NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ.410.011.03.2020

Pan
Władysław Diakun
Burmistrz Polic
Urząd Miejski w Policach
ul. Stefana Batorego 3
72-010 Police

WYSTĄPIENIE POKONTROLNE

P/20/004 - Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Urząd Miejski w Policach[1]
ul. Stefana Batorego 3, 72-010 Police.

Kierownik jednostki kontrolowanej

Władysław Diakun, Burmistrz Polic[2] od 19 listopada 1998 r.

Zakres przedmiotowy kontroli

Świadczenie przez urzędy jednostek samorządu terytorialnego e-usług. Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji w urzędzie i ich stosowanie.

Okres objęty kontrolą

Od 1 stycznia 2016 r. do dnia zakończenia kontroli[3].

Podstawa prawna podjęcia kontroli

Artykuł 2 ust. 2 ustawy o NIK ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4].

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Szczecinie.

Kontroler

Tomasz Cyranka główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/112/2020 z 19 czerwca 2020 r.

(akta kontroli str. 1-3)

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

Wdrożone w Urzędzie zasady dotyczące e-usług przyczyniły się do sprawnego i terminowego ich świadczenia. Nie wprowadzono jednak odpowiednich rozwiązań organizacyjnych w zakresie bezpieczeństwa informacji (z wyjątkiem danych osobowych).

W okresie objętym kontrolą w Urzędzie podejmowano działania w celu udostępnienia i upowszechnienia wśród mieszkańców usług świadczonych drogą elektroniczną (e-usług), m.in. poprzez publikowanie na stronie internetowej informacji o sposobach załatwiania spraw drogą elektroniczną i informowanie o możliwościach wykorzystania w tym celu nowego dowodu osobistego z warstwą elektroniczną. Za pośrednictwem ogólnopolskiej platformy ePUAP Urząd udostępnił 25 usług i świadczył za jej pośrednictwem e-usługi dla obywateli. Kierowane do Urzędu elektronicznie sprawy przekazywane były do załatwienia bez zbędnej zwłoki, a w przypadku potrzeby uzupełnienia przedkładanych dokumentów obywatele nie byli wzywani do osobistego stawiennictwa. We wszystkich sprawach, w których wnioskodawcy wyrazili taką wolę, dokumenty przekazano w formie elektronicznej. Zapewniono sprawne i nieprzerwane działanie wykorzystywanego pomocniczo w Urzędzie systemu elektronicznego obiegu dokumentów, poprzez zawarcie stosownych umów asysty technicznej. Zorganizowano szkolenia dla pracowników

[1] Dalej: Urząd.
[2] Dalej: Burmistrz.
[3] Tj. do 23 października 2020 r.
[4] Dz. U. z 2020 r., poz. 1200, dalej: ustawa o NIK.
[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

zaangażowanych w proces przetwarzania informacji. Osobom, które zakończyły zatrudnienie w Urzędzie zablokowano dostęp do systemów informatycznych.

W ocenie NIK działania w zakresie zapewnienia bezpieczeństwa przetwarzania informacji nie były wystarczające. W Urzędzie nie ustanowiono Systemu Zarządzania Bezpieczeństwem Informacji[6]. Obowiązujące w Urzędzie „Polityka Bezpieczeństwa Informacji", „Instrukcja Zarządzania Systemem Informatycznym", a następnie „Polityka ochrony danych osobowych" oraz „Instrukcja eksploatacji systemów informatycznych" dotyczyły bezpieczeństwa danych osobowych. W Urzędzie nie przeprowadzono okresowych audytów wewnętrznych z zakresu bezpieczeństwa informacji, o których mowa w § 20 ust. 2 pkt 14 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7]. Urząd nie posiadał w pełni aktualnych informacji o zasobach informatycznych, w zakresie wymaganym przepisami § 20 ust. 2 pkt 2 ww. rozporządzenia. Nie zablokowano także możliwości zainstalowania nieautoryzowanego oprogramowania użytkownikom systemów informatycznych niebędących pracownikami służb informatycznych.

III. Opis ustalonego stanu faktycznego

OBSZAR

Świadczenie przez urzędy jednostek samorządu terytorialnego e-usług

Opis stanu faktycznego

1. W przyjętym 26 września 2006 r. dokumencie „Strategia Rozwoju dla Gminy Police do 2020" w części Priorytet III jako cel 7 wskazano podjęcie działań umożliwiających obywatelom interaktywne załatwianie spraw urzędowych za pośrednictwem systemów teleinformatycznych. Strategia nie określała terminu wdrożenia tych działań.

