R. M. Wiśniewska

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.001.02.2017
R/17/001

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	R/17/001 – Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w województwie podlaskim
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	Paweł Tołwiński – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/22/2017 z dnia 1 lutego 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Miejski w Michałowie, ul. Białostocka 11, 16-050 Michałowo (zwany dalej: „Urzędem")
Kierownik jednostki kontrolowanej	Włodzimierz Konończuk– Burmistrz Michałowa[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Urząd w okresie objętym kontrolą[3] nie podejmował wszystkich działań, wymaganych przepisami prawa oraz regulacjami wewnętrznymi, zmierzających do zapewnienia ochrony posiadanych zasobów informacyjnych, co obniżało poziom ich bezpieczeństwa.

Uzasadnienie oceny ogólnej

Stwierdzono bowiem następujące nieprawidłowości:

- nie wywiązano się z obowiązku zgłoszenia Generalnemu Inspektorowi Ochrony Danych Osobowych (dalej: „GIODO") do zarejestrowania 37 z 42 przetwarzanych w Urzędzie zbiorów danych osobowych,
- 17 (z 24) pracowników merytorycznych Urzędu (w tym osoba pełniąca obowiązki ASI), przetwarzało dane w zbiorach danych osobowych, bez upoważnienia Burmistrza,
- w jednym zbiorze (z 21 objętych analizą) przetwarzano dane osobowe, które nie były wykorzystywane do realizacji zadań, w związku z którymi Urząd go prowadził, a w kolejnym zakres gromadzonych danych wykraczał poza określony w zgłoszeniu skierowanym do GIODO,
- nie wyegzekwowano od ABI obowiązku prowadzenia rejestru zawierającego wykaz zbiorów danych osobowych przetwarzanych w Urzędzie,
- nie opracowano polityki bezpieczeństwa informacji spełniającej wymogi określone w przepisach § 2 pkt 15 i § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4],
- nie pozbawiono dostępu do systemów zawierających dane osobowe pracownika, z którym rozwiązano stosunek pracy,
- nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
- od kierowników komórek organizacyjnych Urzędu nie wyegzekwowano realizacji obowiązku prowadzania okresowej analizy ryzyka dla poszczególnych systemów,

---

[1] Pełniący funkcję od 1 grudnia 2014 r.

[2] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna. Jeżeli sformułowanie oceny ogólnej według proponowanej skali byłoby nadmiernie utrudnione albo taka ocena nie dawałaby prawdziwego obrazu funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą, stosuje się ocenę opisową bądź uzupełnia ocenę ogólną o dodatkowe objaśnienie.

[3] Kontrolą objęty został okres o 1 stycznia 2016 r. do zakończenia czynności kontrolnych.

[4] Dz. U. z 2016 r. poz. 113, ze zm. Rozporządzenie zwane dalej: „rozporządzeniem KRI".

- niewłaściwie przechowywano papierową część 14 (z 42) powadzonych zbiorów danych osobowych,
- na pięciu (z 26) poddanych oględzinom komputerach, wykorzystywanych do przetwarzania danych osobowych, stwierdzono użytkowanie programów niezgodnie z warunkami ich licencji,
- sposób przechowywania kopii zapasowych nie odpowiadał regulacjom wewnętrznym, określonym w § 14 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- na jednym z 26 komputerów nie zainstalowano programu antywirusowego, a na kolejnym program ten nie posiadał aktualnej bazy sygnatur wirusów,
- 10 (z 11) programów, w którym przetwarzano dane osobowe nie umożliwiało każdej osobie, której dane przetwarzano, sporządzenie i wydrukowanie raportu zawierającego informacje dotyczące m.in.: daty pierwszego wprowadzenia danych osobowych, identyfikatora użytkownika wprowadzającego dane osobowe do systemu.

III. Opis ustalonego stanu faktycznego

1. Dokumentacja i procedury dotyczące ochrony danych

1.1. Dokumentacja dotycząca ochrony danych osobowych

Opis stanu faktycznego

Administratorem Danych Osobowych (dalej: „ADO") przetwarzanych w Urzędzie był Burmistrz Michałowa, który z dniem 1 stycznia 2016 r.[5] wyznaczył Administratora Bezpieczeństwa Informacji (dalej: „ABI"), o którym mowa w art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[6]. Rolę ABI powierzono osobie fizycznej prowadzącej działalność gospodarczą, niebędącej pracownikiem Urzędu. Postanowienia umowy określały m.in.: okres obowiązywania (od 1 stycznia 2016 r. do 31 grudnia 2017 r.), oświadczenie o spełnianiu wymogów dotyczących sprawowania funkcji ABI przez osobę, której ta funkcja została powierzona, wysokość wynagrodzenia za sprawowanie tej funkcji (839 zł netto), wysokość opłat za usługi wykonywane przez ABI poza zakresem umowy, jednomiesięczny okres wypowiedzenia. Burmistrz wyjaśnił, że powodem podjęcia decyzji o wyznaczeniu do pełnienia funkcji ABI osoby niebędącej pracownikiem Urzędu były *„ograniczone zasoby kadrowe"*. Dodał, że: *„Wybór „zewnętrznego" ABI okazał się korzystny również ze względu na niewygórowane warunki finansowe ABI, znacznie niższe niż np. koszty zatrudnienia specjalisty"*. (dowód: akta kontroli str. 4-12)

Ponadto w umowie wskazano zadania ABI określone w art. 36a ust. 2 pkt 1 powołanej ustawy, w tym: [1] sprawdzanie zgodności przetwarzania danych z przepisami o ochronie danych oraz opracowanie w tym zakresie sprawozdania dla administratora danych; [2] nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną (polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych); [3] nadzorowanie przestrzegania zasad określonych we wskazanej dokumentacji; [4] zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych. W umowie nie określono natomiast obowiązku prowadzenia przez ABI rejestru zbiorów danych przetwarzanych przez ADO, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 4-12)

W ramach pełnionej funkcji, ABI zobowiązał się m.in. do: sprawowania kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, opracowania sprawozdania dla administratora danych z przeprowadzanej kontroli, sprawdzenia i dokonania przeglądu aktualizacji polityk bezpieczeństwa danych osobowych wraz ze szczegółowym wykazem zbiorów danych, prowadzenia szkoleń wśród

[5] Zarządzeniem nr 9/2015 Kierownika Ośrodka Pomocy Społecznej w Krynkach z dnia 18 czerwca 2015 r. w sprawie powołania Administratora Bezpieczeństwa Informacji w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Krynkach.

[6] Dz. U. z 2016 r. poz. 992.

pracowników, audytu, zarządzania incydentami naruszenia polityki bezpieczeństwa danych osobowych, inwentaryzacji zbiorów i programów, ich wzajemnych relacji oraz miejsc przetwarzania danych osobowych. (dowód: akta kontroli str. 4-7)

Burmistrz, w myśl przepisu art. 46b ust. 1 ustawy o ochronie danych osobowych, zgłosił[7] do rejestracji GIODO fakt powołania ABI. Zgłoszenie zawierało elementy określone w art. 46b ust. 2 ww. ustawy, tj. m.in.: oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, imię, nazwisko i nr PESEL ABI oraz datę powołania. Zgłoszenie nie zawierało oświadczenia Burmistrza o spełnianiu przez ABI warunków określonych w art. 36a ust. 5 i 7 ustawy o ochronie danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". Z uwagi na ww. braki Urząd został poinformowany przez GIODO[8] o niezarejestrowaniu ABI i konieczności złożenia korekty ww. zgłoszenia, co nastąpiło 3 marca 2017 r. Analiza informacji (wg. stanu na 24 marca 2017 r.) zawartych w rejestrze prowadzonym przez GIODO, wykazała że znajdowały się w nim dane osoby wyznaczonej w Urzędzie na stanowisko ABI. Do zakończenia kontroli NIK nie dokonywano zmian na tym stanowisku. (dowód: akta kontroli str. 8-22, 180)

ABI w odniesieniu do zadań określonych w umowie oraz art. 36a ust. 2 pkt 1 ustawy o ochronie danych osobowych, podejmował działania wymienione poniżej.

