NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.013.02.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi
ul. Kilińskiego 210, 93-106 Łódź
T + 48 42 239 32 00, F + 48 42 239 32 90
llo@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli Delegatura w Łodzi

Kontrolerzy

Dariusz Nowak, doradca ekonomiczny, upoważnienie do kontroli nr LLO/89/2018 z dnia 14 czerwca 2018 r.

Arkadiusz Kałużny, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr 133 z dnia 07 września 2018 r.

(dowód: akta kontroli str. 1, 390)

Jednostka kontrolowana

Urząd Gminy i Miasta Szadek (dalej „Urząd" lub „UGiM") 98-240 Szadek, ul. Warszawska 3

Kierownik jednostki kontrolowanej

Artur Ławniczak, Burmistrz Gminy i Miasta Szadek

(dowód: akta kontroli str. 2)

Wykaz skrótów i objaśnienie pojęć użytych w wystąpieniu:

- RODO – Rozporządzenie 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)[1];
- rozporządzenie KRI – rozporządzenie 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[2];
- Administrator – zgodnie z definicją zawartą w RODO oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
- Administrator Bezpieczeństwa Informacji, ABI – osoba nadzorująca, z upoważnienia Administratora, przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
- Administrator Systemów Informatycznych, ASI lub Informatyk – osoba odpowiedzialna za funkcjonowanie systemu (-ów) lub sieci informatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci informatycznych;
- incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają prawdopodobieństwo zakłócenia działań biznesowych i zagrażają zachowaniu bezpieczeństwa informacji;

[1] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1. Tekst rozporządzenia dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1527242776060&uri=CELEX:32016R0679.
[2] Dz. U. z 2017 r. poz. 2247.

- Inspektor Ochrony Danych, IOD – wyznaczany w związku z art. 37 RODO. Zasadniczą rolą inspektorów ochrony danych jest doradzanie administratorowi danych i weryfikacja prawidłowości wykonywania obowiązków wynikających z przepisów prawa dotyczących przetwarzania danych;
- Polityka Bezpieczeństwa Informacji, PBI – zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w jednostce;
- System Zarządzania Bezpieczeństwem Informacji, SZBI – system stanowiący cześć całościowego systemu zarządzania, zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

II. Ocena kontrolowanej działalności

Ocena ogólna i jej uzasadnienie

Najwyższa Izba Kontroli ocenia negatywnie[3] działalność Burmistrza w zakresie zarządzania bezpieczeństwem informacji w Urzędzie, pomimo podejmowania działań na rzecz zapewnienia bezpieczeństwa informacji.

W Urzędzie nie zapewniono należytej organizacji bezpieczeństwa informacji oraz nie stosowano wystarczających rozwiązań służących ochronie przetwarzanych danych. W działalności Urzędu stwierdzono szereg nieprawidłowości, w tym m.in.:

- nie opracowano i nie wdrożono kompletnego systemu zarządzania bezpieczeństwem informacji, w szczególności kompletnej polityki bezpieczeństwa informacji, co było niezgodne z § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI,
- wszyscy skontrolowani pracownicy Urzędu (12) stosowali hasła niespełniające wymogów określonych we wprowadzonym od 30 maja 2018 r. Regulaminie ochrony danych osobowych,
- system operacyjny stosowany w Urzędzie nie wymuszał cyklicznej zmiany haseł co 30 dni, co było niezgodne z zapisami ww. Regulaminu,
- nie zapewniono wymaganych rozwiązań w zakresie zabezpieczenia pomieszczenia serwerowni, co było niezgodne z § 20 ust. 2 pkt 9 rozporządzenia KRI,
- w 2017 r. nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że audyt wewnętrzny w zakresie bezpieczeństwa informacji przeprowadza się nie rzadziej niż raz na rok.

W Urzędzie prawidłowo realizowano zadania dotyczące m.in.:

- przeprowadzenia aktualizacji uregulowań wewnętrznych - w zakresie ochrony danych osobowych - pod kątem ich dostosowania do nowych wymogów w związku z wejściem w życie przepisów RODO,
- powołania Inspektora Ochrony Danych i umożliwienia mu realizacji zadań w sposób niezależny, stosownie do art. 37 ust. 1 lit. a RODO,
- zapewnienia, że pracownicy Urzędu uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI,
- prowadzenia inwentaryzacji zasobów informatycznych w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, co było zgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.