(akta kontroli str. 5)

Sekretarz Gminy Police[8] wyjaśniła „*W związku z realizacją ww. celu prowadzona jest strona internetowa Gminy Police oraz Biuletyn Informacji Publicznej Urzędu Miejskiego w Policach, gdzie zawarte są informację dotyczące funkcjonowania Gminy i Urzędu, w tym opisy procedur załatwianych spraw, druki wniosków, informacja o platformie ePUAP, za pośrednictwem której możliwy jest kontakt obywateli i innych podmiotów z Urzędem. Ponadto dla mieszkańców dostępny jest Policki System Informacji Przestrzennej (tzw. geoportal zawierający informacje lokalizacyjne)(…). Aktualnie w trakcie rozstrzygania jest przetarg na wdrożenie zintegrowanych systemów dziedzinowych oraz niezbędnej infrastruktury w Urzędzie Miejskim i jednostkach Gminy Police do świadczenia e-usług publicznych wraz z migracją danych i szkoleniami – ZSMP. W najbliższym czasie zostanie podpisana umowa z wykonawcą na realizację usługi, polegającej na kompleksowej informatyzacji Urzędu i gminnych jednostek organizacyjnych, w tym e-usługi dla mieszkańców.*"

(akta kontroli str. 46-55)

2. Według stanu na 31 maja 2020 r. za pośrednictwem platformy ePUAP[9] Urząd udostępniał mieszkańcom 25 usług w następujących grupach:

[6] Dalej: SZBI.
[7] Dz. U. z 2017 r., poz. 2247,dalej: rozporządzenie KRI.
[8] Dalej: Sekretarz.
[9] Pod adresem: https://epuap.gov.pl/wps/portal/strefa-klienta/katalog-spraw/profil-urzedu/9s49g1knlz

- pismo ogólne, skargi, wnioski, zapytania do urzędu – trzy;
- budownictwo, architektura, urbanistyka – jedną;
- dowody osobiste, meldunki, wybory – sześć;
- gospodarka komunalna – jedną;
- ochrona środowiska – jedną;
- podatki i opłaty – cztery;
- sprawy obywatelskie (dowody osobiste, meldunki, wybory) – sześć;
- urodzenia, małżeństwa, zgony – trzy.

Mieszkańcom Gminy Police udostępniona została także aplikacja[10], umożliwiająca kontakt z Urzędem w celu dokonywania zgłoszeń awarii i szkód, m.in. uszkodzeń nawierzchni, oświetlenia, kanalizacji oraz aplikacja do obsługi Policki Budżetu Obywatelskiego[11], pozwalająca na elektroniczne składanie wniosków oraz głosowanie.

(akta kontroli str. 46-55,186)

3. W okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. poprzez platformę ePUAP do Urzędu wpłynęło 2029 spraw, w tym: 456 spraw od 1 stycznia do 29 lutego 2020 r., 604 sprawy od 1 marca do 30 kwietnia 2020 r. (wzrost o 32%) i 969 spraw od 1 maja do 30 czerwca 2020 r. (wzrost o 60% w porównaniu do dwóch poprzednich miesięcy i o 113% w porównaniu do pierwszych dwóch miesięcy 2020 r.). W okresie marzec/kwiecień i maj/czerwiec, w stosunku do dwóch pierwszych miesięcy 2020 r., istotnie wzrosła liczba następujących e-usług :

- dopisanie do spisu i rejestru wyborców/głosowanie korespondencyjne – wzrost odpowiednio o 850% i 13 250% (z dwóch spraw do 19 i 267);
- zameldowanie na pobyt stały, czasowy – wzrost odpowiednio o 283% i 983% (z sześciu spraw do 23 i 65);
- wniosek o wydanie aktu zgonu/urodzenia, zgłoszenie urodzenia – wzrost odpowiednio o 284% i 356% (z 49 spraw do 188 i 228);
- deklaracja na odpady komunalne – wzrost odpowiednio o 100% i 200% (od braku spraw do jednej i dwóch);
- wniosek o udostępnienie danych osobowych – po spadku o 50%, wzrost o 200% w okresie maj/czerwiec (z dwóch spraw do jednej i sześciu);
- wniosek o wydanie dowodu osobistego – po spadku o 7%, wzrost o 90% w okresie maj/czerwiec (z 54 spraw na 50 i 102).

