NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.023.08.2017
P/17/062

00374618

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	Paweł Tołwiński – specjalista kontroli państwowej, upoważnienie do kontroli nr LBI/159/2017 z 21 listopada 2017 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Urząd Gminy w Milejczycach, ul. Szkolna 5, 17-332 Milejczyce (zwany dalej: „Urzędem")
Kierownik jednostki kontrolowanej	Jerzy Iwanowiec – Wójt Gminy Milejczyce[1] (dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności[2]

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie zapewnienie przez Urząd ochrony elektronicznych zasobów informacyjnych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem[3].

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające m.in. na:

- nadaniu użytkownikom wszystkich komputerów Urzędu uprawnień administratora systemu operacyjnego,
- nieanalizowaniu i niezabezpieczeniu przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów,
- umożliwieniu zdalnego dostępu do zasobów firmom serwisującym składniki systemu bez konieczności autoryzacji i bez nadzoru administratora systemu,
- nieprzestrzeganiu przyjętych zasad i procedur dotyczących tworzenia i przechowywania kopii zapasowych baz danych,
- nieprzeprowadzaniu okresowych analiz utraty integralności, dostępności lub poufności informacji,
- nieprzestrzeganiu wymagań dla stacji roboczych do obsługi SRP ŹRÓDŁO, w zakresie zablokowania dostępu tych urządzeń do Internetu,
- niewywiązaniu się z obowiązków dotyczących utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację oraz przeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji,
- niezgłoszeniu do zarejestrowania Generalnemu Inspektorowi Ochrony Danych Osobowych[4] 17 (z 33) zbiorów danych osobowych oraz niezaktualizowaniu danych rejestracyjnych kolejnych czterech zbiorów,
- nieaktualizowaniu dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ich ochronę,
- nieprowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych oraz niezapewnieniu szkoleń wszystkim pracownikom zaangażowanym w proces przetwarzania informacji.

---

1 Od 16 listopada 2014 r.
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.
4 Dalej: „GIODO".

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 przetwarzania danych wykorzystywano 13 systemów / aplikacji informatycznych, tj.: SRP ŹRÓDŁO[5], SELWIN, EMUiA[6], SIO[7], CEIDG[8], EZD, Kataster OnLine, Księgowanie zobowiązań, Księgowość budżetowa, Płace, Podatki, Program WODA, RejestrVAT. W przypadku pięciu z nich[9], przetwarzanie odbywało po uzyskaniu przez Urząd dostępu od podmiotów prowadzących i administrujących tymi systemami.

W Urzędzie użytkowano 21 komputerów, w tym trzy laptopy. Przetwarzanie danych osobowych odbywało się na 17 z tych urządzeń. Oględziny 20[10] komputerów wykorzystywanych w Urzędzie wykazały, że – poza dwoma urządzeniami (przeznaczonymi do obsługi aplikacji SRP ŹRÓDŁO) – posiadały one stały dostęp do Internetu. Ponadto jeden z komputerów umożliwiających korzystanie z aplikacji SRP ŹRÓDŁO był okresowo (na czas działań podejmowanych przez podmiot serwisujący) podłączany do Internetu, co szerzej opisano w pkt 4.4 niniejszego wystąpienia pokontrolnego.

(dowód: akta kontroli str. 4-21)

1.2. W Urzędzie do 25 stycznia 2018 r. nie wywiązano się obowiązku, o którym mowa 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[11], przeprowadzenia analizy zagrożeń występujących w systemach informatycznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 22-23)

1.3. Według stanu na 25 stycznia 2018 r., 10 (z 11) pracowników Urzędu zaangażowanych było w proces przetwarzania danych osobowych w stopniu adekwatnym do realizowanych zadań, wynikających z ich zakresów obowiązków. Posiadali oni upoważnienia Wójta do przetwarzania danych osobowych w zbiorach, do których mieli dostęp. W jednym przypadku, pracownik został upoważniony i przetwarzał dane w zbiorze CEIDG, mimo że nie wynikało to z jego zakresu obowiązków, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

W okresie objętym kontrolą w Ośrodku nie zachodziły okoliczności (np.: zmiana zakresu obowiązków lub zwolnienie), które wymagałyby dokonywania zmiany uprawnień użytkowników w systemach wykorzystywanych do przetwarzania danych.

(dowód: akta kontroli str. 24-26)

Każdy z pracowników zaangażowanych w przetwarzanie danych w systemach informatycznych Urzędu posiadał własny login i hasło do systemów dziedzinowych zainstalowanych na jednostkach komputerowych, które to systemy wykorzystywano do przetwarzania danych osobowych. Dostęp do każdego z tych urządzeń zabezpieczono hasłem o złożoności odpowiadającej wymaganiom 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[12]. Zmiana hasła była wymuszana w sposób automatyczny. Przyjęte regulacje wewnętrzne nie określały warunków dotyczących złożoności haseł w systemach

---

[5] Aplikacja do obsługi Systemu Rejestrów Państwowych.
[6] Ewidencja Miejscowości Ulic i Adresów.
[7] System Informacji Oświatowej.
[8] Centralna Ewidencja i Informacja o Działalności Gospodarczej.
[9] SRP ŹRÓDŁO, EMUiA, CEIDG, SIO oraz Kataster OnLine.
[10] Jeden z komputerów nie został poddany oględzinom, gdyż był przeznaczonych do przetwarzania informacji niejawnych.
[11] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: „rozporządzeniem KRI".
[12] Dz. U. Nr 100, poz. 1024. Rozporządzenie zwane dalej rozporządzeniem w sprawie dokumentacji oraz warunków technicznych.

informatycznych Urzędu. Określały jedynie katalog haseł (np. imiona osób, nazwy miejscowości), których użycie jest zabronione. Użytkownikom wszystkich 20 komputerów nadano jednak uprawnienia administratora systemu operacyjnego tych urządzeń, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 8-21, 57-70)

1.4. Ustalenia biegłego (powołanego przez NIK) wskazują, że w Urzędzie nie prowadzono papierowej wersji rejestru dostępu do systemów informatycznych wykorzystywanych do przetwarzania danych. Nie opracowano polityki gromadzenia, zabezpieczania i automatycznej analizy logów. Poszczególne elementy sieci generowały i przechowywały logi zgodnie z domyślnymi ustawieniami producenta. Logi związane z pracą systemu nie były analizowane. Logi zapisywane przez poszczególne elementy sieci nie były zabezpieczone przed utratą integralności i zniszczeniem, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 22-23, 71-74)