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

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1.– 1.2. W Urzędzie nie było opracowanego i wdrożonego kompletnego systemu zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 w zw. z § 20 ust. 3 rozporządzenia KRI (opisano w części *Ustalone nieprawidłowości*).
W okresie objętym kontrolą w Urzędzie obowiązywały dokumenty dotyczące bezpieczeństwa przetwarzania danych osobowych, tj. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, Polityka bezpieczeństwa danych osobowych (przed 30 maja 2018 r.) oraz Polityka ochrony danych osobowych i Regulamin ochrony danych osobowych i Instrukcja sprzętu i oprogramowania (od 30 maja 2018 r.). Zgodnie z wymogami wynikającymi z rozporządzenia KRI, ww. dokumentacja powinna odnosić się do wszystkich danych przetwarzanych w Urzędzie (nie zaś ograniczać do danych osobowych).
Burmistrz Gminy i Miasta Szadek wyjaśnił m.in., że ww. dokumentacja, obowiązująca przed dniem 30 maja 2018 r., została przygotowana oraz wdrożona w oparciu o obowiązujące wówczas przepisy ustawy o ochronie danych osobowych. Przygotowanie ww. dokumentacji powierzono podmiotowi zewnętrznemu, który profesjonalnie zajmował się zagadnieniami związanymi z ochroną danych osobowych. Podjęte działania miały na celu zachowanie należytej staranności przy wdrożeniu polityki ochrony danych osobowych.
Dokumenty te zatwierdzone zostały przez Burmistrza i przedstawione do zapoznania się i stosowania pracownikom Urzędu.
(dowód: akta kontroli str. 3-34, 35-58, 59-75, 113-126, 127-135, 136-182, 183-192, 289, 370-371, 387-389)

1.3. W związku z wejściem w życie RODO w Urzędzie opracowano i wdrożono dokumentację spełniająca wymogi określone w RODO, tj.:

- Politykę ochrony danych osobowych,
- Regulamin ochrony danych osobowych,
- Analizę ryzyka,
- Rejestr czynności przetwarzania,
- Rejestr czynności prowadzonych przez administratora,
- Wykaz podmiotów przetwarzających,
- Wykaz zbiorów danych osobowych,
- Rejestr umów powierzenia,
- ewidencję osób upoważnionych do sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych,
- procedurę audytów,
- procedury przywracania dostępności danych osobowych,
- Instrukcję zarządzania RODO,
- Upoważnienia do przetwarzania danych osobowych oraz Formularz rejestracji incydentu.

Dokumentacja taka została zatwierdzona i zakomunikowana pracownikom Urzędu. Uruchomiono skrzynkę e-mail, służącą do kontaktu z powołanym w Urzędzie IOD.
(dowód: akta kontroli str. 113-126, 127-135, 136-182, 183-192, 289, 370-371)

1.4. Zmian w dokumentacji dotyczącej ochrony danych osobowych dokonano w związku z wprowadzeniem – od 30 maja 2018 r. – zasad określonych w RODO.
(dowód: akta kontroli str. 280-281, 282-287)

W ocenie Kierownika referatu prowadzone były różnego rodzaju działania dla zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym

zmieniającego się otoczenia. W zakresie działań technicznych wprowadzano nowe technologie zapewniające poprawę bezpieczeństwa informacji, jak np. wdrożenie oprogramowania „AXENCE Nvision". W skład działań wchodziły także wszelkiego rodzaju wskazówki dla użytkowników urządzeń narażonych na utratę bądź wyciek danych. Zgodnie z wdrażanymi przepisami, w celu dostosowania do nich infrastruktury, wprowadzano szereg ustawień konfiguracyjnych systemów, mających na celu zwiększenie bezpieczeństwa. Na bieżąco przy użyciu oprogramowania monitorowano wszystkie parametry urządzeń oraz sieci w celu zwiększenia bezpieczeństwa i stabilności funkcjonowania urządzeń.