Brak zainteresowania (poniżej pięciu zrealizowanych usług w półroczu) dotyczył jednej e-usługi dotyczącej „Deklaracji na odpady komunalne". Skarbnik wyjaśniła, iż „brak zainteresowania poszczególnymi e-usługami wynikał przypuszczalnie z chęci załatwiania przez mieszkańców spraw w sposób tradycyjny".

(akta kontroli str. 58-62,187)

4. Poziom wykorzystania e-usług realizowanych poprzez ePUAP nie był objęty przez Urząd monitoringiem. Jak wyjaśniła Skarbnik z powodu nieodnotowania nieprawidłowości w funkcjonowaniu tego systemu oraz braku przepisów prawa, które nakładałyby na gminy taki obowiązek.

(akta kontroli str. 58-62)

5. W kontrolowanym okresie do Urzędu nie wpłynęła żadna skarga dotycząca świadczenia usług publicznych w formie elektronicznej. Nie wpłynęły także wnioski w sprawie usprawnienia tej formy komunikacji.

(akta kontroli str. 46-62)

[10] Pod adresem: https://sip2.police.pl/imap/ oraz w wersji mobilnej
[11] Pod adresem: https://police.budzet-obywatelski.org/

6. Zarządzeniem nr 81/2011 z dnia 14 kwietnia 2011 r. w sprawie systemu wykonywania czynności kancelaryjnych w Urzędzie Miejskim w Policach, Burmistrz wskazał system tradycyjny jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw dla Urzędu.
W Urzędzie nie opracowano procedur obiegu (zarządzania) dokumentami, regulujących komunikację elektroniczną i załatwianie spraw w formie elektronicznej, w tym zobowiązujących pracowników do weryfikacji opatrzenia dokumentów elektronicznych wpływających do Urzędu aktualnym podpisem elektronicznym. Sekretarz wyjaśniła: „(…) Urząd stosuje bezpośrednio przepisy rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 roku w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. Nr 14 poz. 67 z późn. zm.).” W Urzędzie wspomagająco funkcjonował system elektronicznego obiegu dokumentów NIL BPM, zakupiony w 2005 r. W systemie tym występowały następujące etapy obiegu korespondencji:

- wpływ dokumentu do kancelarii (drogą elektroniczną lub tradycyjną);
- w przypadku dokumentu elektronicznego na platformie ePUAP sprawdzenie podpisu, wydrukowanie przysłanych dokumentów oraz Urzędowego Poświadczenia Odbioru;
- opatrzenie datą wpływu, skanowanie do systemu NIL BMP;
- dekretacja na poszczególne wydziały Urzędu i zwrot do kancelarii;
- przesłanie zadekretowanych dokumentów w systemie NIL BMP oraz w wersji papierowej do odpowiednich wydziałów;
- badanie sprawy i przygotowanie rozstrzygnięcia;
- podpisanie rozstrzygnięcia w wersji papierowej lub elektronicznej (w przypadku gdy wnioskodawca chce otrzymać odpowiedź poprzez ePUAP);
- skanowanie dokumentów sprawy do systemu NIL BMP.

System NIL BMP nie komunikował się z innymi systemami informatycznymi Urzędu w zakresie przesyłania danych niezbędnych dla załatwienia sprawy.
Nie wszystkie sprawy były zamieszczane w tym systemie. Burmistrz wyjaśnił: „System NIL BMP jest systemem pomocniczym dla tradycyjnego systemu obiegu dokumentów w Urzędzie Miejskim w Policach. Służy on do ewidencjonowania korespondencji wpływającej do Urzędu, dlatego też w większości przypadków nie są w nim rejestrowane wszystkie czynności związane z przebiegiem załatwienia sprawy”.

(akta kontroli str. 6, 46-55,181-185, 270-272)

Według stanu na 29 czerwca 2020 r. profil zaufany posiadało 11[12] pracowników Urzędu, podpis elektroniczny 25[13] osób.
Dokumenty wysyłane z Urzędu drogą elektroniczną podpisywali m.in.: Burmistrz, Zastępca Burmistrza, Sekretarz Gminy, Zastępca Naczelnika Wydziału i Podinspektor Wydziału.
Łącznie w okresie od 1 stycznia do 29 czerwca 2020 r. podpisano elektronicznie 486 dokumentów.