1.5. Urząd posiadał serwerownię usytuowaną w wyodrębnionym pomieszczeniu, które zabezpieczono przed dostępem osób nieuprawnionych. Umieszczono w niej urządzenia sieciowe, które – jak wskazał biegły – zabezpieczono hasłem, uniemożliwiającym nieautoryzowany dostęp do nich. Regulacje wewnętrzne nie określały warunków korzystania i zabezpieczenia sieci Wi-Fi (taka sieć nie funkcjonowała w Urzędzie).
(dowód: akta kontroli str. 57-79)

1.6. W Urzędzie nie wprowadzono regulacji umożliwiających wykorzystanie przez pracowników prywatnego sprzętu komputerowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych. Konfiguracja sieciowa nie pozwalała na bezpośrednie podłączenie do infrastruktury jednostki sprzętu (laptopy, telefony, tablety) niestanowiącego własności pracodawcy – wszystkie urządzenia działające w sieci musiały posiadać nadany statyczny adres IP. Informacje o podłączeniu do komputerów nośników pamięci (np. pendrive, dysk przenośny) były domyślnie zapisywane w logach systemu komputerowego. Dostęp do zasobów sieciowych uwierzytelniany był na poziomie użytkownika. (dowód: akta kontroli str. 57-79)

W trakcie oględzin nie stwierdzono przypadków podłączenia do sieci Urzędu urządzeń niebędących jego własnością. (dowód: akta kontroli str. 8-21, 75-79)

1.7. Dokumentacja dotycząca zabezpieczenia danych w Urzędzie nie zawierała raportów potwierdzających wystąpienie przypadków naruszenia bezpieczeństwa danych osobowych. Zgodnie z wyjaśnieniami Wójta, w latach 2016 – 2018 (do 25 stycznia) w Urzędzie nie odnotowano przypadków naruszenia bezpieczeństwa systemu informatycznego lub utraty integralności, dostępności lub poufności informacji. Nie wystąpiła również konieczność przywrócenia danych z wykonanych kopii bezpieczeństwa.
(dowód: akta kontroli str. 22-23, 57-70, 80-82)

1.8. W Urzędzie nie wprowadzono regulacji wewnętrznych dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym. Powołany biegły stwierdził, że nie przewidziano zdalnego dostępu do zasobów sieci lokalnej przez pracowników. Zaznaczył jednak, że sieć komputerowa Urzędu oparta została na routerze, który administrowany był przez Urząd Marszałkowski Województwa Podlaskiego. Osoba zajmująca się administrowaniem systemu informatycznego Urzędu nie posiada do niego dostępu. Monitorowanie pracy wspomnianego urządzenia leżało po stronie Urzędu Marszałkowskiego, do sieci którego zestawiono VPN. Ponadto biegły zaznaczył, że obawy budzić może wykorzystanie aplikacji pulpitu zdalnego TeamViewer i VNC, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 57-74)

1.9. Urząd we wszystkich trzech umowach serwisowych obowiązujących w okresie objętym kontrolą i dotyczących oprogramowania komputerowego zawarł regulacje zobowiązujące wykonawców tych usług do zachowania poufności i stosowania zasad określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[13]. Było to zgodne z przepisem § 20 ust. 2 pkt 10 rozporządzenia KRI, w myśl którego w umowach

[13] Dz. U. 2016 r. poz. 922.

serwisowych podpisanych ze stronami trzecimi zawiera się zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji w odniesieniu do danych z jakimi będą mieli styczność w związku z realizowanymi umowami. (dowód: akta kontroli str. 86-92)

1.10. Wszystkie 20 komputerów wchodzących w skład sieci lokalnej było zabezpieczonych dedykowanym do tego celu oprogramowaniem antywirusowym oraz firewallem. Dostęp do sieci lokalnej kontrolowany był przez firewall zainstalowany na routerze CISCO. Badane komputery posiadały aktualne wersje aplikacji zabezpieczających. Biegły stwierdził, że zastosowanie aplikacji bezpieczeństwa, która posiadałaby moduł centralnego zarządzania oprogramowaniem pozwoliłoby na znacznie większą kontrolę nad działaniem systemu. (dowód: akta kontroli str. 8-21, 71-74)

1.11. W okresie objętym kontrolą obowiązywały dwie umowy dotyczące świadczenia na rzecz Urzędu usług poczty elektronicznej. W każdej z nich zawarto zapisy zobowiązujące dostawcę (podmiot zewnętrzny) m.in. do: *„monitorowania i magazynowania zdarzeń serwerowych (logów) ponad standardy przyjęte w tym obszarze"*, zabezpieczania przesyłanych wiadomości protokołem SSL, wykonania i udoskonalania filtrów antyspamowych. Ponadto Urząd posiadał konta poczty elektronicznej na serwerze poczty prowadzonym przez Urząd Marszałkowski Województwa Podlaskiego. Dostęp ten uzyskał w związku z udziałem w projekcie *„Wdrażanie elektronicznych usług dla ludności w województwie podlaskim"*[14]. (dowód: akta kontroli str. 22-23, 93-97)

1.12. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania zostały określone w pkt IV Instrukcji zarządzania systemem informatycznym[15]. Wskazano w nich m.in. że: [1] pełne kopie danych osobowych przetwarzanych w systemach elektronicznych Urzędu wykonywane są automatycznie w systemie po zakończeniu pracy; [2] w odstępie siedmiu dni wykonywany jest zapis najnowszej wersji wszystkich kopii zapasowych na zewnętrzny pozaserwerowy system dyskowy; [3] po upływie 30 dni wykonywana jest pełna kopia danych z wszystkich programów przetwarzających dane osobowe, która poddana jest obróbce kompresji, szyfrowania, przeniesiona na nośnik DVD i składowana w wyznaczonym miejscu (miejsce to nie zostało wskazane); [4] kopie zapasowe przechowywane są w ściśle określony miejscu, które powinno być różne od miejsca przechowywania zbiorów danych poddanych procesowi tworzenia kopii. Ponadto w myśl uregulowań pkt IX Instrukcji zarządzania systemem informatycznym wskazano na konieczność okresowego sprawdzania możliwości odtworzenia danych z kopii zapasowej.