(dowód: akta kontroli str. 282-287)

1.5. W Urzędzie wyznaczeni zostali pracownicy odpowiedzialni za bezpieczeństwo informacji. Na podstawie zakresów obowiązków oraz stosownych zarządzeń Burmistrza Gminy i Miasta Szadek ustalono, że za poszczególne zadania w badanym okresie (od czerwca 2017 r.) odpowiadali:

- Kierownik referatu - w zakresie spraw związanych z zapewnieniem prawidłowego działania systemów teleinformatycznych. Od 1 czerwca 2017 r. do wyznaczenia IOD pełnił on funkcję Informatyka (ASI) i osoby odpowiedzialnej za bezpieczeństwo sieci. Od 24 lipca 2017 r. wyznaczony został na administratora systemu odpowiedzialnego za funkcjonowanie oraz przestrzeganie zasad i wymagań bezpieczeństwa systemu teleinformacyjnego „ASK" (przetwarzanie informacji niejawnych),
- radca prawny z konsorcjum firm (od 30 maja 2018 r.) – w zakresie ochrony danych osobowych IOD,
- pełnomocnik ds. ochrony informacji niejawnych – wyznaczony na inspektora bezpieczeństwa teleinformatycznego (weryfikacja i kontrola zgodności systemu „ASK" ze szczególnymi wymaganiami bezpieczeństwa oraz kontrola przestrzegania procedur bezpiecznej eksploatacji systemu). Stanowisko ABI pełnił do 10 maja 2018 r.

Powyższe stanowiska podlegały bezpośrednio Burmistrzowi Gminy i Miasta Szadek, który był administratorem danych. W zarządzeniach Burmistrza zostały określone podstawowe zakresy obowiązków na poszczególnych stanowiskach. Wyznaczeni na ww. stanowiska pracownicy posiadali niezbędne kompetencje do pełnienia powierzonych im zadań z zakresu bezpieczeństwa informacji, poparte wykształceniem, praktyką zawodową, szkoleniami i kursami, obejmującymi również problematykę RODO, oraz stosownymi upoważnieniami z Agencji Bezpieczeństwa Wewnętrznego.

(dowód: akta kontroli str. 193-226, 227-236, 296, 297-298, 299)

1.6. Zgodnie z art. 37 ust. 1 lit. a RODO w Urzędzie został wyznaczony IOD. Osoba pełniąca tę funkcję (radca prawny, działający na podstawie zarządzenia Burmistrza Gminy i Miasta Szadek Nr 59/2018 z dnia 30 maja 2018 oraz stosownej umowy) posiadała niezbędne kwalifikacje, wynikające z art. 37 ust. 5 RODO.

(dowód: akta kontroli str. 299)

1.7. W Urzędzie umożliwiono IOD wykonywanie obowiązków w sposób niezależny. W Regulaminie Organizacyjnym Urzędu nie wyodrębniono IOD jako oddzielnego stanowiska. Wskazano natomiast utworzenie samodzielnego stanowiska ds. bezpieczeństwa informatycznego, bez określenia szczegółowych zadań dla tego stanowiska. Zakres zadań IOD został określony natomiast w zarządzeniu Burmistrza Gminy i Miasta Szadek, dotyczącym wyznaczenia pracownika na to stanowisko. Spełniono tym samym wymóg art. 38 ust. 1 RODO. Osoba będąca IOD realizowała także inne zadania, tj. dotyczące obsługi prawnej

UGiM. Wykonywanie tych obowiązków nie wywoływało konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

(dowód: akta kontroli str. 280-281, 299, 305-319, 320-333)

1.8. W ramach wdrożenia dokumentacji w zakresie ochrony danych osobowych (obowiązującej do dnia wprowadzania zmian wynikających z RODO) sporządzono polityki i procedury, określające m.in. szczegółowe zasady wdrożenia zabezpieczeń technicznych:

- Polityka bezpieczeństwa danych osobowych, w ramach której określono m.in. postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych, postepowanie w wypadku klęski żywiołowej lub sytuacji kryzysowych;
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych - uregulowano w niej m.in. przydział uprawnień i identyfikatorów, rejestrowanie i wyrejestrowanie użytkowników, procedury rozpoczęcia, zawieszenia i zakończenia pracy, procedury tworzenia kopii zapasowych, zabezpieczenia systemu informatycznego, wymagania sprzętowe;
- Politykę zarządzania sprzętem i oprogramowaniem komputerowym (uregulowano w niej m.in. sposób inwentaryzacji oprogramowania, audyt wewnętrzny sprzętu i oprogramowania, korzystania ze skrzynek emaliowych);
- zasady zapewnienia ciągłości działania i plan zachowania ciągłości działania - obejmujące: instrukcję przeciwpożarową, instrukcję bezpieczeństwa pożarowego, instrukcję organizacji pracy na Głównym Stanowisku Kierowania Burmistrza w stałej siedzibie i zapasowym miejscu pracy.

Zarządzeniem 58/2018 Burmistrza Gminy i Miasta Szadek z dnia 30 maja 2018 r. w sprawie wdrożenia RODO w UGiM Szadek wprowadzono procedury dostosowujące przyjęte w Urzędzie uregulowania do wymagań RODO w formie m.in.:

- Polityki ochrony danych osobowych,
- Regulaminu ochrony danych osobowych,
- Rejestru czynności przetwarzania danych.

(dowód: akta kontroli str. 3-75, 136, 137, 138-158, 170-174, 175-178, 180-182, 289)

1.9. Regulacje wewnętrzne były dostępne wyłącznie dla osób odpowiedzialnych za realizację poszczególnych czynności wymaganych tymi dokumentami. W zakładce strony internetowej Urzędu dotyczącej ochrony danych osobowych udostępnione zostały informacje wynikające z postanowień art. 13 ust. 1 i 2 RODO.

(dowód: akta kontroli str. 183-192)

1.10. Na podstawie Rejestru czynności przetwarzania danych stwierdzono m.in., że w Urzędzie zidentyfikowano zbiory danych podlegających zabezpieczeniu. Zbiorom tym przypisano odpowiedni poziom ochrony, zgodny z ich wagą. Informacje klasyfikowano z uwzględnieniem wymagań prawnych wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację. Określono w nim kategorię osób, których dane dotyczą, zakres przetwarzania danych, źródło, cel przetworzenia, nazwę systemu/oprogramowania, formę rejestru i podstawę prawną.

(dowód: akta kontroli str. 138-158)

1.11. W wyniku oględzin ustalono, że jednostka posiadała informację o zasobach informatycznych obejmującą ich rodzaj i konfigurację. Prowadzony był elektroniczny rejestr zasobów teleinformatycznych - nazywany bazą konfiguracji, zawierający listę wszystkich elementów, które były zarządzane w celu świadczenia usług IT i informacje, w jaki sposób te elementy są ze sobą powiązane. Zrealizowano tym samym wymogi określone w § 20 ust. 2 pkt 2 rozporządzenia KRI. W jednostce odnotowywano na bieżąco zarówno zmiany zachodzące w posiadanej

infrastrukturze informatycznej jak i w jej konfiguracji, w szczególności wynikające z instalowania lub odinstalowania oprogramowania. Posiadane zasoby informatyczne przypisano do osób, które odpowiadały za dany sprzęt.

(dowód: akta kontroli str. 334-369)

Ustalone nieprawidłowości

W działalności Urzędu w zakresie organizacji bezpieczeństwa informacji stwierdzono następującą nieprawidłowość:

W Urzędzie nie opracowano i nie wdrożono kompletnego systemu zarządzania bezpieczeństwem informacji, w szczególności nie wdrożono kompletnej polityki bezpieczeństwa informacji.
Było to niezgodne z § 20 ust. 1 rozporządzenia KRI stanowiącego, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto, § 20 ust. 3 rozporządzenia KRI wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-EN ISO/IEC 27001[4], a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[5]. W pkt. 5.1 normy PN-EN ISO/IEC 27002 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji.
W wyjaśnieniach Sekretarz Urzędu zdeklarowała zamiar aktualizacji obowiązującej dokumentacji w związku ze stwierdzonymi brakami.