1. Opracował plan sprawdzeń, o którym mowa w § 3 ust. 3-5 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[9], zatwierdzony przez Burmistrza 12 lutego 2016 r.
2. Opracował i 1 grudnia 2016 r. przekazał ADO projekt uaktualnionego dokumentu „Polityka Bezpieczeństwa Informacji" wraz z załącznikami, tj.: [1] Regulaminem Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych, [2] wzorami: wykazu pomieszczeń, w których odbywa się przetwarzanie danych osobowych, wykazu zbiorów danych oraz systemów informatycznych stosowanych do przetwarzania tych zbiorów, upoważnienia do przetwarzania danych osobowych, oświadczenia o zachowaniu poufności i zapoznaniu się z przepisami, ewidencji osób upoważnionych do przetwarzania danych osobowych, oświadczenia pracownika o zapoznaniu się z treścią Polityki Bezpieczeństwa Informacji. Dokument ten nie został jednak przyjęty i wdrożony w Urzędzie, gdyż – jak wyjaśnił Burmistrz – *„Opracowana przez ABI „Polityka Bezpieczeństwa Informacji", a w szczególności załącznik do niej „Regulamin Zarządzania Systemem Informatycznym" wymagały poprawek. Wersja dokumentu z 1 grudnia 2016 r. nie była wersją ostateczną".*
3. Przeprowadził 4 listopada 2016 r. szkolenie z zakresu ochrony danych osobowych dla 15 (z 28) pracowników merytorycznych Urzędu. Szkolenie zostało zakończone egzaminem dotyczącym, zagadnień na nim poruszanych. ABI sporządził sprawozdanie z przebiegu i analizy egzaminu. (dowód: akta kontroli str. 8-12, 33)

ABI nie prowadził rejestru, o którym mowa w art. 36a ust. 2 pkt 2 ww., zawierającego wykaz zbiorów danych osobowych przetwarzanych w Urzędzie, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Nie przeprowadził też zaplanowanego w 2016 roku sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (o którym mowa w art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych i w § 3 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora

---

[7] Data wysłania zgłoszenia: 2 lutego 2016 r.

[8] Pismem z dnia 27 lutego 2017 r. nr DR/406/000824/16/AŁ/13983/17.

[9] Dz. U. poz. 745. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie trybu i sposobu realizacji zadań przez administratora bezpieczeństwa informacji".

bezpieczeństwa informacji[10], co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 33)

W Urzędzie, w myśl przepisu art. 39 ust. 1 ww. ustawy, prowadzono ewidencją osób upoważnionych do przetwarzania danych osobowych. Zawierała ona elementy określone w art. 39 ust 1 pkt 1-3 ww. ustawy, tj.: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator. Według stanu na 2 lutego 2017 r. w ewidencji osób upoważnionych ujęto tylko upoważnienia dotyczące dostępu do systemów służących do przetwarzania danych osobowych w Urzędzie.

Analiza zakresów obowiązków 24 pracowników merytorycznych Urzędu i wydanych dla nich (przez Burmistrza) upoważnień do przetwarzania danych osobowych wykazała, że:

- wszyscy posiadali dostęp do zbiorów danych osobowych wynikający z ich zakresów obowiązków,
- siedmiu z nich było upoważnionych do przetwarzania danych we wszystkich zbiorach, do których mieli dostęp,
- 17 przetwarzało dane osobowe w zbiorach danych bez stosownego upoważnienia Burmistrza, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 34-37, 39-40, 95-97)

Według stanu na 8 lutego 2017 r., Urząd zgłosił GIODO do zarejestrowania 12 zbiorów danych osobowych. Przeprowadzone w trakcie kontroli NIK oględziny tych zbiorów wykazały m.in., że:

- Urząd nie prowadził sześciu (z 12) zgłoszonych zbiorów danych osobowych (dane w nich zawarte zostały przekazane Miejskiemu Ośrodkowi Pomocy Społecznej w Michałowie, Starostwu Powiatowemu w Białymstoku i Gminnej Bibliotece w Michalowie),
- cztery zbiory danych osobowych prowadził Urząd, a zakres danych w nich gromadzonych odpowiadał zgłoszeniu,
- w jednym przypadku zakres gromadzonych danych w zbiorze wykraczał poza zgłoszony GIODO (dotyczyło to: nr NIP, daty urodzenia i płci),
- w kolejnym nie przetwarzano danych osobowych (gromadzono jedynie dane finansowe). (dowód: akta kontroli str. 41-42)

W Urzędzie, wg. stanu na 28 lutego 2017 r., prowadzono 42 zbiory danych osobowych, z których tylko pięć zgłoszono do rejestracji przez GIODO (w 1999 roku), co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Zgłoszenia w tych sprawach zawierały elementy wymagane art. 41 ust. 1 ustawy o ochronie danych osobowych. Do 28 lutego 2017 r. nie stwierdzono przypadku odmowy rejestracji przez GIODO zgłaszanego zbioru danych, ani aktualizacji zbiorów już zgłoszonych. (dowód: akta kontroli str. 30-32)

W Urzędzie do 28 lutego 2017 r. nie wydawano innych wewnętrznych aktów prawnych, procedur, instrukcji lub poleceń dotyczących sposobu gromadzenia i przetwarzania zasobów informacyjnych w Urzędzie, niż dokumenty przyjęte w 2009 roku[11], tj.: „Polityka bezpieczeństwa", „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych", „Regulamin organizacji i przetwarzania danych osobowych". Od momentu przyjęcia tych dokumentów w 2009 roku, ich zapisy i postanowienia nie były aktualizowane. Nie opracowano również procedur, instrukcji dotyczących nadzoru oraz zapewnienia kontroli nad rodzajem danych osobowych i osobą wprowadzającą takie dane do danego zbioru, ani wskazaniem odbiorcy danych osobowych. Burmistrz wyjaśnił, że: *„W przypadku zbiorów prowadzonych w formie papierowej do konkretnych rejestrów dostęp mają konkretni pracownicy. Ewidencja i kontrola dostępu do tych danych nie jest*

[10] Dz. U. poz. 745. Rozporządzenie zwane dalej: „rozporządzeniem w sprawie trybu i sposobu realizacji zadań przez administratora bezpieczeństwa informacji".

[11] Zarządzeniem nr 243/09 Burmistrza Michałowa z dnia 14 września 2009 r. w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Miejskim w Michałowie.

prowadzona. W przypadku zbiorów prowadzonych w formie elektronicznej za pomocą oprogramowania dziedzinowego (programy produkcji : U.I. Infosystem, Aram, Geobid, Arisco) dostęp jest zabezpieczony za pomocą osobistych loginów i haseł. Wszelkie zmiany danych osobowych w tych bazach są rejestrowane w logach systemowych aplikacji. Dostęp do tych logów ma Administrator Systemu Informatycznego (ASI)".

(dowód: akta kontroli str. 8-12, 46-47)

Obowiązki związane z administrowaniem systemami informatycznymi[12] Burmistrz Michałowa powierzył z dniem 20 kwietnia 2012 r.[13] pracownikowi Urzędu, zatrudnionemu na stanowisku informatyka w Referacie Organizacyjnym. Według stanu na 23 lutego 2017 r. pracownik ten posiadł upoważnienie (z dnia 4 stycznia 2016 r.) do przetwarzania danych osobowych jedynie w zbiorze „Elektroniczny obieg dokumentów", mimo że w związku z pełnioną funkcją ASI, miał dostęp do danych gromadzonych we wszystkich systemach wykorzystywanych w Urzędzie, co opisano też w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 34-37, 46-47)

Od 1 stycznia 2016 r. do 28 lutego 2017 r. w Urzędzie nie przeprowadzano okresowych (co najmniej rocznych) audytów wewnętrznych z zakresu bezpieczeństwa informacji, wynikających z § 20 ust. 2 pkt. 14 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 46-47)

W latach 2016 – 2017 (do 28 lutego) zorganizowano jedno (nieodpłatne) szkolenie z zakresu ochrony danych osobowych dla 15 (z 28) pracowników merytorycznych Urzędu. Szkolenie przeprowadził 4 listopada 2016 r. ABI. Zakończono je egzaminem, dotyczącym poruszanych zagadnień[14], z którego przebiegu ABI sporządził sprawozdanie. Pracownicy zaangażowani w proces przetwarzania informacji nie uczestniczyli w tym okresie w innych szkoleniach z zakresu bezpieczeństwa i ochrony danych. Burmistrz wyjaśnił, że szkoleniem objęto 15 pracowników, gdyż *„w dniu szklenia obecnych było jedynie 23 pracowników merytorycznych Urzędu. Część z nich nie mogła uczestniczyć w szkoleniu z uwagi na konieczność obsługi interesantów przebywających w Urzędzie w trakcie szkolenia. Pracownicy nieobecni tego dnia na szkoleniu będą przeszkoleni podczas najbliższego szkolenia 28 lipca bieżącego roku".* (dowód: akta kontroli str. 26-29, 46-51)

Od 1 stycznia 2016 r. do 28 lutego 2017 r. nie prowadzono w Urzędzie zewnętrznych kontroli w zakresie bezpieczeństwa danych oraz nie wpłynęły skargi dotyczące przypadków związanych z ujawnieniem danych osobowych lub naruszeniem przepisów związanych z ich ochroną. (dowód: akta kontroli str. 46-47)

Ustalone nieprawidłowości

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

1. W umowie[15] dotyczącej wyznaczenia ABI nie zobowiązano go do prowadzenia rejestru zbiorów danych przetwarzanych w Urzędzie, mimo wymogu wynikającego z art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych. Burmistrz wyjaśnił, że: *„nie wiedział o takim obowiązku. ABI nie poinformował ADO o obowiązku prowadzenia rejestru zawierającego wykaz zbiorów danych osobowych przetwarzanych w Urzędzie".* W konsekwencji ABI do 28 lutego 2017 r. nie prowadził tego rejestru. Ponadto ABI nie przeprowadzał zaplanowanego w 2016 roku sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (o którym mowa w art. 36a ust. 2 pkt 1 lit. a ww. ustawy i w § 3 rozporządzenia w sprawie trybu i sposobu realizacji zadań przez administratora bezpieczeństwa informacji). Burmistrz wyjaśnił, że nie wyegzekwował obowiązku prowadzenia ww. rejestru, gdyż *„ADO nie miał świadomości istnienia takiego przepisu. ABI nie poinformował ADO o takim obowiązku".* Dodał, że nie wyegzekwował od ABI obowiązku przeprowadzenia zaplanowanego

---

[12] Dalej: „ASI".