(akta kontroli str. 45-55)

[12] Zastępca naczelnika Wydziału Organizacyjno–Prawnego, zastępca kierownika Urzędu Stanu Cywilnego, dwie pracownice kancelarii, cztery pracownice Wydziału Finansowo – Budżetowego (w tym zastępca naczelnika Wydziału), dwie pracownice Wydziału Gospodarki Odpadami, jeden pracownik na stanowisku ds. Policki Systemu Informacji Przestrzennej.
[13] Burmistrz i jego zastępcy, skarbnik, sekretarz, pięciu pracowników Wydziału Działalności Gospodarczej, jeden pracownik Wydziału Ochrony Środowiska, jeden pracownik Wydziału Gospodarki Odpadami, jeden pracownik Urzędu Stanu Cywilnego, czterech pracowników Wydziału Organizacyjno–Prawnego, sześciu pracowników Wydziału Spraw Obywatelskich, dwóch pracowników Wydziału Finansowo – Budżetowego.

W dwóch z 20 poddanych badaniu przypadkach[14] rozstrzygnięcia zostały podpisane zarówno w wersji papierowej i elektronicznej. Jak wyjaśniła inspektor w Wydziale Organizacyjno-Prawnym Urzędu, zajmująca się obsługą skrzynki ePUAP, „w aktach sprawy zostały już umieszczone oryginały rozstrzygnięć w wersji papierowej, a nie jak to się praktykuje kopie dokumentów wysłanych elektronicznie".
Przy użyciu platformy ePUAP były wysyłane odpowiedzi podpisane wyłącznie podpisem elektronicznym.

(akta kontroli str. 183-185)

7. W wyniku kontroli 20 spraw, które wpłynęły do Urzędu w formie elektronicznej za pośrednictwem platformy ePUAP[15] stwierdzono, że dekretacja spraw następowała w dniu wpływu dokumentów do Urzędu. W jednym przypadku złożony wniosek wymagał uzupełnienia i drogą elektroniczną wezwano wnioskodawcę do jego uzupełnienia. Wnioskodawcy nie byli wzywani do dostarczania danych/informacji będących już w posiadaniu Urzędu lub innego urzędu administracji publicznej. Urząd nie komunikował się z innymi jednostkami administracji publicznej za pośrednictwem platformy ePUAP w celu uzyskania koniecznych danych/informacji/dokumentów. Dla załatwienia sprawy Urząd korzystał z danych gromadzonych w zewnętrznych rejestrach takich jak: PESEL, ewidencja gruntów i budynków lub Krajowy Rejestr Sądowy. Nie wzywano wnioskodawców do dostarczenia dodatkowych informacji, których Urząd nie posiadał. We wszystkich sprawach, w których wnioskodawcy wyrazili wolę otrzymywania odpowiedzi lub decyzji elektronicznie, dokumenty przekazano w takiej formie.

(akta kontroli str. 183-185)

W Urzędzie nie było możliwości elektronicznego uzyskania informacji na temat aktualnego stanu załatwianej sprawy. Sekretarz wyjaśniła „Takiej możliwości w chwili obecnej nie zapewniają systemy informatyczne, którymi Urząd dysponuje. Rozwiązania te będą możliwe po wdrożeniu kompleksowej informatyzacji Urzędu i gminnych jednostek organizacyjnych (zamówienie jest w trakcie rozstrzygania). Informacje można uzyskać drogą tradycyjną (ustnie, pisemnie, telefonicznie)".

(akta kontroli str. 46-62)

8. W Urzędzie nie opracowano zasad dokonywania zgłoszeń problemów technicznych występujących w funkcjonowaniu platformy ePUAP[16]. Sekretarz wyjaśniła, że takie problemy nie występowały.

(akta kontroli str. 46-55)

9. W związku z funkcjonowaniem w Urzędzie pomocniczego systemu elektronicznego obiegu dokumentów, zawarto umowy serwisowe zapewniające stałe i nieprzerwane działanie systemu oraz usuwanie występujących usterek (umowy zawierane były na okresy roczne i obowiązywały w całym okresie objętym kontrolą). Zapisy umów gwarantowany usunięcie awarii, błędu, usterki w czasie odpowiednio: ośmiu godzin, dwóch dni i pięciu dni. Serwis telefoniczny świadczony był w dni robocze od godziny 9 do 17.

(akta kontroli str. 46-55,123-160)

10. Urząd informował obywateli o możliwości załatwienia spraw drogą elektroniczną na swojej stronie internetowej[17] oraz w Biuletynie Informacji Publicznej. W danych kontaktowych podany był adres ogólny e-mail Urzędu oraz adres skrzynki ePUAP.