(dowód: akta kontroli str. 113-126, 127-135, 136-182, 183-192, 289, 370-371)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Urzędu w zbadanym zakresie. Ocenę uzasadnia brak opracowania i wdrożenia kompletnego systemu zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 w zw. z § 20 ust. 3 rozporządzenia KRI.

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

Opis stanu faktycznego

2.1. W Polityce zarządzania sprzętem i oprogramowaniem komputerowym zostały określone obowiązki, odpowiedzialność, zasady i ograniczenia dotyczące instalacji i wykorzystania oprogramowania przez pracowników. Na podstawie oględzin 10 komputerów i dwóch laptopów ustalono, że zalogowani do nich użytkownicy nie mieli przyznanych uprawnień administracyjnych, umożliwiających instalację dowolnego oprogramowania. Ponadto, w wykorzystywanym w Urzędzie systemie IT (oprogramowanie umożliwiające centralne zarządzanie tożsamościami i dostępem użytkowników komputerów – AXENCE Nvision) wprowadzono reguły ograniczające możliwość podłączenia do komputerów Urzędu nieautoryzowanych pamięci przenośnych. Powyższe działania były zgodne z wymogami określonymi w § 20 ust. 2 pkt 4 rozporządzenia KRI.

(dowód: akta kontroli str. 59-75, 112, 282-287, 334-369)

2.2. W obowiązujących w Urzędzie w kontrolowanym okresie uregulowaniach wewnętrznych określono zasady nadawania/cofania uprawnień do pracy w systemach informatycznych. Na podstawie badania próby 15 użytkowników

---

[4] Polska Norma PN-EN ISO/IEC 27001:2017 Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.

[5] W tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

systemów informatycznych ustalono, że wszyscy posiadali uprawnienia do pracy w systemach adekwatne do zakresu realizowanych zadań i zgodne z zakresami obowiązków. Powyższe działania spełniały wymogi § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI.

(dowód: akta kontroli str. 3-34, 113-126, 334-369)

2.3. Od czerwca 2017 r. do dnia zakończenia kontroli w Urzędzie rozwiązano stosunek pracy z pięcioma osobami. Na podstawie akt personalnych stwierdzono, że po zakończonej pracy ww. cofnięto uprawnienia do dostępu do danych (w trzech przypadkach), bądź uprawnienia wygasły ze względu na czasowe ich przyznanie (dla dwóch osób). Blokowanie kont odbywało się niezwłocznie po otrzymaniu przez ASI informacji od komórki ds. kadrowych w Urzędzie, co było zgodne z przyjętymi w tym zakresie zasadami.

(dowód: akta kontroli str. 270-279)

2.4. W systemach informatycznych Urzędu w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem wprowadzono zabezpieczenia polegające na konieczności logowania się do systemu (login i hasło). Ponadto do stanowiska przypisany był zakres uprawnień (wynikający z zakresu obowiązków).

Wymogi dotyczące złożoności haseł do systemów informatycznych zostały określone w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz – po 30 maja 2018 r. – w Regulaminie ochrony danych osobowych. W myśl tych zasad, każdy z użytkowników winien stosować hasła o wymaganej złożoności.

W wyniku badania trzech systemów informatycznych ustalono, że używanie przez pracowników hasła o złożoności 8-9 znaków nie spełniały wymogów obowiązującego od dnia 30 maja 2018 r. Regulaminu ochrony danych osobowych (opisano w części *Ustalone nieprawidłowości*). W Regulaminie tym wskazano, że hasła powinny składać się co najmniej z 12 znaków. Ponadto ustalono, że system operacyjny stosowany w Urzędzie nie wymuszał cyklicznej zmiany haseł (miesięcznej), pomimo że w ww. Regulaminie UGiM Szadek ustalono, że hasła muszą być zmieniane co 30 dni.