[13] Zarządzeniem nr 143/2012 r. Burmistrza Michałowa z dnia 20 kwietnia 2012 r. w sprawie wyznaczenia Administratora Systemów Informatycznych w Urzędzie Miejskim w Michałowie.

[14] Obejmowały one m.in.: zasady użytkowania sprzętu komputerowego, nadawanie upoważnień i uprawnień do przetwarzania danych osobowych, procedury rozpoczęcia, zwieszenia i zakończenia pracy, zasady korzystania z poczty elektronicznej.

[15] Umowa nr 65/16 z 31 grudnia 2015 r.

sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, gdyż *„ADO nie kontrolował w ostatnim okresie (od 1 stycznia 2016 r. do 28 lutego 2017 r.) realizacji obowiązku sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych ABI. ABI nie poinformował ADO o takim obowiązku."* W latach 2016 – 2017 (do 28 lutego) wydatki Urzędu poniesione w związku z wyznaczeniem ABI wyniosły 14,4 tys. zł.

(dowód: akta kontroli str. 4-18, 22-23, 33, 53)

2. Według stanu na 23 lutego 2017 r. 17 (z 24) pracowników merytorycznych Urzędu (w tym osoba pełniąca obowiązki ASI) przetwarzało dane w zbiorach danych osobowych bez stosownego upoważnienia Burmistrza. Stanowiło to naruszenie przepisu art. 37 ustawy o ochronie danych osobowych, w myśl którego do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Burmistrz wyjaśnił, że: *„(...) Powodem takiej sytuacji było niedopatrzenie i błędne przeświadczenie, iż upoważnienia do przetwarzania danych osobowych obejmują jedynie zbiory przetwarzane w specjalistycznych programach bazodanowych, a nie wszystkie zbiory (przetwarzane w formie papierowej czy programach biurowych). (...)".* (dowód: akta kontroli str. 34-37, 54-55, 95-97,175-176)

3. Nie zgłoszono GIODO do zarejestrowania 37 z 42 zbiorów danych prowadzonych w Urzędzie, co naruszało wymogi art. 40 ustawy o ochronie danych osobowych. Dane osobowe w tych zbiorach były przetwarzane przed powołaniem ABI[16]. Burmistrz wyjaśnił, że: *„Przyczyną zaistniałego niedopełnienia obowiązków był wieloletni brak nadzoru nad wypełnianiem zapisów ustawy o ochronie danych osobowych w Urzędzie. Jest to jedna z przyczyn powołania ABI, który od początku roku 2016, zgodnie z art. 36a ust. 2 pkt 2 ustawy o ochronie danych osobowych, obowiązek prowadzenia jawnego rejestru zbiorów danych osobowych spoczywa na ABI".*

(dowód: akta kontroli str. 8-12, 30-37, 43-46)

4. Od 1 stycznia 2016 r. do 28 lutego 2017 r. w Urzędzie nie przeprowadzano okresowych (co najmniej rocznych) audytów wewnętrznych z zakresu bezpieczeństwa informacji, wynikających z § 20 ust. 2 pkt. 14 rozporządzenia KRI. Burmistrz wyjaśnił, że *„W Urzędzie nie prowadzono audytów wewnętrznych w zakresie bezpieczeństwa informacji ponieważ nie ma pracowników posiadających odpowiednie doświadczenie i niezbędną wiedzę do przeprowadzenia takiego audytu".*

(dowód: akta kontroli str. 8-12, 46-47)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że zgłoszenie do rejestracji przez GIODO faktu powołania ABI, przesłane 2 lutego 2016 r. (tj. w terminie 30 dni od dnia jego powołania), nie zawierało oświadczenia Burmistrza o spełnianiu przez ABI warunków określonych w art. 36a ust. 5 i 7 ustawy o ochronie danych osobowych. Z uwagi na ww. braki, dane ABI nie zostały zamieszczone w rejestrze. Urząd został poinformowany przez GIODO[17] o konieczności korekty zgłoszenia, co nastąpiło 3 marca 2017 r. (niezwłocznie po otrzymaniu ww. pisma GIODO) Burmistrz wyjaśnił, że powodem niezamieszczenie oświadczenia było przeoczenie. (dowód: akta kontroli str. 8-21)

1.2. Dokumentacja dotycząca warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne

Opis stanu faktycznego

W Urzędzie, zarządzeniem nr 243/09 Burmistrza Michałowa z 14 września 2009 r.[18], wprowadzono: *Politykę Bezpieczeństwa, Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* oraz *Regulamin organizacji i przetwarzania danych osobowych*. Dokumenty te nie były aktualizowane. W żadnym z nich nie określono poziomów bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 46-47, 56-94, 142-147)

---

[16] Zgodnie z art. 43 ust. 1a ustawy o ochronie danych osobowych obowiązkowi rejestracji zbiorów danych nie podlega administrator danych, który powołał ABI i zgłosił go do rejestracji GIODO.

[17] Pismem z dnia 27 lutego 2017 r. nr DR/406/000824/16/AŁ/13983/17.

[18] Zarządzenie w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Miejskim w Michałowie.

W Urzędzie poza ww. dokumentami nie wydawano innych regulacji, procedur, instrukcji dotyczących gromadzenia i przetwarzania zasobów informatycznych oraz danych osobowych. (dowód: akta kontroli str. 46-47)

Polityka bezpieczeństwa zawierała elementy określone w § 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 do przetwarzania danych osobowych[19], za wyjątkiem opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". Wykaz zbiorów danych osobowych (stanowiący załącznik Nr 1 do Polityki bezpieczeństwa) zawierał 11 z 42 prowadzonych przez Urząd zbiorów danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 56-65, 91, 98-99)

Przyjęta Instrukcja zarządzania zawierała wszystkie elementy wymagane przepisem § 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, tj. m.in.: [1] procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej (ASI) za te czynności, [2] stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem, [3] sposób zabezpieczenia systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania. (dowód: akta kontroli str. 66-77, 98-99)

Urząd nie opracował polityki bezpieczeństwa informacji, o której mowa w § 2 pkt 15, spełniającej wymogi § 20 ust. 1 rozporządzenia KRI, zaś przyjęte rozwiązania opisane w Instrukcji zarządzania i w Polityce bezpieczeństwa dotyczyły wyłącznie ochrony danych osobowych. Nie aktualizowało też regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 48-52, 98-99)

Spośród 11 systemów informatycznych Urzędu[20], w których przetwarzane były dane osobowe, tylko jeden (SmartDoc) zapewniał realizację wymogu określonego w § 7 ust. 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, tj. możliwość sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące m.in. daty pierwszego wprowadzenia danych osobowych i identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Niezrealizowanie ww. wymogu w odniesieniu do 10 pozostałych systemów, szerzej opisano poniżej, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 91, 100-101)

Ustalone nieprawidłowości

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

1. W przyjętych w Urzędzie dokumentach: Polityka bezpieczeństwa, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz w Regulaminie organizacji i przetwarzania danych osobowych nie określono poziomów bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Stanowiło to naruszenie przepisu § 6 rozporządzenia w sprawie dokumentacji oraz warunków technicznych. Burmistrz wyjaśnił, że: *„określenie odpowiedniego poziomu bezpieczeństwa wymaga przeprowadzenia analizy ryzyka. A taka nie była przeprowadzona...".* (dowód: akta kontroli str. 46, 56-94, 98-99, 137-147)
2. Polityka bezpieczeństwa, mimo wymogu określonego w § 4 pkt 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, nie zawierała opisu struktury zbiorów danych, wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi. Burmistrz wyjaśnił, że: *„Błąd w Polityce bezpieczeństwa (...)*

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

[20] SmartDOC, SRP Źródło, Alarm SELWIN, pakiet InfoSystem, serwis CIDG, Arisco GOMIG, Geobid EWMAPA, Geobid EWOPIS, serwis EMUiA, SIO, Home Banking.

wynikał z przeoczenia. Opracowywany obecnie projekt nowej Polityki bezpieczeństwa uwzględnia zapisy § 4 pkt 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych".