Według stanu na 12 grudnia 2017 r. w Urzędzie nie przestrzegano przyjętych procedur tworzenia kopii zapasowych danych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Wójt Gminy wyjaśnił, że od 1 stycznia 2016 r. do 6 lutego 2018 r. nie wystąpiła w Urzędzie konieczność odtworzenia zbiorów danych ze sporządzanych kopii bezpieczeństwa.
(dowód: akta kontroli str. 57-70, 75-82)

1.13. Biegły stwierdził, że wszyscy pracownicy dysponowali możliwością ściągania aplikacji i plików wykonywalnych oraz posiadali uprawnienia instalowania ich na stacjach komputerowych, do których mieli dostęp, co szerzej opisano w pkt 1.3 wystąpienia pokontrolnego. Oględziny wszystkich 20 komputerów Urzędu, wykazały że na 14 zainstalowano aktualne systemy operacyjne, jeden posiadał system operacyjny, który nie był aktualizowany (komputer wykorzystywany do obsługi aplikacji SRP ŹRÓDŁO), a kolejne pięć działało z wykorzystaniem systemu, dla którego producent zakończył wsparcie techniczne, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Uwagi dotyczące badanej działalności". (dowód: akta kontroli str. 8-21, 71-74)

W Urzędzie nie prowadzono ewidencji programów zainstalowanych na poszczególnych stacjach komputerowych. Wójt wyjaśnił, że: *„Z uwagi na specyfikę pracy w małym Urzędzie na wszystkich stanowiskach pracy zainstalowane są: system operacyjny, program*

---

[14] Projekt nr Z/2/20/I/1.5/9/05 realizowany przez Urząd Marszałkowski Województwa Podlaskiego.

[15] Stanowiącej załącznik nr 4 do zarządzenia nr 5/2012 Wójta Gminy Milejczyce z dnia 16 marca 2012 r. w sprawie ochrony informacji prawnie chronionych przetwarzanych w Urzędzie Gminy Milejczyce. Zarządzenie zwane dalej: „zarządzeniem nr 5/2012 Wójta Gminy Milejczyce z dnia 16 marca 2012 r.".

antywirusowy oraz pakiet biurowy, dodatkowo komputery z księgowości są wyposażone w oprogramowanie narzędziowe. Wszystkie komputery spisane są w inwentaryzacji. Są stosunkowo nowe, a programy od lat nie zmieniają się. Z uwagi na powyższe nie prowadzono takiej ewidencji". (dowód: akta kontroli str. 22-23, 80-82)

1.14. Biegły stwierdził, że systemy operacyjne urządzeń pracujących w sieci LAN były aktualizowane automatycznie, zgodnie z harmonogramem ustawionym domyślnie przez producenta systemów (za wyjątkiem komputerów działających na systemie XP). Bazy zagrożeń aplikacji bezpieczeństwa i oprogramowanie dziedzinowe wykorzystywane do przetwarzania danych osobowych były aktualne. Ich aktualizacja odbywała się automatycznie, zgodnie z harmonogramem założonym przez producentów.
(dowód: akta kontroli str. 71-74)

1.15. W Urzędzie nie wprowadzono wewnętrznych regulacji dotyczących wykonywania płatności (przelewów) drogą elektroniczną. Wszystkie płatności bezgotówkowe Urzędu dokonywanie z pomocą połączenia ustanawianego w programie Home Banking zainstalowanym na jednym z komputerów. Po wprowadzeniu danych dotyczących przelewu, następuje autoryzacja dokonywana przez Wójta oraz Skarbnika (przy użyciu PIN). Przekazanie środków dokonywane jest przez pracownika obsługującego Home Banking po uwierzytelnieniu kodem PIN. (dowód: akta kontroli str. 98)

Ustalone nieprawidłowości

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

1. W Urzędzie do 25 stycznia 2018 r. nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Konieczność przeprowadzania takich analiz wynika z § 20 ust. 2 pkt 3 rozporządzenia KRI i obowiązuje od 31 maja 2012 r. Wójt wyjaśnił, że: *„Wynikało to z ograniczeń w Budżecie Gminy oraz minimalnych środków przeznaczanych na utrzymanie infrastruktury teleinformatycznej oraz trudności z zatrudnieniem osoby posiadającej odpowiednią wiedzę".*
(dowód: akta kontroli str. 21-22, 99-105)

2. Użytkownikom wszystkich 20 komputerów nadano uprawnienia administratora systemu operacyjnego tych urządzeń, mimo że – zgodnie z ich zakresem obowiązków – nie realizowali oni zadań w zakresie administrowania systemami. W wyniku tego, jak ustalił biegły, dysponowali oni możliwością ściągania aplikacji i plików wykonalnych oraz instalowania ich na stacjach komputerowych, do których mieli dostęp. Ponadto według stanu na 25 stycznia 2018 r., jeden (z 11) pracowników Urzędu został upoważniony i przetwarzał dane w zbiorze CEIDG, chociaż nie wynikało to z jego zakresu obowiązków. Powyższe działania były sprzeczne z przepisem § 20 ust. 2 pkt 4 rozporządzenia KRI, zgodnie z którym kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Wójt wyjaśnił, że: *„Wynikało to ze specyfiki pracy w małym urzędzie oraz braku informatyka. Na stanowiskach pracy pracownicy z serwisantami wykonują prace wymagające uprawnień administratora".* Zdaniem biegłego, takie rozwiązania stwarzają znaczne zagrożenie bezpieczeństwa danych. (dowód: akta kontroli str. 8-21, 24-56, 71-74, 99-105)

3. Nie analizowano i nie zabezpieczono przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w Urzędzie. W opinii biegłego poszczególne elementy sieci generowały i przechowywały logi zgodnie z domyślnymi ustawieniami producenta. Informacje te nie były analizowane ani zabezpieczone przez utratą integralności i zniszczeniem. Monitorowanie dostępu do informacji jest – w myśl § 20 ust. 2 pkt 7 lit. a rozporządzenia KRI – jednym z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Wójt wyjaśnił, że: *„Powodem tego są ograniczenia w Budżecie Gminy oraz minimalne*

środki przeznaczone na utrzymanie infrastruktury teleinformatycznej. Realizacja tego zadania wiąże się z dużymi dodatkowymi nakładami".