[14] Sprawy o nr. 2812/2020 i 6514/2020.
[15] Z zakresu takich obszarów życia publicznego jak: sprawy osobowe (dowód osobisty, meldunki, akty stanu cywilnego, wybory); pismo ogólne, skargi, wnioski, zapytania do urzędu; komunikacja, drogownictwo, transport, geodezja; gospodarka komunalna; podatki i opłaty.
[16] Są one opisane na stronie ePUAP po adresem: https://epuap.gov.pl/wps/portal/strefa-klienta/pomoc
[17] www.police.pl

Umieszczono również wykaz stanowisk wszystkich pracowników Urzędu wraz z ich adresami e-mail. W zakładce „Wykaz wydziałów i spraw" znajdowały się informacje dotyczące trybu załatwienia danej sprawy (tj. wnioski, załączniki, opłaty, czas załatwienia sprawy, sposób składania dokumentów). Na głównej stronie internetowej Urzędu w trakcie kontroli zamieszczono odnośnik do dokumentu znajdującego się na stronie BIP „Sprawy do załatwienia/Elektroniczna skrzynka podawcza" opisującego możliwość dostarczania dokumentów w wersji elektronicznej poprzez ePUAP. Umieszczono informację, że w celu skorzystania z e-usług konieczne jest posiadanie profilu zaufanego[18] wraz z odnośnikiem do strony głównej ePUAP. Nie zamieszczono informacji, że do tego celu może służyć również dowód osobisty z warstwą elektroniczną oraz listy spraw[19] możliwych do załatwienia poprzez ePUAP – podczas kontroli uzupełniono te dane. Przy wydawaniu obywatelom dowodów osobistych z warstwą elektroniczną, pracownicy Urzędu udostępniali ulotkę zawierającą najważniejsze informacje na temat możliwości jego wykorzystania. Ponadto w gablocie obok pomieszczenia, w którym wydawane były dowody osobiste, umieszczono ulotkę z informacjami na temat e-dowodu.

(akta kontroli str. 46-62,188-192)

11. Szkolenie zewnętrze „Podstawowe zadania i zasady ochrony przetwarzanych danych osobowych w świetle nowelizacji UODO i RODO 2018" zostało przeprowadzone 9 maja 2018 r. Dotyczyło ono podstawowych zadań i zasad ochrony przetwarzanych danych osobowych w świetle przeprowadzonej w 2018 r. nowelizacji przepisów dotyczących ochrony danych osobowych, realizowanych przez administratorów danych, użytkowników i kierowników komórek merytorycznych. Szkolenie to obejmowało także aspekty ochrony informacji, zabezpieczenia sprzętu i oprogramowania. Przeszkolonych zostało 144 ze 157 zatrudnionych wówczas w Urzędzie pracowników.
Dwóch pracowników kancelarii Urzędu 24 stycznia 2020 r. uczestniczyło w szkoleniu zewnętrznym „Praktyczne warsztaty korzystania z platformy ePUAP".
Burmistrz wyjaśnił „*W Urzędzie Miejskim w Policach w chwili obecnej nie jest tworzony harmonogram szkoleń. Pracownicy kierowani są na szkolenia na wniosek bezpośrednich przełożonych w zależności od zaistnienia bieżącej potrzeby przeszkolenia pracownika w konkretnym zakresie".*

(akta kontroli str.46-57, 161-180, 270-272)

Zdaniem NIK podnoszenie świadomości zagrożeń i konsekwencji zaistnienia incydentów naruszenia bezpieczeństwa informacji jest istotnym elementem systemu zapewnienia bezpieczeństwa informacji. Szkolenia z tego zakresu powinny być organizowane cyklicznie w związku ze zmieniającymi się zagrożeniami oraz stosowanymi zabezpieczeniami technicznymi i organizacyjnymi, aby dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów naruszenia bezpieczeństwa informacji.