Wykaz zbiorów danych osobowych (stanowiący załącznik Nr 1 do Polityki bezpieczeństwa) nie zawierał także 31 z 42 prowadzonych w Urzędzie zbiorów danych osobowych. Burmistrz wyjaśnił, że: *„Wykaz był tworzony przez ASI i zawiera jedynie zbiory prowadzone w formie elektronicznej, za pomocą aplikacji dziedzinowych. Nie zawiera zbiorów prowadzonych w formie papierowej bądź za pomocą oprogramowania biurowego (arkusze MS-Excel czy dokumenty tekstowe MS-Word)".* Dodał, że pozostałe zbiory omyłkowo nie zostały ujęte w tym wykazie.

(dowód: akta kontroli str. 34-37, 48-52, 58-65, 91, 98-99)

3. W Urzędzie nie opracowano polityki bezpieczeństwa informacji, o której mowa w § 2 pkt 15, spełniającej wymogi § 20 ust. 1 rozporządzenia KRI, zaś przyjęte rozwiązania opisane w Instrukcji zarządzania i w Polityce bezpieczeństwa dotyczyły jedynie ochrony danych osobowych. Burmistrz wyjaśnił, że: *„Wdrożenie nowej polityki bezpieczeństwa informacji (...) wymaga dodatkowych nakładów pracy. Z uwagi na ograniczone zasoby kadrowe nie zostało to jeszcze uczynione. Prace nad opracowaniem polityki bezpieczeństwa trwają od roku 2016. Dokument ma być gotowy do końca maja br. Do końca września br. ADO planuje pełne wdrożenie polityki bezpieczeństwa informacji."* (dowód: akta kontroli str. 48-52, 98-99)

4. W 10[21] (z 11) systemów informatycznych Urzędu, w których przetwarzane były dane osobowe, nie zapewniało realizacji wymogu określonego w § 7 ust. 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, tj. możliwości sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące m.in. daty pierwszego wprowadzenia danych osobowych czy identyfikatora użytkownika wprowadzającego dane osobowe do systemu. ASI wyjaśnił, że: *„Nie wiedział o takim wymogu stawianym dla oprogramowania, ani też nie wie czy pozostałe programy mają możliwość sporządzania takich raportów..."*

(dowód: akta kontroli str. 91, 100-106)

Ocena cząstkowa

Urząd nie w pełni wywiązał się z obowiązku opracowania wymaganej dokumentacji i procedur dotyczących ochrony danych. Przyjęta w 2009 roku Polityka bezpieczeństwa nie była aktualizowana i nie zawierała niektórych elementów określonych w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych. Ponadto, mimo wymogu określonego w § 2 pkt 15 w związku § 20 ust. 1 rozporządzenia KRI, nie opracowano całościowej polityki bezpieczeństwa informacji. Z kolei ABI nierzetelnie wykonywał przypisane mu zadania. Nie wyegzekwowano od niego obowiązku prowadzenia rejestru zawierającego wykaz zbiorów danych osobowych oraz przeprowadzenia sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Brak działań podejmowanych przez ABI mógł być też powodem, dla którego 17 (z 24) pracowników merytorycznych Urzędu (w tym ASI) bez upoważnienia Burmistrza, tj. z naruszeniem art. 37 ustawy o ochronie danych osobowych, przetwarzało dane w zbiorach danych osobowych. Ponadto Urząd, wbrew przepisom art. 40 ustawy o ochronie danych osobowych, nie zgłosił GIODO do rejestracji 37 z 42 prowadzonych zbiorów danych osobowych. Tylko jeden zaś z 11 programów, w którym przetwarzano dane osobowe, umożliwiał każdej osobie, której dane przetwarzano, sporządzenie i wydrukowanie raportu zawierającego informacje dotyczące m.in.: daty pierwszego wprowadzenia danych osobowych, identyfikatora użytkownika wprowadzającego dane osobowe do systemu, co było wymogiem § 7 ust. 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych.

2. Zakres przetwarzanych zasobów informacyjnych

Opis stanu faktycznego

Dane w Urzędzie przetwarzane były w 42 zbiorach danych, z których 20 prowadzono w wersji elektronicznej i papierowej, a pozostałe w wyłącznie w formie papierowej.

[21] SRP Źródło, Alarm SELWIN, pakiet InfoSystem, serwis CIDG, Arisco GOMIG, Geobid EWMAPA, Geobid EWOPIS, serwis EMUiA, SIO, Home Banking.

Do GIODO zgłoszono pięć zbiorów, z tego jeden wskazując mniejszy niż gromadzono zakres danych w nim przetwarzanych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 30-37, 41-42, 52)

Do prowadzenia zbiorów danych osobowych w wersji elektronicznej wykorzystywanych było 11 systemów informatycznych, tj.: SmartDOC, SRP Źródło, Alarm SELWIN, pakiet InfoSystem, serwis CIDG, Arisco GOMIG, Geobid EWMAPA, Geobid EWOPIS, serwis EMUiA, SIO, Home Banking oraz oprogramowanie biurowe – arkusze programu MS-Word i MS-Excel. (dowód: akta kontroli str. 34-38, 91)

Wg. stanu na 8 lutego 2017 r. w Urzędzie nie prowadzono sześciu zbiorów danych: *„zasiłki rodzinne i pielęgnacyjne", „pomoc kombatantom", „dane osobowe osób korzystających z dodatku mieszkaniowego", „dane osobowe osób korzystających z pomocy społecznej", „usługi biblioteczne", „rejestr pojazdów i kierowców"*, które zostały zgłoszone do GIODO. Burmistrz wyjaśnił, że: *„Wszystkie ww. zbiory, poza zborem: „rejestr pojazdów i kierowców" nigdy nie były prowadzone przez Urząd. (...) Zbiory zostały omyłkowo zgłoszone do GIODO. Zbiór „rejestr pojazdów i kierowców" w roku 1999 został przekazany Starostwu Powiatowemu w Białymstoku".* Pomimo nie przetwarzania w Urzędzie danych w tych zbiorach, nie zwrócono się o ich wykreślenie z rejestru prowadzonego przez GIODO, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 8-12, 30-42, 91, 137-141)

W czterech (z pięciu) zbiorach zgłoszonych GIODO i prowadzonych przez Urząd (wg. danych na 8 lutego 2017 r.), zakres przetwarzanych danych był zgodny ze zgłoszeniem. W jednym gromadzono natomiast informacje nie objęte zgłoszeniem, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W okresie objętym kontrolą, nie aktualizowano zakresu danych gromadzonych w zbiorach zgłoszonych GIODO. (dowód: akta kontroli str. 30-33, 41-42)

Analiza 21 (z 42) zbiorów danych prowadzonych w poszczególnych komórkach organizacyjnych Urzędu wykazała, że w 20 przypadkach wszystkie dane gromadzone w zbiorach były wykorzystywane (niezbędne) do realizacji zadań, dla których zbiory te były prowadzone. W jednym przypadku gromadzono dane, które nie były wykorzystywane przy realizacji wykonywanych zadań, co opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 34-37, 107-109)

ADO wszystkich zbiorów danych (do których dostęp posiadali pracownicy Urzędu), z wyjątkiem SRP ŹRÓDŁO, serwis CEIDEG, serwis EMUiA[22], w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych, był Burmistrz. Urząd uzyskał dostęp do zbioru danych SRP ŻRÓDŁO z dniem 1 marca 2015 r., na podstawie upoważnienia Ministra Spraw Wewnętrznych z 29 grudnia 2014 r. Urząd spełnił wymogi dostępu do tego zbioru danych, tj. m.in. uniemożliwił dostęp do „otwartego" Internetu, na stanowiskach komputerowych z których obsługiwany jest ten system, pracownicy otrzymali upoważnienia do przetwarzania danych osobowych w tym systemie. Dostęp do serwisu CEIDG Urząd uzyskał natomiast na podstawie zgłoszenia z 29 kwietnia 2013 r. oraz zapewnił dwóm pracownikom obsługującym ten serwis, certyfikowany podpis elektroniczny. Możliwość przetwarzania danych w serwisie EMUiA została udostępniona na podstawie porozumienia zawartego 22 maja 2012 r. z Głównym Geodetą Kraju. Urząd wywiązał się z obowiązków zapewnienia odpowiedniej infrastruktury technicznej niezbędnej do użytkowania aplikacji oraz wskazania administratora i użytkowników tej aplikacji.