(dowód: akta kontroli str. 71-74, 99-105)

4. Podmioty serwisujące oprogramowanie Urzędu posiadały możliwość zdalnego dostępu do zasobów sieciowych za pomocą aplikacji TeamViewer i VNC, niewymagających autoryzacji od podmiotu serwisującego – korzystał on z autoryzacji użytkownika, który udostępniał mu pulpit (serwisant pracował na koncie z uprawnieniami użytkownika zalogowanego do systemu) bez nadzoru administratora systemu. Autoryzacja w przypadku wspomnianych aplikacji dotyczyła jedynie nawiązania połączenia (kanału), a nie dostępu do zasobów komputera. 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. Wójt wyjaśnił, że takie rozwiązanie funkcjonowało w Urzędzie, gdyż: *„Uznaliśmy, że skoro prace serwisowe prowadzone są na programach narzędziowych po uprzedniej akceptacji pracownika Urzędu, to taka forma nadzoru i kontroli jest wystarczająca".* (dowód: akta kontroli str. 8-21, 71-74, 99-105)

5. Według stanu na 12 grudnia 2017 r. w Urzędzie nie przestrzegano – przyjętych w pkt IV Instrukcji zarządzania systemem informatycznym – procedur tworzenia kopii zapasowych danych. Między innymi: [1] kopie danych zapisywane były na dysku, który był podłączony na stałe do sieci i znajdował się w serwerowni Urzędu, mimo że zgodnie z regulacjami wewnętrznymi należało je przechowywać w miejscu, które powinno być różne od miejsca przechowywania zbiorów danych poddanych procesowi tworzenia kopii; [2] proces tworzenia kopii obejmował pięć spośród 12 baz danych programów wykorzystywanych do przetwarzania danych, mimo że dla każdego z nich powinny być one wykonywane automatycznie po zakończeniu pracy; [3] wszystkie kopie baz danych znajdowały się na ww. dysku, mimo że co 30 dni powinna być wykonywana pełna kopia danych z wszystkich programów przetwarzających dane osobowe, którą należało poddać obróbce kompresji i szyfrowania oraz przenieść na nośnik DVD. Sposób tworzenia kopii baz danych był ponadto niezgodny z przepisem pkt IV ust. 4 lit. a załącznika do rozporządzenia w sprawie dokumentacji oraz warunków technicznych, zgodnie z którym kopie zapasowe przechowuje się w miejscach zabezpieczających je przed uszkodzeniem lub zniszczeniem. Wójt wyjaśnił, że było to spowodowane brakiem środków na zakup nowych urządzeń oraz ograniczeniami technicznymi infrastruktury informatycznej. (dowód: akta kontroli str. 8-21, 57-74, 99-105)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że na pięciu z 20 komputerów wykorzystywanych w Urzędzie zainstalowane były systemy operacyjne Windows XP, które nie były objęte wsparciem producenta. Zdaniem biegłego, należy wyłączyć z zasobów sieci urządzenia pracujące na od dawna niewspieranym systemie operacyjnym, gdyż ich użytkownie stanowi zagrożenie bezpieczeństwa sieci. (dowód: akta kontroli str. 8-21, 71-74)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie skuteczność przyjętych w Urzędzie 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 osobowych

Opis stanu faktycznego

2.1. Dane w Urzędzie przetwarzane były w 33 zbiorach danych, z których osiem prowadzono w wersji elektronicznej, 25 zaś w formie elektronicznej i papierowej. Do GIODO zostało zgłoszonych 10 zbiorów[16], sześć zbiorów nie podlegało obowiązkowi rejestracji, a kolejne 17 nie zostało zgłoszone, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". W okresie objętym kontrolą Urząd nie

[16] W tym jeden ze zgłoszonych zbiorów – „Ewidencja ludności i dowody osobiste" obejmował sześć zbiorów danych osobowych prowadzonych w Urzędzie, tj.: Rejestr dowodów osobistych, Kartotekę osobową mieszkańców, Rejestr mieszkańców, Rejestr poborowych, Rejestr wyborców, Rejestr zamieszkania cudzoziemców.

dokonywał zgłoszeń rejestracji zbiorów do GIODO i nie wystąpiły przypadki odmowy rejestracji zbiorów danych osobowych. (dowód: akta kontroli str. 5-8, 22-23, 106-107)

2.2. W Urzędzie do 25 stycznia 2018 r. nie skorzystano z możliwości powołania Administratora Bezpieczeństwa Informacji (dalej: „ABI"), o której mowa w art. 36a ust. 1 ustawy o ochronie danych osobowych. Wójt wyjaśnił, że: *„Jako Wójt pracę wykonuję od listopada 2014 roku borykam się z brakiem w zatrudnieniu kompetentnych osób, dlatego powierzenie realizacji obowiązków ABI przy obecnym składzie osobowym Urzędu nie jest możliwe".* (dowód: akta kontroli str. 22-23, 57-70, 99-105)

2.3. W myśl przepisu art. 36b ustawy o ochronie danych osobowych, w przypadku niewyznaczenia ABI, zadania określone w art. 36a ust 2 pkt 1 tej ustawy, z wyłączeniem obowiązku sporządzania sprawozdania, realizuje Administrator Danych Osobowych (dalej: „ADO"). Pomimo to w Urzędzie nie realizowano ww. zadań, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 22-23)

2.4. W Urzędzie, wbrew przepisom art. 39 ust. 1 ustawy o ochronie danych osobowych, nie prowadzono ewidencji osób upoważnionych do przetwarzania danych osobowych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 22-23, 57-70)

Wszyscy pracownicy Urzędu (poza przypadkiem opisanym w pkt 1.3. niniejszego wystąpienia pokontrolnego) posiadali dostęp do zbiorów danych osobowych, w zakresie wynikającym z ich zakresów obowiązków oraz upoważnienia do przetwarzania danych wydanego przez ADO. (dowód: akta kontroli str. 24-25)

Zgodnie z regulacjami wewnętrznymi Urzędu, realizację obowiązku wynikającego z przepisu art. 38 ustawy o ochronie danych osobowych, dotyczącego zapewnienia kontroli na tym jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, powierzono użytkownikom systemów informatycznych wykorzystywanych do przetwarzania danych. W okresie objętym kontrolą regulacje te nie były przestrzegane, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 22-23, 57-70)

2.5. W Urzędzie nie wydawano innych wewnętrznych aktów prawnych, procedur, instrukcji lub poleceń dotyczących sposobu gromadzenia i przetwarzania zasobów informacyjnych, niż Polityka bezpieczeństwa danych osobowych oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych przyjętych zarządzeniem nr 5/2012 Wójta Gminy Milejczyce z dnia 16 marca 2012 r.
(dowód: akta kontroli str. 22-23, 57-70)

2.6. Regulacje wewnętrzne Urzędu nie przewidywały zadań realizowanych przez Administratora Systemów Informatycznych – w okresie objętym kontrolą nie powołano osoby do pełnienia tej funkcji. (dowód: akta kontroli str. 22-23, 57-70)

2.7. W okresie objętym kontrolą w Urzędzie nie przeprowadzano corocznych 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. 22-23)

2.8. Do 25 stycznia 2018 r. żaden z pracowników Urzędu nie uczestniczył w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych oraz bezpieczeństwem informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 22-23)