12./13. W okresie od 29 maja 2015 r. do 21 sierpnia 2019 r. w Urzędzie obowiązywała „Polityka Bezpieczeństwa Informacji" i „Instrukcja Zarządzania Systemem Informatycznym", wprowadzone zarządzeniem Burmistrza nr 130/2015, które zostały opracowane w oparciu o normę PN-ISO/IEC 27001:2007 i 17799:2007 w związku z rozporządzeniem 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

[18] Pod adresem: http://bip.police.pl/artykuly/352/elektroniczna-skrzynka-podawcza
[19] Dostępna jest pod adresem: https://epuap.gov.pl/wps/portal/strefa-klienta/katalog-spraw/profil-urzedu/9s49g1knlz

bezpieczeństwa informacji[20] oraz rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych[21], a także zmianami w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[22]. Od 22 sierpnia 2019 r. zarządzeniem Burmistrza nr 217/2019 wprowadzona została w Urzędzie „Polityka ochrony danych osobowych" oraz „Instrukcja eksploatacji systemów informatycznych" i utraciło moc zarządzenie nr 130/2015.
W Urzędzie nie było opracowanego i wdrożonego SZBI, o którym mowa w § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI, co opisano w sekcji „Stwierdzone nieprawidłowości". Obowiązujące w kontrolowanym okresie w Urzędzie „Polityka Bezpieczeństwa Informacji", „Instrukcja Zarządzania Systemem Informatycznym", „Polityka ochrony danych osobowych" oraz „Instrukcja eksploatacji systemów informatycznych" dotyczyły bezpieczeństwa danych osobowych.

(akta kontroli str. 46-62, 63-122, 270-272)

14. W ramach posiadanej przez Urząd Polityki Ochrony Danych Osobowych prowadzone były następujące rejestry i ewidencje dotyczące ochrony danych osobowych:

1) rejestr czynności przetwarzania danych osobowych;
2) rejestr kategorii przetwarzanych danych osobowych;
3) rejestr poleceń – upoważnień do przetwarzania danych osobowych;
4) rejestr umów powierzenia przetwarzania przez podmioty przetwarzające;
5) rejestr upoważnień w związku z usługą serwisową systemu informatycznego;
6) procedura nadawania upoważnień;
7) klauzule stosowane w relacjach z osobami fizycznymi;
8) karty oceny ryzyka;
9) katalog form naruszeń i incydentów w zakresie ochrony danych osobowych;
10) procedura realizacji uprawnień podmiotu danych;
11) rejestr udostępniania danych osobowych;
12) ewidencja naruszeń i procedura postępowania w przypadkach naruszeń;
13) wykaz obszarów przewarzania danych (budynki i pomieszczenia);
14) zasady korzystania z przenośnych urządzeń przetwarzania danych i nośników wymiennych w związku z wymogami dotyczącymi ochrony danych osobowych (uszczegółowienie IESI);
15) instrukcja eksploatacji systemów informatycznych, która przewiduje stosowanie następujących procedur:

a. procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
b. metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
c. procedura rozpoczęcia, zawieszenia oraz zakończenia pracy systemu informatycznego przeznaczona dla użytkowników systemu;
d. procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
e. procedura likwidacji nośników zawierających kopie zapasowe danych po ich wycofaniu na skutek utraty przydatności lub uszkodzenia;
f. procedura postępowania użytkownika na okoliczność zidentyfikowania określonego typu zagrożeń przez program antywirusowy;
g. procedura wykonywania przeglądów i konserwacji systemów;

[20] Dz. U. poz. 745, uchylone z dniem 6 lutego 2019 r.
[21] Dz.U. poz. 719, uchylone z dniem 6 lutego 2019 r.
[22] Dz. U. z 2016 r. poz. 922, ze zm. uchylona z dniem 6 lutego 2019 r.

h. procedura wykonywania przeglądów i konserwacji nośników informacji służących do przetwarzania danych;
i. procedura postępowania w sytuacji naruszenia ochrony danych osobowych.

(akta kontroli str. 45-57, 63-122)

15. W Urzędzie ewidencja sprzętu i oprogramowania prowadzona była: w arkuszu kalkulacyjnym w Wydziale Organizacyjno-Prawnym oraz w oprogramowaniu do ewidencji środków trwałych oraz ewidencji wartości niematerialnych i prawnych w Wydziale Finansowo-Budżetowym.
Oględziny sprzętu informatycznego pod kątem poprawności zapisu w ewidencji prowadzonej w Wydziale Organizacyjno-Prawnym wykazały, że Urząd nie posiadał aktualnych informacji o badanym zasobie informatycznym oraz jego konfiguracji, co zostało opisane w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 46-57,196-266)

16. Pracownicy Urzędu mieli możliwość zainstalowania nieautoryzowanego oprogramowania na użytkowanych przez siebie stanowiskach komputerowych, co zostało opisane w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 267-268)