(dowód: akta kontroli str. 34-37, 107-109, 111-136)

Ustalone nieprawidłowości

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

1. Wg. stanu na 8 lutego 2017 r. w Urzędzie nie prowadzono sześciu zbiorów danych: *„zasiłki rodzinne i pielęgnacyjne", „pomoc kombatantom", „dane osobowe osób*

[22] System Rejestrów Państwowych aplikacja ŹRÓDŁO, Centralna Ewidencja i Informacja o Działalności Gospodarczej, Ewidencja Miejscowości Ulic i Adresów.

korzystających z dodatku mieszkaniowego", „dane osobowe osób korzystających z pomocy społecznej", „usługi biblioteczne", „rejestr pojazdów i kierowców", które zostały zgłoszone GIODO. Pomimo to, nie zwrócono się do GIODO o ich wykreślenie z prowadzonego rejestru. Ponadto w zbiorze: *„Wymiar podatków i rachunkowość podatkowa"* zakres gromadzonych danych osobowych wykraczał poza zgłoszony GIODO (dotyczyło to przetwarzania: nr NIP, daty urodzenia i płci). Naruszono w ten sposób art. 41 ust. 2 ustawy o ochronie danych osobowych, zgodnie z którym ADO jest obowiązany zgłaszać GIODO zmianę zakresu gromadzonych danych w zbiorze, w terminie 30 dni od dnia dokonania zmiany. Burmistrz wyjaśnił, że powodem nieprawidłowości było niedopatrzenie. Wyjaśnił również, że: *„Podczas zgłaszania zbioru „Wymiar podatków i rachunkowość podatkowa" do rejestracji w GIODO błędnie nie wykazano przetwarzania: nr NIP, daty urodzenia i płci. Od momentu zgłoszenia nie zmieniała się struktura zbiorów w tym rejestrze i w związku z tym nie korygowano danych zgłoszonych do GIODO. ADO nie analizował zgłoszeń do GIODO i nie miał informacji o braku: nr NIP, daty urodzenia i płci w zgłoszeniu do GIODO".*

(dowód: akta kontroli str. 8-12, 30-32, 41-42)

2. W zbiorze danych *„Nauczanie indywidualne i rewalidacyjne"* gromadzono kopie orzeczeń o potrzebie kształcenia specjalnego oraz orzeczeń o potrzebie wcześniejszego wspomagania rozwoju dziecka, które nie były wykorzystywane (niezbędne) do realizacji zadań, dla których zbiór ten był prowadzony. Gromadzenie danych osobowych niewykorzystywanych do realizacji zadań narusza przepis art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, zgodnie z którym przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa. Burmistrz wyjaśnił, że: *„Kopie ww. orzeczeń nie są niezbędne do realizacji zadań, dla których jest prowadzony zbiór (...). Są one przechowywane na potrzeby ewentualnej kontroli prawidłowości i zasadności wydania decyzji o nauczaniu indywidualnym i rewalidacyjnym".*

(dowód: akta kontroli str. 107-109, 137-141)

Ocena cząstkowa

Urząd przetwarzając dane osobowe wykroczył poza uprawnienia wynikające z przepisów oraz realizowanych zadań. Nie wywiązał się bowiem z obowiązku poinformowania GIODO o zaprzestaniu przetwarzania danych w sześciu zbiorach danych osobowych (które przekazano innym jednostkom), w jednym z 21 analizowanych zbiorów zakres gromadzonych informacji wykraczał poza dane niezbędne do realizacji zadań, w związku z którymi Urząd go prowadził, a w kolejnym zakres gromadzonych danych wykraczał poza określony w zgłoszeniu skierowanym do GIODO. Spełniono zaś wymogi dotyczące dostępu do zbiorów danych osobowych, których administratorami były podmioty zewnętrzne.

3. Sposób przechowywania oraz fizycznego zabezpieczenia danych

Opis stanu faktycznego

W Urzędzie 20 z 42 zbiorów danych osobowych prowadzono z wykorzystaniem systemów elektronicznych, a pozostałe papierowo. W rozdziale VIII Polityki bezpieczeństwa, określono środki ochrony dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Przyjęte rozwiązania w sposób ogólny określały środki ochrony fizycznej, wskazują że obejmują one m.in.: [1] lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie, [2] ustalenie zasad gospodarki kluczami do pomieszczeń i szaf, [3] wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, we wzmocnione drzwi, odpowiednio zabezpieczone okna, meble, zamknięcia i niezbędne zabezpieczenia alarmowe, [4] składowanie danych sensytywnych oraz nośników wymiennych i nośników kopii zapasowych, w odpowiednio zabezpieczonych szafach, [5] odpowiednie wyposażenie i zabezpieczenie pomieszczeń serwerowni. Jak wyjaśnił Burmistrz w przyjętej Polityce bezpieczeństwa nie zawarto precyzyjnych zapisów dotyczących sposobu zabezpieczenia szaf wykorzystywanych do składowania danych sensytywnych, nośników wymiennych i nośników kopii zapasowych oraz wyposażenia i zabezpieczeń pomieszczeń serwerowni, gdyż: *„podczas tworzenia obowiązującej Polityki bezpieczeństwa ADO uznał istniejące zapisy za wystarczające. Obecnie przygotowywana jest nowa Polityka bezpieczeństwa. W nowym dokumencie zawarte będą szczegółowe opisy dotyczące ww. zabezpieczeń".* Ponadto nie

wyegzekwowano, od kierowników Urzędu, realizacji obowiązku określonego w § 19 ust. 2 Polityki bezpieczeństwa, prowadzania okresowej analizy ryzyka dla poszczególnych systemów, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 34-37, 58-65, 100-101, 137-141)

Oględziny pomieszczeń, w których przetwarzane były zbiory danych osobowych wykazały, że zgodnie z postanowieniami Polityki bezpieczeństwa: [1] przetwarzanie danych odbywało się w miejscach do tego wyznaczonych; [2] w Urzędzie zainstalowano monitoring wizyjny oraz system alarmowy; [3] dane sensytywne (określone w art. 27 ustawy o ochronie danych osobowych) przechowywane były w zamykanych szafach; [4] pomieszczenie serwerowni posiadało zabezpieczenia w postaci: systemu alarmowego, gaśnicy, drzwi przeciwpożarowych, czujnika otwarcia drzwi, systemu klimatyzacji. Stwierdzone odstępstwa od przyjętych zasad zabezpieczenia fizycznego danych dotyczyły m.in.: nieustalenia polityki gospodarowania kluczami, braku zabezpieczeń w postaci wzmacnianych drzwi i antywłamaniowych okien do pomieszczeń w których przetwarzane są dane osobowe, niewłaściwego przechowywania papierowej części 14 (z 42) powadzonych zbiorów danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 34-37, 142-147)

Kopie zapasowe baz danych, zgodnie z postanowieniami § 14 ust. 2 Instrukcji zarządzania systemem informatycznym, znajdowały się poza stałym miejscem przetwarzania tych danych. Przyjętym regulacjom wewnętrznym nie odpowiadał natomiast sposób przechowywania tych kopii, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 66-77, 142-147, 165-166)

W Urzędzie nie gromadzono danych, o których mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 100-101)

W latach 2016 – 2017 (do 28 lutego) w Urzędzie nie likwidowano sprzętu komputerowego, będącego nośnikiem danych oraz nie wystąpiły przypadki, w których sprzęt komputerowy naprawiany był przez podmioty zewnętrzne. Nośniki danych przeznaczone do utylizacji przechowywane były w pomieszczeniu serwerowni. ASI wyjaśnił, że: *„Zgromadzone obecnie w serwerowni nośniki danych przeznaczone do zniszczenia nie zajmują dużo miejsca i nie ma problemu z ich przechowywaniem".* (dowód: akta kontroli str. 100-101, 142-147)

Niszczenie dokumentów zawierających dane osobowe prowadzono w niszczarkach, które zlokalizowano w każdym pomieszczeniu stanowiącym obszar przetwarzania danych osobowych. W Urzędzie nie opracowano regulacji wewnętrznych w tym zakresie.
(dowód: akta kontroli str. 56-77, 100-101)

W § 23 ust. 3 Instrukcji zarządzania określono, że osoby użytkujące komputery przenośne, które są wykorzystywane do przetwarzania danych osobowych, zobowiązane są do stosowania właściwych zabezpieczeń technicznych i ochrony kryptograficznej oraz zachowania szczególnej ostrożności podczas ich transportu i przechowywania. Trzech pracowników Urzędu korzystało ze służbowych komputerów przenośnych poza siedzibą jednostki, tj.: Skarbnik, Kierownik Referatu Inwestycyjno-Geodezyjnego oraz Informatyk. Komputery będące w ich posiadaniu, w myśl postanowień 23 ust. 3 Instrukcji zarządzania posiadały ochronę kryptograficzną (szyfrowane dyski). Konfiguracja systemów informatycznych Urzędu uniemożliwia korzystanie z nich spoza siedziby jednostki.
(dowód: akta kontroli str. 66-77, 100-101)

Sprzątanie pomieszczeń, w których przetwarzano dane osobowe prowadzono po zakończeniu pracy przez pracowników upoważnionych do przetwarzania danych. W Urzędzie nie wprowadzono wewnętrznych regulacji w tym zakresie. Osoby sprzątające pobierały klucze do pomieszczeń z miejsc ich przechowywania (z sekretariatu i biura podawczego). Żadna z dwóch osób sprzątających nie uzyskała pisemnej zgody od ADO, o której mowa w pkt. I ust. 2 załącznika do rozporządzenia w sprawie dokumentacji oraz warunków technicznych, na przebywanie w obszarze przetwarzania danych. Burmistrz

wyjaśnił: *„ADO nie zwrócił uwagi na te zapisy rozporządzenia. Opracowana obecnie nowa „Polityka bezpieczeństwa" będzie zawierała wzory takich upoważnień".*

