akta kontroli str. 462-464)

Burmistrz wyjaśnił, że obowiązek informacyjny, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, w części był realizowany. Ogłoszenie o naborze na wolne stanowiska urzędnicze zawierało określenie administratora danych osobowych (Burmistrz Miasta) z podaniem pełnego adresu, jako podmiotu przetwarzającego dane, oraz określało cel i podstawę prawną przetwarzania danych osobowych (ustawa o pracownikach samorządowych). Mając na względzie zgodne z prawem przetwarzanie danych osobowych klientów Urzędu, jest analizowany sposób realizacji obowiązku wynikającego z art. 24 ww. ustawy. (dowód: akta kontroli str. 472-473)

**Ocena cząstkowa**

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonej nieprawidłowości sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności Urzędu, a w odniesieniu do zbiorów zewnętrznych – spełniał wymogi związane z dostępem do tych zbiorów.

## 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[20], wnosi o:

1. Analizowanie i zabezpieczenie przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w Urzędzie.
2. Umożliwianie zdalnego dostępu firmom serwisującym składniki systemu Urzędu po uzyskaniu odpowiedniej autoryzacji, która pozwoli na zidentyfikowanie działań podejmowanych przez te podmioty w serwisowanych systemach.
3. Zapewnienie zgodności zbiorów danych przetwarzanych w Urzędzie i ich zakresu ze zgłoszeniem do GIODO oraz z wykazem zamieszczonym w dokumentacji Urzędu.
4. Zapewnienie szkoleń pracownikom zaangażowanym w proces przetwarzania informacji, w szczególności w związku ze zmianami uregulowań wewnętrznych i zewnętrznych w tym obszarze.
5. Zakończenie realizacji sprawdzeń przez ABI oraz zaktualizowanie dokumentacji przetwarzania danych osobowych Urzędu stosownie do wyników tych sprawdzeń.
6. Zapewnienie obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, podczas zbierania danych osobowych.

## 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 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 23 stycznia 2018 r.

| | |
|---|---|
| Kontroler<br>Wojciech Olszewski<br>doradca ekonomiczny | DYREKTOR DELEGATURY<br>Najwyższej Izby Kontroli w Białymstoku<br>z up. WICEDYREKTOR<br>Robert Skwarko |
| .....<br>*podpis* | .....<br>*podpis* |

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