(dowód: akta kontroli str. 3-34, 127-135, 334-369)

Pracownicy Urzędu nie korzystali z adresów poczty elektronicznej zamieszczonych na komercyjnych serwisach. Urząd dysponował własną domeną, a poczta elektroniczna przechowywana była na zabezpieczonych urządzeniach klienckich.

(dowód: akta kontroli str. 59-75, 131-132, 282-287, 334-369)

2.5. W wyniku oględzin pięciu stanowisk pracy stwierdzono, że na trzech stanowiskach, realizujących zadania z zakresu rejestracji stanu cywilnego, ewidencji ludności oraz wydawania dowodów osobistych, monitory pracowników zostały usytuowane w sposób uniemożliwiający interesantom wgląd do wyświetlanych danych. Powyższe działanie spełniało wymogi § 20 ust. 2 pkt 7 rozporządzenia KRI.

(dowód: akta kontroli str. 334-369)

2.6 Stosownie do § 20 ust. 2 pkt 8 rozporządzenia KRI w Urzędzie ustanowiono zasady umożliwiające bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Pracownicy korzystający ze sprzętu zostali zapoznani z powyższymi uregulowaniami i zobowiązani do ich stosowania.

(dowód: akta kontroli str. 3-34, 177)

Kierownik referatu wyjaśnił, że urządzenia mobilne nie były wykorzystywane poza terenem budynku UGiM Szadek.

(dowód: akta kontroli str. 282-287)

2.7. Dane zgromadzone na urządzeniach mobilnych były zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym. W Urzędzie uregulowano zasady używania urządzeń lub nośników zawierające dane osobowe. Laptopy użytkowane były na terenie Urzędu i przechowywane w monitorowanych oraz zabezpieczonych kratami pomieszczeniach.

(dowód: akta kontroli str. 3-34, 127-134, 177, 334-369)

2.8. Zabezpieczenie serwerowni polegało m.in. na umiejscowieniu jej w innym niż Urząd budynku, bez oznakowania lokalu przeznaczonego do tego celu, zastosowaniu zamków patentowych. Klucze do tego pomieszczenia były niedostępne dla osób postronnych. Część zastosowanych rozwiązań służących zabezpieczeniu serwerowni w niewystarczającym stopniu chroniła pomieszczenie (opisano w części *Ustalone nieprawidłowości*).
W okresie objętym kontrolą testowano lub serwisowano znajdujące się w pomieszczeniu zasilacze awaryjne, klimatyzator i czujnik sygnalizacji pożaru.
W serwerowni zapewniono rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwerów i urządzeń sieciowych.

(dowód: akta kontroli str. 170-181, 334-369)

2.9. Na podstawie analizy umów serwisowych zawieranych z podmiotami zewnętrznymi (sześciu z siedmiu) ustalono, że zamieszczano w nich – zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI – zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.

(dowód: akta kontroli str. 76-111)

2.10. W Urzędzie zostały określone zasady dotyczące postępowania w przypadku przekazywania sprzętu teleinformatycznego poza jednostkę, np. w celu wykonania napraw.
W Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wskazano, że prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania firm zewnętrznych odbywają się za wiedzą ABI, przez uprawnionych przedstawicieli tych firm, pod nadzorem informatyka. Przed przekazaniem sprzętu przewidziano m.in. usuwanie danych, bądź uszkadzanie lub niszczenie nośników w sposób uniemożliwiający odzyskanie danych.

(dowód: akta kontroli str. 3-34, 175, 177)

2.11. Zgodnie z § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI w Urzędzie przeprowadzano aktualizację systemów operacyjnych. Nie stwierdzono wykorzystywania systemów operacyjnych nieobjętych wsparciem producenta (np. *Windows XP*).