(dowód: akta kontroli str. 100-101, 137-141)

Procedury dotyczące przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych zostały określone w § 24 Instrukcji zarządzania. Określono w nich m.in., że ASI dokonuje sprawdzenia działania technicznych zabezpieczeń, funkcjonalności i jakości pracy oraz określenia przydatności elektronicznych nośników informacji. Odpowiada on również za terminowość (raz na kwartał) przeprowadzania tych przeglądów i konserwacji oraz ich prawidłowy przebieg. W latach 2016 – 2017 (do 28 lutego) ASI nie prowadził udokumentowanych działań w tym zakresie. Wyjaśnił on, że: *„Przeglądy i konserwacja systemów oraz nośników informacji służących do przetwarzania danych osobowych są przeprowadzane regularnie (co kwartał). Podczas dotychczasowych czynności nie ujawniono nieprawidłowości".*

(dowód: akta kontroli str. 66-77, 100-106)

Urząd nie posiadał wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia awarii długotrwałego braku zasilania. ASI wyjaśnił, że: *„Budynek Urzędu jest wyposażony w dodatkowe, awaryjne przyłącze energetyczne. Podczas długotrwałego braku zasilania przyłącze może być zasilane za pomocą zewnętrznego agregatu prądotwórczego. Takim agregatem dysponuje zakład budżetowy Gminy – ZGKiM w Michałowe".*

(dowód: akta kontroli str. 100-106)

ASI wyjaśnił, że: *„co jakiś czas testuje kopie zapasowe serwerów (zazwyczaj co ok. 30 dni). Nie jest prowadzona jedynie dokumentacja tych czynności".*

(dowód: akta kontroli str. 102-106)

Ustalone nieprawidłowości

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

1. W latach 2016 – 2017 (do 28 lutego) nie wyegzekwowano od kierowników komórek organizacyjnych Urzędu realizacji obowiązku określonego w § 19 ust. 2 Polityki bezpieczeństwa, dotyczącego prowadzenia okresowej analizy ryzyka dla poszczególnych systemów. Burmistrz wyjaśnił: *„Powodem było niedopatrzenie. ADO nie zwrócił uwagi na zapisy § 19 ust. 2 Polityki bezpieczeństwa i nie wyegzekwował obowiązku ich realizacji".* (dowód: akta kontroli str. 58-65, 100-101, 137-141)

2. Oględziny pomieszczeń, w których przetwarzane były zbiory danych osobowych wykazały odstępstwa od przyjętych zasad zabezpieczenia fizycznego danych, które dotyczyły m.in.: nieustalenia polityki gospodarowania kluczami (mimo wymogu określonego w § 20 ust. 2 lit. B Polityki bezpieczeństwa), braku zabezpieczeń w postaci wzmacnianych drzwi i antywłamaniowych okien do pomieszczeń, w których przetwarzano dane osobowe, niewłaściwego przechowywania (na półkach nieposiadających zabezpieczeń) papierowej części 14 (z 42) zbiorów danych osobowych. Burmistrz wyjaśnił, że: *„W Urzędzie praktykowana jest zasada, iż pracownicy mają dostęp do kluczy jedynie swoich pomieszczeń i szafek. (...) ADO nie stworzył dokumentu określającego zasady gospodarki kluczami do pomieszczeń i szaf, gdyż dotychczasowe, ustne przekazywane zasady uważał za wystarczające".* Ponadto dodał, że powodem przechowywania papierowej formy 14 (z 42) zbiorów danych osobowych na półkach (bez zabezpieczeń) *„... są ograniczone możliwości finansowe. ADO wie o istniejących brakach w zabezpieczeniach fizycznych danych osobowych przechowywanych w formie papierowej. ADO planuje zakup dodatkowych szafek z odpowiednimi zabezpieczeniami".* (dowód: akta kontroli str. 137-147)

3. Kopie zapasowe systemów Urzędu przechowywano na nośnikach danych w pomieszczeniu serwerowni oraz w pokoju nr 27. W pokoju tym nośniki zawierające kopie zapasowe umiejscowiono na biurku pracownika (ASI). Były one stale podłączone do sieci Urzędu. Pomieszczenie nr 27, w którym znajdowały się te nośniki nie posiadało żadnych zabezpieczeń typu: alarm, system przeciwpożarowy, drzwi antywłamaniowe, zabezpieczenia okna, sejf lub zabezpieczona szafa. Sposób przechowywania kopii zapasowych nie odpowiadał regulacjom wewnętrznym, określonym w Instrukcji

zarządzania (§14), zgodnie z którymi *„kopie zapasowe przechowuje się w metalowych szafach w pomieszczeniach, które nie są stałym miejscem ich przetwarzania i zapewniają właściwą ochronę przez nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub zniszczeniem"*. ASI wyjaśnił, że przyjęty sposób przechowywania kopii zapasowych w pokoju nr 27 wynika z braku odpowiednio przystosowanego i wyposażonego pomieszczenia. (dowód: akta kontroli str. 66-77, 137-147, 177-178)

4. W Urzędzie nie gromadzono bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmujących ich rodzaj i konfigurację, mimo obowiązku wynikającego z w § 20 ust. 2 pkt 2 rozporządzenia KRI. Burmistrz wyjaśnił *„Powodem są ograniczone zasoby kadrowe. Prowadzenie szczegółowej ewidencji sprzętu IT, infrastruktury IT i oprogramowania wymaga znacznych nakładów pracy. Na początku lutego br. ASI rozpoczął wdrażanie darmowego systemu de ewidencji oprogramowania i sprzętu IT – Spiceworks Inventory. Pełne wdrożenie systemu planowane jest do końca maja br."*
(dowód: akta kontroli str. 100-101, 137-147)

Ocena cząstkowa

Przyjęte w Urzędzie regulacje wewnętrzne dotyczące ochrony danych osobowych nie były w pełni egzekwowane, co mogło mieć wpływ na poziom bezpieczeństwa przetwarzanych danych. Od kierowników komórek organizacyjnych Urzędu nie wyegzekwowano realizacji obowiązku określonego w § 19 ust. 2 Polityki bezpieczeństwa, prowadzania okresowej analizy ryzyka dla poszczególnych systemów. Niewłaściwie przechowywano (na półkach nieposiadających zabezpieczeń) papierową część 14 (z 42) zbiorów danych osobowych. Z kolei sposób przechowywania kopii zapasowych nie odpowiadał regulacjom wewnętrznym, określonym w § 14 Instrukcji zarządzania. Ponadto w Urzędzie nie gromadzono bieżących informacji o inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację, czym naruszono przepis § 20 ust. 2 pkt 2 rozporządzenia KRI.

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

Opis stanu faktycznego

W Urzędzie do przetwarzania danych wykorzystywano 11 systemów informatycznych, które zostały wymienione w pkt 2 niniejszego wystąpienia pokontrolnego.

W latach 2016 – 2017 (do 28 lutego) w Urzędzie nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 100-101)

Według stanu na 2 lutego 2017 r. 23 (z 24) pracowników merytorycznych Urzędu zaangażowanych było w proces przetwarzania informacji w stopniu adekwatnym do realizowanych zadań, ustalonych w ich zakresach obowiązków. Nieposiadanie przez 17 pracowników upoważnień do przetwarzania danych osobowych we wszystkich zbiorach, do których mieli dostęp, został szerzej opisany w pkt 1.1 wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 34-37, 95-97)

Analiza sposobu odbierania siedmiu pracownikom, z którymi od 1 stycznia 2016 r. do 28 lutego 2017 r. rozwiązano stosunek pracy, uprawnień do systemów wykorzystywanych do przetwarzania danych w Urzędzie wykazała m.in., że:

- trzech w okresie zatrudnienia nie posiadało dostępu do systemów zawierających dane osobowe,
- trzech posiadało dostęp do systemu SmartDoc, w którym ich konta użytkownika zostały zablokowane z chwilą rozwiązania stosunku pracy,
- w jednym przypadku, pracownik z którym rozwiązano stosunek pracy z dniem 1 kwietnia 2016 r. posiadał aktywne konto użytkownika we wszystkich systemach, do których miał dostęp w okresie zatrudnienia, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

(dowód: akta kontroli str. 148)

Każdy z pracowników zaangażowanych w przetwarzanie danych w systemach informatycznych Urzędu posiadał własny login i hasło do systemu operacyjnego jednostek komputerowych i dostępnych w nich systemów dziedzinowych. Oględziny wykazały, że wszystkim użytkownikom komputerów nadano uprawnienia administratora systemu operacyjnego, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". (dowód: akta kontroli str. 149-164)