Wójt Gminy w odniesieniu do zmian przepisów o ochronie danych osobowych, które mają wejść w życie 25 maja 2018 r., w związku z implementacją rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) wyjaśnił, że: *„Zadania, które będziemy mieli obowiązek realizować są nowe i dla tak małego urzędu jak nasz, trudne do wykonania. Zamierzam osobiście*

wziąć udział w kilku spotkaniach oraz szkoleniach, wnikliwie przeanalizować obowiązki i podjąć decyzję dotyczącą realizacji zadań wynikających ze zmiany przepisów dotyczących ochrony danych osobowych, które mają wejść w życie 25 maja 2018 r."
(dowód: akta kontroli str. 80-82)

2.9. Od 1 stycznia 2016 r. do 25 stycznia 2018 r. w Urzędzie nie prowadzono 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. 22-23)

2.10. Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym przyjęte zostały 16 marca 2012 r. Dokumenty te do nie były aktualizowane, mimo takiej konieczności, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 22-23, 57-70)

Polityka bezpieczeństwa określała jedynie środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności, tj. elementy wymagane przepisem § 4 pkt 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych.

W Instrukcji zarzadzania systemem informatycznym zawarto natomiast wszystkie zapisy wymagane przepisem § 5 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, za wyjątkiem określenia sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe.

Dokumenty te nie zawierały natomiast elementów wymaganych przepisem § 4 pkt 1 – 4 oraz § 5 pkt 5 lit. a rozporządzenia w sprawie dokumentacji oraz warunków technicznych, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 57-70, 99-105)

W żadnym z ww. dokumentów nie określono poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych Urzędu, mimo takiego wymogu określonego w § 6 ust. 1 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, a także nie wywiązano się z obowiązku wynikającego z § 2 pkt 15 w związku z § 20 ust. 1 rozporządzenia KRI, wdrożenia regulacji wewnętrznych stanowiących politykę bezpieczeństwa informacji, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 22-23, 57-70)

Ustalone nieprawidłowości

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

1. Do rejestracji przez GIODO nie zgłoszono 17[17] (z 33) zbiorów danych osobowych prowadzonych w Urzędzie (dane rozpoczęto w nich przetwarzać przed 2016 rokiem), co naruszało wymogi art. 40 ustawy o ochronie danych osobowych. Wójt wyjaśnił, że: *„Nie miałem takiej świadomości, że pracownicy nie dokonali zgłoszeń"*. Zgodnie z ww. przepisem obowiązek zgłaszania rejestracji zbiorów danych osobowych spoczywa na ADO, którego zadania wykonywał Wójt. (dowód: akta kontroli str. 5-7, 99-107)
2. W Urzędzie w okresie objętym kontrolą nie realizowano zadań określonych przepisem art. 36a ust 2 pkt 1 ustawy o ochronie danych osobowych (z wyjątkiem obowiązku sporządzania sprawozdania), które – zgodnie z art. 36b tej ustawy – w przypadku niewyznaczenia ABI obowiązany jest realizować ADO. Do zadań tych należało m.in. dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ich ochronę. Wójt Gminy wyjaśnił,

[17] Wśród zbiorów, które nie zgłoszono do rejestracji były m.in.: „Zwrot podatku akcyzowego na paliwo", „Rejestr Vat", „Wnioski do gminnej komisji rozwiązywania problemów alkoholowych", „Ewidencja zezwoleń na sprzedaż napojów alkoholowych", „Gospodarka odpadami komunalnymi", „Podział i rozgraniczenia nieruchomości", „Zezwolenia na zajęcie pasa drogowego prowadzenie robót, umieszczenie urządzeń infrastruktury technicznej", „Wycinka drzew i krzewów", „Sprzedaż nieruchomości, użytkowanie wieczyste", „Decyzje o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia", „Wnioski o nadanie numeru porządkowego", „Gospodarka wodna", „Skargi i wnioski", „Wnioski o udzielenie informacji publicznej", „Oświadczenia majątkowe", „Rejestr sołtysów", „Kancelaria i elektroniczny obieg dokumentów".

że nierealizowanie tych zadań wynikało *„z dużej liczby innych obowiązków oraz braku osób o odpowiedniej wiedzy w zakresie danych osobowych".*

(dowód: akta kontroli str. 22-23, 99-105)

3. Od 25 stycznia 2018 r. w Urzędzie nie prowadzano ewidencji osób upoważnionych do przetwarzania danych osobowych, mimo takiego wymogu określonego w art. 39 ustawy o ochronie danych osobowych oraz określenia zarządzeniem nr 5/2012 Wójta Gminy Milejczyce z 16 marca 2012 r. wzoru tej ewidencji. Wójt wyjaśnił, że: *„Było to wynikiem braku wystarczającej wiedzy w zakresie wymagań dotyczących ochrony danych osobowych. W najbliższym czasie rejestr zostanie wykonany".*

(dowód: akta kontroli str. 22-23, 60, 99-105, 108-118)

4. W Urzędzie nie przestrzegano regulacji określonych w pkt VIII Instrukcji zarządzania systemem informatycznym, dotyczących realizacji obowiązku wynikającego z przepisu art. 38 ustawy o ochronie danych osobowych. Zgodnie z nimi użytkownicy powinni zapisywać w rejestrze informacje o odbiorcach danych osobowych w rozumieniu art. 7 pkt 6 powołanej ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia. Wójt wyjaśnił, że: *„Działania te nie były prowadzone z uwagi na przeoczenie takiego obowiązku wynikającego ze specyfiki naszego Urzędu, gdzie jeden pracownik często realizuje zadania dotyczące wielu różnych dziedzin".*

(dowód: akta kontroli str. 22-23, 57-70, 80-82)

5. W okresie objętym kontrolą w Urzędzie nie przeprowadzano corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, mimo wymogu wynikającego z § 20 ust. 2 pkt. 14 rozporządzenia KRI. Wójt wyjaśnił, że: *„Nie przeprowadzano audytów wewnętrznych z uwagi na brak środków na zlecenie takiej usługi podmiotom zewnętrznym i brak osób o odpowiednich kwalifikacjach w Urzędzie".*

(dowód: akta kontroli str. 22-23, 99-105)

6. Do 25 stycznia 2018 r. żaden z pracowników Urzędu nie uczestniczył w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych. Obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo wynikał z § 20 ust. 2 pkt 6 rozporządzenia KRI. Jak wyjaśnił Wójt, było to wynikiem braku środków finansowych na ten cel. (dowód: akta kontroli str. 22-23, 99-10)