(dowód: akta kontroli str. 282-287, 334-369)

2.12. Zasady dotyczące tworzenia i przechowywania kopii zapasowych danych w Urzędzie zostały określone w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, a następnie w dokumentacji przyjętej w związku z wprowadzeniem RODO. Ustalono, że kopie wszystkich komputerów i serwerów oraz baz danych były wykonywane zgodnie z przyjętymi regulacjami. Proces tworzenia kopii został zautomatyzowany poprzez zastosowanie systemu informatycznego i skryptów. Kopie były przechowywane w jednej z szaf w serwerowni oraz w dwóch lokalizacjach poza serwerownią. Dostęp do tych pomieszczeń został ograniczony, tj. zastosowano zabezpieczenia fizyczne i ograniczenie osób uprawnionych do wstępu/pobrania kopii. W Instrukcji nie określono zasad testowania kopii zapasowych. Określono jedynie, że Informatyk odpowiada za sprawdzanie poprawności wykonania kopii zapasowych na nośnik zewnętrzy. W wyniku kontroli ustalono, że w tym zakresie wykorzystywano

oprogramowanie do weryfikacji poprawności procesu tworzenia kopii komputerów/serwerów oraz że Informatyk weryfikował na bieżąco utworzone kopie. W okresie objętym kontrolą nie wystąpiły przypadki konieczności odtworzenia danych z kopii zapasowych.
Przyjęte rozwiązania i działania w ww. zakresie zapewniały zgodność z wymogami określonymi w § 20 ust. 2 pkt 7 oraz ust. 2 pkt 12 lit. b i e rozporządzenia KRI.
(dowód: akta kontroli str. 3-34, 172-173)

2.13. Na podstawie oględzin 10 komputerów ustalono, że był na nich zainstalowany i uruchomiony program antywirusowy, który wykorzystywał aktualną na moment badania wersję bazy definicji wirusów. Było to zgodne z § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI.
Kierownik referatu wyjaśnił, że w Urzędzie stosowano dwa oprogramowania antywirusowe zabezpieczające przed szkodliwym oprogramowaniem - jedno zintegrowane z systemem operacyjnym, drugie dedykowane, zakupione przez Urząd.
(dowód: akta kontroli str. 282-287, 334-369)

2.14. W ramach obowiązujących w Urzędzie uregulowań nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerach Urzędu. Ustalono jednak, że stosownie do zalecenia sformułowanego w pkt A.12.1.3 załącznika A normy PN-ISO/IEC 27001:2017, pojemność przestrzeni dyskowej w serwerach była na bieżąco monitorowana przez Informatyka. Określono próg ostrzegawczy na poziomie około 80% zajętości przestrzeni oraz wdrożono narzędzie do automatycznego monitorowania pojemności dwóch macierzy dyskowych, służących do przechowywania kopii zapasowych.
(dowód: akta kontroli str. 282-287, 334-369)

2.15. W uregulowaniach Urzędu z zakresu bezpieczeństwa informacji zostały uwzględnione działania związane z zarządzaniem zmianami w wykorzystywanym oprogramowaniu. W rozdziałach od VII do IX Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, zostały określone: procedury wykonywania przeglądów i konserwacji systemów informatycznych, zasady sprawdzania poprawności działania programów i narzędzi programowych m.in. w wyniku zmian oprogramowania, sprzętu i konfiguracji oraz testowania zmian. Analogiczne rozwiązania przyjęto w dokumentacji przyjętej w związku z wejściem RODO.
(dowód: akta kontroli str. 3-34, 175)

2.16. Stosownie do art. 30 RODO, IOD sporządził i prowadził rejestr czynności przetwarzania, który zawierał informacje wymagane powołanym przepisem.
(dowód: akta kontroli str. 138-158)

Ustalone nieprawidłowości

W działalności Urzędu w zakresie wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji, stwierdzono następujące nieprawidłowości:

1. Na wszystkich poddanych oględzinom komputerach (12) pracownicy Urzędu stosowali hasła niespełniające wymogów określonych w punkcie 3 Regulaminu ochrony danych osobowych w zakresie liczby znaków w haśle. W Regulaminie tym przewidziano m.in., że hasła powinny składać się co najmniej z 12 znaków. W wyniku oględzin stwierdzono natomiast używanie przez 12 pracowników haseł o długości 8-9 znaków. Ponadto, wbrew zasadzie określonej w ww. Regulaminie, system operacyjny stosowany w Urzędzie nie wymuszał cyklicznej zmiany haseł (co 30 dni).