W Urzędzie nie prowadzono papierowej wersji rejestru dostępu do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych. Informacje w tym zakresie gromadzone były w logach czterech (z 11) użytkowanych systemów. Pozostałe nie posiadały możliwości technicznych pozwalających na gromadzenie takich danych. Logi tworzone były w sposób automatyczny (bez możliwości zmiany ich treści) i przechowywane na centralnym serwerze Urzędu, gdzie znajdowały się serwery poszczególnych systemów dziedzinowych. Ponadto w lutym 2017 roku w Urzędzie skonfigurowano i zainstalowano urządzenie klasy UTM[23], pozwalające m.in. na prowadzenie zaawansowanego rejestru zdarzeń dla każdego z użytkowników sieci. Analiza logów zawartych w urządzeniu wykazała, że od chwili jego uruchomienia wykryło ono i zablokowało m.in. 17 prób włamania do sieci Urzędu. Logi zawierające ww. dane przechowywano w pamięci urządzenia oraz na serwerze centralnym Urzędu, przez okres odpowiednio: jednego i sześciu miesięcy. Jak wyjaśnił Burmistrz, zakup i wdrożenie urządzenia klasy UTM nie nastąpiło wcześniej *„Ze względu na koszty. Zakup takiego urządzenia był planowany od kilku lat, jednak priorytetem była wymiana pozostałego sprzętu IT (wymiany komputerów, zakup dysków do archiwizacji, zakup drukarek)".* Koszt zakupu ww. urządzenia wyniósł 3,9 tys. zł, a koszt licencji na program antywirusowy, filtry i aktualizację oprogramowania – 1,2 tys. zł.
(dowód: akta kontroli str. 137-141, 149-166)

Oględziny wszystkich 26 komputerów wykorzystywanych do przetwarzania danych, osobowych wykazały m.in., że:

- na każdym urządzeniu dostęp do systemu operacyjnego możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- comiesięczna zmiana hasła wymuszana była w sposób automatyczny jedynie w systemach dziedzinowych (nie wymuszano zmiany haseł do systemów operacyjnych komputerów),
- w 22 komputerach zapewniono bieżącą aktualizację systemów operacyjnych,
- w czterech jednostkach zainstalowany był system operacyjny nieposiadający wsparcia technicznego producenta, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności",
- w jednym z 21 komputerów posiadających dostęp do „otwartego" Internetu nie zainstalowano programu antywirusowego, a na kolejnym program nie był zaktualizowany, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości",
- w pięciu komputerach stwierdzono użytkowanie programów niezgodnie z warunkami ich licencji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości",
- we wszystkich jednostkach skonfigurowano wygaszacz ekranu uruchamiany po upływie trzech minut (powrót do systemu operacyjnego wymagał podania loginu i hasła użytkownika),
- nie stwierdzono przypadków wykorzystywania jednego konta użytkownika systemu operacyjnego przez więcej niż jedna osobę. (dowód: akta kontroli str. 149-164)

W Urzędzie nie określono wewnętrznych regulacji dotyczących sieci bezprzewodowej WiFi. Sieć ta działała w budynku Urzędu w oparciu o dwa urządzenia dostępowe, z których korzystanie możliwe było po wprowadzeniu klucza w standardzie WPA-2. Dostęp do tej sieci posiadali: ASI, asystent Burmistrza oraz pracownicy Referatu Inwestycyjno-

[23] UTM (ang. unified threat management) – wielofunkcyjna zapora sieciowa zintegrowana w postaci jednego urządzenia.

Geodezyjnego (siedem osób). Klucz dostępowy (nadany przez ASI) został wprowadzony do laptopów posiadających dostęp do sieci WiFi. (dowód: akta kontroli str. 100-101)

W Urzędzie nie wprowadzono regulacji umożliwiających wykorzystanie przez pracowników prywatnego sprzętu komputerowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych. Działająca w Urzędzie sieć WiFi oraz sieć LAN uniemożliwiały korzystanie z nich na urządzeniach niebędących własnością Urzędu bez znajomości klucza do sieci bezprzewodowej oraz akceptacji (przez ASI) na urządzeniu klasy UTM adresu MAC karty sieciowej urządzenia podłączanego do sieci LAN. Każdy fakt podłączenia urządzenia do sieci był odnotowywany w logach, które przechowywano na urządzeniu klasy UTM oraz na serwerze centralnym Urzędu, przez okres odpowiednio jednego i sześciu miesięcy.
(dowód: akta kontroli str. 100-101, 165-166)

W latach 2016 – 2017 (do 28 lutego) wystąpił jeden udokumentowany przypadek naruszenia bezpieczeństwa systemu informatycznego, polegający na zainfekowaniu jednego z komputerów wirusem znajdującym się w załączniku wiadomości email. W wyniku działania złośliwego oprogramowania zaszyfrowane zostały wszystkie dokumenty na dysku komputera. Podjęte działania polegały na sformatowaniu dysku i ponownej instalacji systemu operacyjnego. Skutkiem naruszenia bezpieczeństwa systemu informatycznego, była utrata wszystkich dokumentów znajdujących się na dysku lokalnym komputera (dane z systemów wykorzystywanych do przetwarzania danych zostały przywrócone z dostępnych kopii zapasowych). W raporcie z tego zdarzenia wskazano, że okolicznością sprzyjającą naruszeniu było podłączenie do sieci nowego komputera, który nie posiadał odpowiedniej ochrony, tj. zaktualizowanej bazy wirusów w zainstalowanym programie antywirusowym. Podjęte środki zapobiegawcze polegały na aktualizacji ww. programu oraz poinstruowaniu pracownika o zakazie otwierania załączników email pochodzących z nieznanych źródeł. Poza opisanym wyżej przypadkiem w latach 2016 – 2017 (do 28 lutego) w Urzędzie nie było konieczności odtworzenia zbioru danych z kopii bezpieczeństwa.
(dowód: akta kontroli str. 100-101, 179)

Przyjęte regulacje wewnętrzne Urzędu[24], dotyczące komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych, zobowiązywały użytkowników sprzętu do *„stosowania właściwych zabezpieczeń technicznych, ochrony kryptograficznej oraz zachowania szczególnej ostrożności podczas ich transportu"*. Ze służbowych komputerów przenośnych korzystało trzech pracowników Urzędu, tj. ASI, Skarbnik oraz Kierownik Referatu Inwestycyjno-Geodezyjnego. Wykorzystywane przez nich laptopy, w myśl przyjętych regulacji, posiadały ochronę kryptograficzną (szyfrowane dyski). Pracownikom wykorzystującym urządzenia przenośne nie zapewniono zdalnego dostępu do zbiorów danych przetwarzanych w Urzędzie. (dowód: akta kontroli str. 66-77, 100-101)

W latach 2016 – 2017 (do 28 lutego) obowiązywała umowa na prowadzenie serwisu oprogramowania wykorzystywanego w Urzędzie, zawarta 4 stycznia 2016 r. z podmiotem zewnętrznym. W pkt 2.4 tej umowy określono postanowienie, zgodnie z którym przy wykonywaniu wszelkich prac prowadzonych przez podmiot serwisujący, zobowiązuje się on do przestrzegania zasad określonych w ustawie o ochronie danych osobowych.
(dowód: akta kontroli str. 167-168)

Ochronę systemów informatycznych Urzędu stanowiło urządzenie klasy UTM, monitorujące ruch na dwóch posiadanych łączach internetowych DSL. Urządzenie to wyposażono w zaporę sieciową w systemem wykrywania włamań – IDS/IPS, kontrolę aplikacji, program antywirusowy i filtrowanie treści, ochronę przed atakami DoS/DDoS, filtr danych. Urządzenie to umożliwiało wykrywanie i zapobieganie włamaniom. Uzupełnienie zabezpieczeń stanowiły programy antywirusowe zainstalowane na poszczególnych komputerach użytkowanych do przetwarzania danych. (dowód: akta kontroli str. 165-166)

W 2010 roku Urząd wykupił usługę hostingu strony internetowej, domenę internetową oraz pocztę elektroniczną w podmiocie zewnętrznym (Świat Internet S.A. należącą do grupy Netia S.A.). Dane przechowywano na serwerach wykonawcy usługi, który był również

[24] Określone w § 23 ust. 3 Instrukcji zarządzania.

administratorem danych. Zgodnie z § 19 regulaminu sieci Netia S.A.[25], podmiot realizujący usługę zapewnia tajemnicę, m.in.: informacji przekazywanych w sieci telekomunikacyjnej, danych osobowych abonenta, informacji dotyczących faktu, okoliczności i rodzaju połączenia telekomunikacyjnego, prób uzyskania takiego połączenia.