7. Od przyjęcia 16 marca 2012 r. Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym nie były aktualizowane, mimo takiej konieczności wynikającej np. z niepowołania ABI, któremu wskazano do realizacji szereg zadań dotyczących ochrony, zabezpieczenia i kontroli przetwarzania danych. Było to sprzeczne z przepisem § 20 ust. 2 pkt 1 rozporządzenia KRI, zgodnie z którym zapewnia się aktualizację regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Ponadto Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym nie zawierały elementów określonych w § 4 pkt 1 – 4 oraz § 5 pkt 5 lit. a rozporządzenia w sprawie dokumentacji oraz warunków technicznych, tj. m.in.: wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzano dane osobowe (w Polityce bezpieczeństwa wskazano jedynie, że obszar taki należy wyznaczyć), wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, sposobu przepływu danych pomiędzy poszczególnymi systemami, sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe. Wójt wyjaśnił, że: *„Brak tych elementów wynikał z braku aktualizacji Polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym od chwili ich przyjęcia".* Dodał, że: *„Struktura i zadania jednostki nie uległy zmianie, a przy obecnym zatrudnieniu z trudem umożliwia to realizację zapisów w/w. zarządzenia".*

(dowód: akta kontroli str. 22-23, 57-70, 99-105)

8. Regulacje składające się na politykę bezpieczeństwa informacji, określoną w § 2 pkt 15 rozporządzenia KRI nie odpowiadały wymogom § 20 ust. 1 ww. rozporządzenia. W szczególności nie wprowadzono poziomu bezpieczeństwa przetwarzania danych

osobowych w systemie informatycznym Urzędu na poziomie wysokim, czym naruszono wymagania § 6 ust. 1 i 4 rozporządzenia w sprawie dokumentacji oraz warunków technicznych. Wójt wyjaśnił, że: *„W dokumentacji wewnętrznej nie wprowadzono poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym Urzędu z uwagi na przeoczenie wymogów prawnych w tym zakresie".*

(dowód: akta kontroli str. 57-70, 99-105)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie opracowanie i wdrożenie w Urzędzie, dokumentacji i procedur wymaganych przepisami ustawy o ochronie danych osobowych.

3. Sposób przechowywania oraz zabezpieczenia danych

Opis stanu faktycznego

3.1. W Polityce bezpieczeństwa określono środki ochrony służące zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych. Przyjęte rozwiązania w sposób ogólny określały środki ochrony fizycznej, wskazując m.in., że: [1] systemy informatyczne przetwarzające dane osobowe należy umieścić w wydzielonych strefach; [2] należy dbać o fizyczną ochronę kopii zapasowych baz danych, dokumentacji dotyczącej konfiguracji systemów i ich zabezpieczeń; [3] zapewnia się ochronę przed niepowołanym dostępem do urządzeń wchodzących w skład systemu informatycznego; [4] opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych; [5] dostęp do budynków i pomieszczeń, w których przetwarzane są dane osobowe podlega kontroli. (dowód: akta kontroli str. 57-70)

Oględziny pomieszczeń Urzędu, w których przetwarzane były zbiory danych osobowych, wykazały, m.in. że: [1] stacje komputerowe znajdowały się w pomieszczeniach zabezpieczonych zamkami; [2] komputery wykorzystywane do przetwarzania danych wyposażone były w zabezpieczenia na wypadek zaniku napięcia (UPS); [3] kopie zapasowe tworzone były na dysku zewnętrznym znajdującym się w serwerowni oraz na nośniku typu pendrive przechowywanym w metalowej, zamykanej na klucz szafie; [4] we wszystkich pomieszczeniach zainstalowano urządzenia alarmowe; [5] klucze do szaf po zakończeniu pracy przechowywano przez pracowników wykonujących swoje obowiązki służbowe w danych pomieszczeniach; [6] okna nie posiadały zabezpieczeń antywłamaniowych, w tym krat metalowych, za wyjątkiem okien do serwerowni oraz pomieszczeń, w których znajdowały się: kasa, księgowość, urząd stanu cywilnego oraz pracował inspektor ds. obronnych; [7] papierowa forma prowadzonych zbiorów danych osobowych przechowywana była w metalowych szafach posiadających możliwość zamknięcia na klucz; [8] wejście do serwerowni zabezpieczono zamykaną na klucz metalową kratą, w oknach zamontowano metalowe kraty oraz siatkę, a pomieszczenie serwerowni wyposażono w system przeciwpożarowy; [9] urządzenia elektroniczne (serwer, szyna danych, router) umiejscowiono w dedykowanej szafie serwerowej; [10] pomieszczenie archiwum znajdowało się w podpiwniczeniu budynku Urzędu, posiadało system przeciwpożarowy, alarmowy oraz mierzący temperaturę powietrza, akta składowano na półkach.

(dowód: akta kontroli str. 75-79)

3.2. W Urzędzie gromadzono informacje dotyczące sprzętu komputerowego na podstawie okresowych inwentaryzacji majątku Urzędu. Nie posiadano natomiast bieżących informacji w zakresie inwentaryzacji oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości". (dowód: akta kontroli str. 22-23)

3.3. W latach 2016 – 2018 (do 25 stycznia) w Urzędzie nie dokonywano likwidacji sprzętu komputerowego, będącego nośnikiem danych oraz nie wystąpiły przypadki, w których naprawa sprzętu komputerowego była realizowana przez podmioty zewnętrzne. Sprzęt komputerowy przeznaczony do likwidacji był przechowywany w serwerowni Urzędu.

(dowód: akta kontroli str. 22-23, 75-79)

3.4. Niszczenie dokumentów zawierających dane osobowe prowadzone było z wykorzystaniem niszczarki, znajdującej się w jednym z pomieszczeń Urzędu – pokój, w którym umiejscowiono ksero. Przyjęte rozwiązania były zgodne z regulacjami określonym w Polityce bezpieczeństwa. (dowód: akta kontroli str. 57-70, 75-79)

3.5. W Polityce bezpieczeństwa i w Instrukcji zarządzania systemem informatycznym nie określono zasad dotyczących użytkowania komputerów przenośnych i sprzęt taki nie był użytkowany poza siedzibą Urzędu. (dowód: akta kontroli str. 57-74)

3.6. Sprzątanie pomieszczeń, w których przetwarzano dane osobowe odbywało się w godzinach pracy i pod obecność pracowników upoważnionych do przetwarzania danych. W Urzędzie nie wprowadzono regulacji wewnętrznych w tym zakresie.