17. W okresie objętym kontrolą w Urzędzie pracę zakończyło 36 osób. Na podstawie wytypowanej próby dotyczącej 15 byłych pracowników Urzędu ustalono, że ich konta znajdujące się tylko na użytkowanych przez nich komputerach zostały usunięte. Brak było możliwości weryfikacji, kiedy to nastąpiło i kiedy dany pracownik logował się ostatni raz. Uniemożliwiło to sprawdzenie czy cofnięcie lub usunięcie konta następowało niezwłocznie po ustaniu stosunku pracy. W Urzędzie nie były sporządzane wnioski o zamknięcie konta i odebranie uprawnień. Według wyjaśnień informatyków Urzędu, odbywało się to niezwłocznie na podstawie ustnej informacji z Wydziału Kadr. W Urzędzie nie określono terminów i formalnych procedur cofnięcia lub wygaszenia udzielonych upoważnień. Brak sformalizowanych procedur dotyczących przekazywania administratorom systemu informacji o zakończeniu przez pracownika pracy w Urzędzie, może skutkować nieodebraniem mu uprawnień do systemów informatycznych jednostki, pomimo ustania zatrudnienia.

(akta kontroli str. 58-62, 270-272)

18. W Urzędzie w latach 2016-2019 nie prowadzono corocznych audytów z zakresu bezpieczeństwa informacji, co opisano w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 46-62, 270-272)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie ustanowiono SZBI, o którym mowa w § 20 ust. 1 w zw. z ust. 3 rozporządzenia KRI.

(akta kontroli str. 46-122)

Burmistrz wyjaśnił: „Po wejściu w życie przepisów dotyczących danych osobowych RODO wdrożono Politykę Ochrony Danych Osobowych określającą zasady organizacji ochrony danych, środki techniczne ochrony danych, obowiązki w zakresie bezpieczeństwa, wykaz prowadzonej dokumentacji, w związku z § 20 ust. 1 rozporządzenia KRI".

(akta kontroli str. 270-272)

Zdaniem NIK obowiązujące do 21 sierpnia 2019 r. „Polityka Bezpieczeństwa Informacji "i „Instrukcja Zarządzania Systemem Informatycznym" oraz od 22 sierpnia 2019 r. „Polityka ochrony danych osobowych" oraz „Instrukcja eksploatacji

systemów informatycznych" dotyczyły bezpieczeństwa danych osobowych i nie regulowały kompleksowo procesu przetwarzania informacji w Urzędzie.

2. Urząd nie posiadał aktualnych informacji o posiadanych zasobach informatycznych oraz ich konfiguracji, co było niezgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Zgodnie z tym przepisem, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację. Także zgodnie z normą PN-ISO/IEC 27002:2014-12, pkt 8.1.1, wszystkie aktywa powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany spis wszystkich aktywów informatycznych.

Burmistrz wyjaśnił: „Przepis wynikający z § 20 ust. 2 pkt. 2 rozporządzenia KRI nakłada na podmioty publiczne utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania. Inwentaryzacja sprzętu komputerowego wykonywana była na bieżąco przez komisję inwentaryzacyjną. Prowadzona była dodatkowo ewidencja zasobów w arkuszach ewidencyjnych".

(akta kontroli str. 270-272)

Inwentaryzacja prowadzona na podstawie przepisów ustawy z dnia 29 września 1994 r. o rachunkowości[23] nie jest tożsama z inwentaryzacją wskazaną w rozporządzeniu KRI, która rozumiana jest jako stałe posiadanie aktualnych informacji w zakresie nie tylko posiadanego sprzętu informatycznego i oprogramowania, ale również jego konfiguracji. Oznacza to potrzebę prowadzenia rejestru zasobów teleinformatycznych, który zawiera listę wszystkich elementów wykorzystywanych w celu świadczenia usług IT (sprzęt komputerowy, oprogramowanie, urządzenia sieciowe, drukarki, urządzenia peryferyjne, mobilne itp.). Oględziny 10 komputerów, jednego serwera, dwóch laptopów, routera i jednej drukarki przeprowadzone w trakcie kontroli NIK pod kątem poprawności ich zapisu w ewidencji prowadzonej w Wydziale Organizacyjno-Prawnym wykazały, że:
- w jednym przypadku komputer znajdował się w innej lokalizacji niż wykazana w ewidencji;
- w trzech przypadkach była przypisana inna osoba odpowiedzialna, niż faktyczny użytkownik sprzętu;
- w jednym przypadku sprzęt nie został oznaczony numerem ewidencyjnym;
- w pięciu przypadkach sprzęt nie został ujęty w tej ewidencji.