(dowód: akta kontroli str. 169-170)

W Urzędzie nie opracowano procedur związanych z płatnościami realizowanymi drogą elektroniczną. Dokonywano ich za pośrednictwem systemu bankowego (HomeBanking), dostępnego na stronie internetowej, z użyciem technologii VPN[26]. Po sprawdzeniu dokumentu pod względem merytorycznym i formalno-rachunkowym oraz zatwierdzeniu go do wypłaty / przelewu, wyznaczony pracownik sporządzał szablon przelewu, który był zatwierdzany przez jedną z dwóch uprawnionych osób z wykorzystaniem bankowego podpisu elektronicznego. (dowód: akta kontroli str. 100-101, 171-174)

Ustalone nieprawidłowości

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

1. W Urzędzie w nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 3 rozporządzenia KRI. ASI wyjaśnił: *„Powodem było niedopatrzenie i że nie wiedział, iż należy dokonywać okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko".*

   (dowód: akta kontroli str. 100-106)

2. Oględziny systemów informatycznych wykazały, że jeden pracownik, z którym rozwiązano stosunek pracy z dniem 1 kwietnia 2016 r., nadal posiadał aktywne konto użytkownika we wszystkich trzech systemach, do których miał dostęp w okresie zatrudnienia[27].ASI wyjaśnił: *„Jest to przeoczenie. Konto powinno być zdezaktywowane najpóźniej dzień po zwolnieniu pracownika".* (dowód: akta kontroli str. 102-106, 148)

3. Na jednym[28] (z 26) poddanych oględzinom komputerów, wykorzystywanych do przetwarzania danych w Urzędzie nie zainstalowano programu antywirusowego, a na kolejnym (znajdującym się w pokoju nr 9) program nie był zaktualizowany. Było to sprzeczne z postanowieniami § 17 Instrukcji zarządzania, w myśl którego system, w którym przetwarzane są dane osobowe jest wyposażony w mechanizmy ochrony antywirusowej, a obowiązkiem ASI jest uaktualnianie sygnatur w bazie antywirusowej. ASI wyjaśnił, że nie zauważył braku oprogramowania antywirusowego na tym komputerze. Komputer ten był przeznaczony do likwidacji i nie służył do ciągłej pracy, a jedynie do podręcznego podglądu. W dniu 26 marca 2017 r. ASI zainstalował na tym komputerze program antywirusowy. W odniesieniu do drugiego komputera ASI dodał, że nie posiadał on zaktualizowanej bazy sygnatur, gdyż fakt uszkodzenia programu antywirusowego został zgłoszony dwa dni przed prowadzonymi oględzinami. Wskazał również, że 26 marca 2017 r. dokonał naprawy polegającej na ponownej instalacji programu antywirusowego. (dowód: akta kontroli str. 102-106, 149-164)

4. Na pięciu (z 26) poddanych oględzinom komputerów, wykorzystywanych do przetwarzania danych użytkowano programy WINRAR i TotalCommander, po upływie okresu testowego, tj. niezgodnie z warunkami ich licencji. ASI wyjaśnił, że: *„Dotychczasowe wewnętrzne kontrole stanowisk komputerowych przeprowadzone przez ASI nie sprawdzały używania testowych wersji oprogramowania i okresu ich testowania.* Wszystkie programy zostały usunięte przez ASI w trakcie oględzin.

   (dowód: akta kontroli str. 102-106, 149-164)

5. Wszystkim użytkownikom komputerów (wykorzystywanych do przetwarzania danych w Urzędzie), nadano uprawnienia administratora systemu operacyjnego. ASI wyjaśnił, że nadanie użytkownikom uprawnień administratora systemu operacyjnego:

---

[25] https://www.netia.pl/files/regulamin.pdf.

[26] VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna) – tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet), w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów.

[27] Info System (Podatek od osób fizycznych i Podatek od osób prawnych), EWOPIS, EWMAPA.

[28] Znajdującym się w pokoju nr 21.

„... to świadome działanie ASI spowodowane faktem, iż cześć z programów wymaga częstych aktualizacji, co wymaga uprawnień administratora. Zdarzało się, że ASI nie mógł nadzorować lub przeprowadzać ich osobiście. Z tego względu ASI nie ograniczał uprawnień administracyjnych dla użytkowników komputerów...". Zdaniem NIK stwarza to ryzyko dla bezpieczeństwa systemu operacyjnego i danych zawartych na urządzeniu. W takiej konfiguracji ewentualne zainfekowanie złośliwym oprogramowaniem podczas pracy na profilu takiego użytkownika, może zainfekować pliki systemowe, do których użytkownik bez praw administratora nie ma dostępu.

(dowód: akta kontroli str. 102-106, 149-164)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że w Urzędzie wykorzystywano cztery komputery (z 26 poddanych oględzinom) z zainstalowanym systemem operacyjnym Windows XP, mimo że z dniem 8 kwietnia 2014 r. producent oprogramowania zakończył udzielanie wsparcia technicznego dla tego systemu. Z wykorzystaniem jednego z tych urządzeń dokonywano płatności w systemie bankowości elektronicznej. ASI wyjaśnił, że: *„Powodem były koszty. Sama wymiana systemów nie jest opłacalna. Należy wymienić komputery ze starym systemem na nowe z systemem posiadającym wsparcie producenta. Sukcesywnie, co roku Urząd kupował po kilka sztuk nowych komputerów z nowym systemem operacyjnym. W styczniu br. zakupiliśmy sześć sztuk komputerów z nowym systemem. Trwa właśnie wymiana ostatnich komputerów z Windows XP na nowsze. Do końca br. wszystkie komputery z Windows XP maja być wycofane z użytkowania".* (dowód: akta kontroli str. 102-106, 149-164)

Ocena cząstkowa

Urząd, w celu skuteczniejszej ochrony systemów przed nieuprawnionym dostępem, zastosował (w lutym 2017 roku) zabezpieczenie w postaci urządzenia klasy UTM na głównym łączu internetowym, wyposażonego w szereg zaawansowanych funkcji zwiększających bezpieczeństwo. Skuteczność tę obniżało jednak nadanie uprawnień administratora wszystkim użytkownikom systemów operacyjnych komputerów oraz zainstalowanie na czterech (z 26) komputerach systemu operacyjnego, którego producent zakończył udzielanie wsparcia, użytkowanie na pięciu programów niezgodnie z warunkami ich licencji, niezainstalowanie na jednym programu antywirusowego, a na kolejnym nieuaktualnienie bazy sygnatur wirusów. Nie przeprowadzano również okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, mimo takiego wymogu zawartego w § 20 ust. 2 pkt 3 rozporządzenia KRI oraz nie pozbawiono dostępu do systemów zawierających dane osobowe pracownika, z którym rozwiązano stosunek pracy z dniem 1 kwietnia 2016 r.

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[29], wnosi o:

1. Prowadzenie przez ABI rejestru zbiorów danych, stosownie do wymogów art. 36 a ust. 2 pkt 2 ustawy o ochronie danych osobowych oraz zgłaszanie GIODO zmian w zakresie danych gromadzonych w zarejestrowanych zbiorach danych osobowych.
2. Upoważnienie pracowników do przetwarzania danych osobowych we wszystkich zbiorach, w których dane są przez nich przetwarzane i w zakresie niezbędnym do realizowanych przez nich zadań.
3. Przeprowadzanie przez ABI sprawdzenia zgodności przetwarzania danych, o którym mowa w art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych i w § 3 rozporządzenia w sprawie trybu i sposobu realizacji zadań przez administratora bezpieczeństwa informacji oraz opracowywanie przez niego sprawozdań z tych sprawdzeń.
4. Opracowanie i wdrożenie polityki bezpieczeństwa informacji oraz podjęcie działań, wynikających z § 20 ust. 1 i ust. 2 pkt. 1, 2, 3 i 14 rozporządzenia KRI, w zakresie aktualizacji przyjętych regulacji wewnętrznych, utrzymywania aktualności inwentaryzacji

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

sprzętu i oprogramowania służącego do przetwarzania informacji, prowadzenia okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz audytów wewnętrznych z zakresu bezpieczeństwa informacji.

5. Dostosowanie zapisów Polityki bezpieczeństwa do wymogów § 4 pkt 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych i ujęcie w niej wszystkich prowadzonych zbiorów danych osobowych.
6. Dostosowanie wszystkich programów wykorzystywanych do przetwarzania danych osobowych do wymogów określonych w § 7 ust. 3 rozporządzenia w sprawie dokumentacji oraz warunków technicznych.
7. Przestrzeganie przyjętych zasad zabezpieczenia fizycznego danych, w tym w zakresie przechowywania kopii zapasowych baz danych i określenie poziomów bezpieczeństwa, o których mowa w § 6 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, dla przetwarzania danych osobowych w poszczególnych systemach informatycznych.
8. Zapewnienie aktualizacji systemów operacyjnych i programów antywirusowych oraz ograniczenie uprawnień administratora systemu użytkownikom innym niż ASI, w celu zagwarantowania technicznego zabezpieczania danych.

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 26 kwietnia 2017 r.

Paweł Tołwiński
starszy inspektor kontroli państwowej

.....
podpis

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

.....
podpis