Zasady gospodarki kluczami do pomieszczeń i szaf, w których przechowywano zbiory danych nie były sformalizowane. Klucze do szaf po zakończeniu pracy były przechowywane przez pracowników wykonujących swoje obowiązki służbowe w danych pomieszczeniach. Klucze do wejścia głównego Urzędu posiadali: Skarbnik Gminy oraz osoba sprzątająca. Drzwi do poszczególnych pomieszczeń Urzędu posiadały możliwość zamknięcia na klucz.
(dowód: akta kontroli str. 22-23, 75-79)

3.7. Procedury dotyczące przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych zostały określone w pkt IX Instrukcji zarządzania systemem informatycznym. Wskazano w nich, że wykonuje się je na bieżąco lub w miarę wystąpienia takich potrzeb. W Urzędzie nie dokumentowano prowadzonych działań w tym zakresie. (dowód: akta kontroli str. 22-23, 57-70)

3.8. Urząd nie posiadał wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania. Nie opracowano także procedur 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". Wójt Gminy wyjaśnił, że: *„Dotychczas nie odnotowano długotrwałych przerw w dostawie energii elektrycznej. UPS przy każdym stanowisku komputerowym są wystarczające przy braku zasilania. Jesteśmy na etapie adaptacji agregatu prądotwórczego".* Jak zaznaczył Wójt, możliwość kilkunastominutowej pracy w przypadku braku energii elektrycznej zapewniały urządzenia typu UPS, w które wyposażone były wszystkie komputery stacjonarne wykorzystywane w Urzędzie.
(dowód: akta kontroli str. 22-23, 57-70, 75-79, 99-105)

3.9. Jak wyjaśnił Wójt, w okresie objętym kontrolą w Urzędzie nie wystąpiły przypadki fizycznej utraty danych. Nie stosowano również procedury postępowania w przypadku naruszenia ochrony danych osobowych, określonej w pkt VII Instrukcji zarządzania systemem informatycznym. (dowód: akta kontroli str. 80-82, 99-105)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość polegającą na niegromadzeniu bieżących informacji w zakresie oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację. Obowiązek gromadzenia tych danych wynikał z § 20 ust. 2 pkt 2 rozporządzenia KRI. Wójt wyjaśnił, że: *„Informacje te nie były gromadzone, gdyż w urzędzie są prowadzone inwentaryzacje roczne sprzętu komputerowego, prawie wszystkie komputery pochodzą z tego samego okresu, a konfiguracje różnią się jedynie oprogramowaniem narzędziowym".* (dowód: akta kontroli str. 22-23, 99-105)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę na potrzebę opracowania wewnętrznych regulacji dotyczących rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych, np. długotrwałego braku zasilania bądź przywracania systemów po awarii, a także planu ciągłości działania umożliwiającego kontynuację wykonywania zadań jednostki. Plan ten powinien określić systemy i aplikacje o znaczeniu krytycznym oraz wszystkie podporządkowane lub powiązane plany. Istotne jest, aby plany te były jasno udokumentowane, przekazane pracownikom i aktualizowane w celu odzwierciedlenia bieżącej działalności Urzędu. Ponadto obowiązek zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej wynikał z regulacji rozdz. A pkt. III załącznika do rozporządzenia w sprawie dokumentacji i warunków technicznych.
(dowód: akta kontroli str. 22-23, 99-105)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonej nieprawidłowości przestrzeganie w Urzędzie przyjętych procedur dotyczących przechowywania i zabezpieczenia danych oraz zapewnienia im właściwej ochrony.

4. Przetwarzanie zasobów informacyjnych zgodnych z zakresem działalności jednostki kontrolowanej

Opis stanu faktycznego

4.1. Dane w Urzędzie przetwarzane były w 33 zbiorach danych, z których osiem prowadzono w wersji elektronicznej, 25 zaś w formie elektronicznej i papierowej. Nie w pełni wywiązano się z obowiązku rejestracji prowadzonych zbiorów do GIODO, co szerzej opisano w pkt 2.1 niniejszego wystąpienia pokontrolnego. W regulacjach wewnętrznych Urzędu nie określono konieczności opracowania wykazu prowadzonych zbiorów danych i taki wykaz nie został sporządzony. (dowód: akta kontroli str. 5-8, 22-23, 106-107)

4.2. W okresie objętym kontrolą Urząd nie aktualizował danych w rejestrze prowadzonym przez GIODO w odniesieniu do zbiorów, które były zarejestrowane, mimo że wystąpiła taka potrzeba (szerzej opisana w pkt 4.3). (dowód: akta kontroli str. 106-107)

4.3. Zakres danych w dziewięciu (z 10) zarejestrowanych zbiorach odpowiadał zakresowi, w jakim były one przetwarzane. W jednym natomiast przypadku był on szerszy niż ujęty w rejestrze GIODO, mimo to Urząd nie zaktualizował danych rejestracyjnych tego zbioru. Ponadto w rejestrze GIODO znajdowały się trzy zbiory danych osobowych (nieprowadzone w Urzędzie), dla których wskazano jako administratora danych Gminę Milejczyce. Brak działań dotyczących aktualizacji danych w rejestrze GIODO szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".
(dowód: akta kontroli str. 106-107)

Analiza wszystkich zbiorów danych prowadzonych w Urzędzie wykazała, że gromadzone w nich dane były wykorzystywane (niezbędne) do realizacji zadań, dla których zbiory te prowadzono. (dowód: akta kontroli str. 106-107)

W latach 2016 – 2018 (do 25 stycznia) Urząd ogłosił jeden konkurs na stanowisko Sekretarza Gminy. W ogłoszeniu wskazano informacje wymagane art. 24 ust. 1 ustawy o ochronie danych osobowych, osoba która złożyła zgłoszenie, wyraziła zgodę na przetwarzanie jej danych osobowych. (dowód: akta kontroli str. 22-23)

4.4. Wójt był ADO zbiorów danych (do których dostęp posiadali pracownicy Urzędu), z wyjątkiem m.in. : SRP ŹRÓDŁO, CEIDG, EMUiA oraz Kataster OnLine, w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych. Urząd uzyskał dostęp do zbioru danych SRP ŹRÓDŁO na podstawie upoważnienia Ministra Spraw Wewnętrznych z 28 listopada 2014 r. Pracownicy Urzędu otrzymali od Wójta wymagane upoważnienia do przetwarzania danych osobowych w tym systemie (informacja o upoważnieniu pracowników została przekazana do Ministerstwa). Urząd nie w pełni realizował wymogi dostępu do tego zbioru danych, gdyż umożliwiał (na jednym z komputerów wykorzystywanych do obsługi SRP ŹRÓDŁO) okresowy dostęp do Internetu, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji „Ustalone nieprawidłowości".