Ponadto jedyną informacją o konfiguracji sprzętu umieszczoną w rejestrze był numer licencji oprogramowania MS Office.

(akta kontroli str. 46-57, 196-266)

3. W Urzędzie nie ograniczono możliwości zainstalowania przez pracowników nieautoryzowanego oprogramowania, pomimo wymogów zapewnienia osobom zaangażowanym w proces przetwarzania informacji stosownych uprawnień w celu zapewnienia bezpieczeństwa informacji, określonych w § 20 ust. 2 pkt 4 rozporządzenia KRI. Także zgodnie z załącznikiem A normy PN-ISO/IEC 27001:2014-12, punkt A.9.2.3 przydzielanie i wykorzystywanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować.

Oględziny jednego z dziesięciu wybranych do badania komputerów wykazały, że użytkownik posiada uprawnienia administratora, które umożliwiały m.in. instalację dowolnego oprogramowania. Informatycy Urzędu oświadczyli, że: „każdy użytkownik posiada uprawnienia administracyjne na użytkowanym przez siebie komputerze

[23] Dz.U. z 2019 r. poz. 351, ze zm.

(pozwalające m.in. na instalowanie oprogramowania). Konieczne jest to w przypadku instalacji oprogramowania niezbędnego na stanowisku pracy. Pracownicy są instruowani o konieczności uzyskania zgody administratora sieci komputerowej na pobranie i instalacje oprogramowania."

(akta kontroli str. 267-268)

Burmistrz wyjaśnił: „W urzędzie trwa wdrożenie Active Directory, do kontrolera domeny sukcesywnie podłączane są nowe stanowiska komputerowe, co w efekcie umożliwi administrowanie prawami użytkowników za jej pośrednictwem. Na chwilę obecną stanowiska w domenie i spoza domeny (wszystkie komputery w Urzędzie) posiadają konfigurację praw użytkowników lokalnych zezwalającą na instalację niezbędnego do pracy na stanowisku oprogramowania. Jednakże instalacja taka wymaga każdorazowo uzyskania zgody administratora sieci komputerowej Urzędu"

(akta kontroli str.270-272)

Posiadanie przez pracowników uprawnień administratora umożliwia zainstalowanie również innego oprogramowania, aniżeli niezbędne na stanowisku pracy. Może to stwarzać ryzyko zainstalowania nieautoryzowanego oprogramowania, np. bez wymaganej licencji albo oprogramowania, które może naruszyć bezpieczeństwo informacji, w szczególności w sytuacji, gdy użytkownicy nie poinformują o tym administratora sieci komputerowej.

4. W Urzędzie w latach 2016-2019 nie prowadzono corocznych audytów z zakresu bezpieczeństwa informacji, co było niezgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że okresowy audyt w zakresie bezpieczeństwa informacji powinien być prowadzony nie rzadziej niż raz na rok.

(akta kontroli str.46-62)

Burmistrz wyjaśnił: „Od 2016 roku Urząd Miejski w Policach prowadzi prace w zakresie koncepcji projektowej: „Integracja i rozbudowa systemów informatycznych do świadczenia e-usług, w celu zrównoważonego rozwoju e-społeczeństwa Miasta Police". Projekt wiąże się z całościową wymianą systemów dziedzinowych i oprogramowania, systemów oraz infrastruktury serwerowej. Audyt z zakresu bezpieczeństwa informacji jest planowany na etap analizy przedwdrożeniowej i zgodności nowych rozwiązań z rozporządzeniem KRI".

(akta kontroli str.270-272)

IV. Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Zapewnienie opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji.
2. Podjęcie działań organizacyjnych w celu zapewnienia prowadzenia i bieżącego aktualizowania ewidencji posiadanych zasobów informatycznych oraz ich konfiguracji.
3. Ograniczenie możliwości instalowania oprogramowania przez pracowników.
4. Zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ust. 1 i 2 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 Szczecinie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 30 od otrzymania wystąpienia pokontrolnego, o sposobie 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.

Szczecin, 4 listopada 2020 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie
Dyrektor

.....
podpis

Kontroler
Tomasz Cyranka
główny specjalista kontroli państwowej

.....
podpis