Dostęp do serwisu CEIDG Urząd uzyskał natomiast na podstawie upoważnienia Ministra Rozwoju z 2015 roku. Możliwość przetwarzania danych w serwisie EMUiA została udostępniona w oparciu o porozumienie zawarte z Głównym Geodetą Kraju w 2014 roku. Natomiast możliwość przetwarzania danych w serwisie Kataster OnLine uzyskano na podstawie umowy z 12 listopada 2014 r. w sprawie zasad korzystania z bazy danych ewidencji gruntów, budynków i lokali, zawartej pomiędzy Wójtem Gminy Milejczyce i Starostą Siemiatyckim. (dowód: akta kontroli str. 8-21, 119-125)

Ustalone nieprawidłowości

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

1. Nie zgłoszono do GIODO aktualizacji danych rejestracyjnych czterech zbiorów danych osobowych. Stanowiło to naruszenie przepisu art. 41 ust. 1 pkt 2 i pkt 3 oraz ust. 2 ustawy o ochronie danych osobowych, zgodnie z którym w terminie 30 dni od dokonania zmiany, ADO ma obowiązek zgłosić GIODO zmianę zakresu gromadzonych danych w zbiorze. I tak w doniesieniu do zbioru:

- „Podatki i opłaty lokalne" – aktualizacji wymagał zakres gromadzonych danych w zbiorze, gdyż był on szerszy niż zgłoszony GIODO o: PESEL, NIP, serię i nr dowodu osobistego,
- „Rejestr czytelników Gminnej Biblioteki Publicznej", „Świadczeniobiorcy Gminnego Ośrodka Pomocy Społecznej" oraz „Dodatki mieszkaniowe" – aktualizacji wymagały dane dotyczące administratora danych osobowych tych zbiorów, ponieważ nie były one już prowadzone w Urzędzie (przekazano je do Biblioteki Gminnej[18] i Gminnego Ośrodka Pomocy Społecznej w Milejczycach[19]).

Wójt Gminy wyjaśnił, że: *„Było to wynikiem braku wiedzy o niewykonaniu aktualizacji przez pracowników. Niedopatrzenie to zostanie naprawione".*

(dowód: akta kontroli str. 106-107, 99-105)

2. Jeden z dwóch komputerów wykorzystywanych do obsługi aplikacji SRP ŹRÓDŁO był okresowo (na czas działań podejmowanych przez podmiot serwisujący) podłączany do Internetu. Było to niezgodne z *„Wymaganiami dla stacji roboczych stanowisk obsługi dla użytkowników końcowych SRP"*[20], zgodnie z którymi: *„stacja musi być podłączona do sieci dedykowanej oraz z zablokowanym dostępem do powszechnego Internetu".* Wójt Gminy wyjaśnił, że: *„Dostęp jest krótkotrwały i służy jedynie aktualizacji Selwina, każdorazowy dojazd serwisanta generowałby dodatkowe duże koszty".*

(dowód: akta kontroli str. 8-21, 119-125, 99-105)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości sposób przetwarzania zasobów informacyjnych, który był zgodny z zakresem działalności Urzędu, jednak w odniesieniu do jednego ze zbiorów zewnętrznych nie spełniał podstawowego wymogu związanego z uzyskaniem do niego dostępu.

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[21], wnosi o:

1. Nadanie użytkownikom komputerów uprawnień w systemach operacyjnych odpowiadających ich zakresom obowiązków.
2. Przeprowadzanie okresowych analiz utraty integralności, dostępności lub poufności informacji, o których mowa § 20 ust. 2 pkt 3 rozporządzenia KRI.
3. Zaktualizowanie zakresu obowiązków pracownika przetwarzającego dane w zbiorze CEIDG.
4. Analizowanie i zabezpieczenie przed modyfikacją lub zniszczeniem logów systemów operacyjnych komputerów wykorzystywanych w Urzędzie.
5. Umożliwienie zdalnego dostępu do komputerów firmom serwisującym składniki systemu po uzyskaniu autoryzacji i pod nadzorem administratora systemu.
6. Przestrzeganie przyjętych zasad i procedur dotyczących tworzenia i przechowywania kopii zapasowych baz danych Urzędu oraz sposobu realizacji obowiązku, o którym mowa w art. 38 ustawy o ochronie danych osobowych.
7. Wywiązanie się z obowiązków określonych w art. 36a ust 2 pkt 1 ustawy o ochronie danych osobowych oraz wymogów wskazanych art. 40 i 41 tej ustawy, dotyczących rejestracji i aktualizacji danych w rejestrze prowadzonym przez GIODO.
8. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. Zapewnienie szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI, wszystkim pracownikom zaangażowanym w proces przetwarzania informacji.

---

[18] Dotyczy zbioru „Rejestr czytelników Gminnej Biblioteki Publicznej".

[19] Dotyczy zbiorów: „Świadczeniobiorcy Gminnego Ośrodka Pomocy Społecznej" oraz „Dodatki mieszkaniowe".

[20] Str. 1 pkt 1 „Wymagania sprzętowe" instrukcji: „Wymagania sprzętowe dla stacji roboczych i stanowisk obsługi dla użytkowników końcowych SRP", opracowanej przez Centralny Ośrodek Informatyki – dokument dostępny na stronie: http://plid.obywatel.gov.pl/wp-content/uploads/2014/08/Wymagania-dla-stacji-koncowych-SRP-v-5-0.pdf

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

10. Aktualizację Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym, w tym uzupełnienie ich stosownie do wymogów § 20 ust. 1 rozporządzenia KRI oraz § 4 pkt 1 – 4, § 5 pkt 5 lit. a i w § 6 rozporządzenia w sprawie dokumentacji oraz warunków technicznych, w tym wprowadzenie wysokiego poziomu zabezpieczeń przetwarzania danych osobowych w systemach informatycznych Urzędu oraz wyeliminowanie rozbieżności między postanowieniami tych dokumentów a stanem faktycznym w zakresie dotyczącym ABI.
11. Wywiązywanie się z obowiązków wynikających z § 20 ust. 2 pkt. 2 i 14 rozporządzenia KRI, dotyczących utrzymywania aktualności inwentaryzacji oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację oraz przeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji.
12. Przestrzeganie wymagań dla stacji roboczych do obsługi SRP ŹRÓDŁO w zakresie zablokowania dostępu tych urządzeń do Internetu.

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 lutego 2018 r.

Paweł Tołwiński
specjalista kontroli państwowej

podpis

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

podpis