Kierownik referatu wyjaśnił m.in., że trwają prace nad wdrożeniem stosownego rozwiązania w ciągu najbliższego miesiąca. Ponadto wskazał, że w programach z dostępem z poziomu administratora przestrzegano, aby hasła były zmieniane minimum co 30 dni, i zapewniały określony stopień bezpieczeństwa. Dodatkowo dane z najważniejszych programów szyfrowano i zabezpieczono dodatkowym hasłem. Dostęp do tego typu plików miał tylko administrator sieci.

(dowód: akta kontroli str. 127-134, 282-287, 334-369)

2. Przyjęte w Urzędzie rozwiązania służące zabezpieczeniu serwerowni w niewystarczającym stopniu chroniły to pomieszczenie oraz serwer. Stanowiło to naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI.
Burmistrz Gminy i Miasta Szadek wyjaśnił m.in., że zainstalowanie niektórych zabezpieczeń nie było zrealizowane ze względu na planowany kompleksowy remont budynku. Ze względu na racjonalność wydatkowania środków publicznych realizacja zabezpieczeń przed remontem nie była w pełni uzasadniona.

(dowód: akta kontroli str. 334-369, 387-389)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działalność kontrolowanej jednostki w zbadanym zakresie.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Urzędzie w okresie objętym kontrolą przeprowadzono analizę ryzyka utraty integralności, dostępności i poufności informacji, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI. W jej wyniku dokonano identyfikacji, analizy oraz oceny ryzyka, w tym określono jego poziom oraz sposób postępowania w poszczególnych przypadkach.

(dowód akta kontroli str. 159-168)

W Polityce bezpieczeństwa danych osobowych został nałożony na odpowiednie osoby obowiązek identyfikacji ewentualnych zagrożeń i przedkładania – do ABI – projektów i propozycji rozwiązań celem zabezpieczenia przed naruszeniem ochrony danych osobowych (§ 8 ust. 3).

(dowód: akta kontroli str. 35-58)

W obowiązującej od 30 maja 2018 r. Polityce ochrony danych osobowych (pkt. 2) prowadzenie analizy ryzyka powierzono Administratorowi. Ocena skutków miała być wykonana z udziałem IOD. W Polityce (pkt. 2.3) określono procedurę przeprowadzenia analizy ryzyka związanego z bezpieczeństwem danych osobowych (opisując zagrożenia, skutki wystąpienia incydentu, zabezpieczenia). W metodyce określono także:
- aktywa informacyjne Urzędu,
- podatności i potencjalne zagrożenia,
- zidentyfikowane ryzyka,
- ocenę ryzyka,
- sposoby reakcji na ryzyka,
- plany postępowania z ryzykiem.

(dowód: akta kontroli str. 113-126)

3.2. Celem realizacji postanowień określonych w § 20 ust. 2 pkt 13 rozporządzenia KRI, w Polityce bezpieczeństwa danych osobowych przewidziano sposób postępowania na wypadek naruszenia lub podejrzenia naruszenia ochrony danych osobowych. Również w Polityce ochrony danych osobowych została opracowana metodyka postępowania w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji. Pracownicy Urzędu zostali

zapoznani z zasadami RODO i zobowiązani do stosowania postanowień w tym zakresie.

(dowód: akta kontroli str. 35-58, 127-134)

Zgodnie z ww. postanowieniami, w Urzędzie był prowadzony rejestr incydentów. W okresie objętym kontrolą (po wprowadzeniu RODO) zostało w nim zarejestrowane sześć zdarzeń dotyczących naruszeń bezpieczeństwa informacji.

(dowód: akta kontroli str. 169)

3.3. Stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI, w obowiązujących w kontrolowanym okresie uregulowaniach wewnętrznych określono wymogi dotyczące realizacji szkoleń z zakresu bezpieczeństwa informacji. Szkolenia organizowano w miarę potrzeb i zależnie od zmieniających się uregulowań prawnych.
W okresie objętym kontrolą zorganizowano dwukrotnie (w styczniu 2017 r. i maju 2018 r.) szkolenia wewnętrzne dla pracowników w zakresie obowiązujących przepisów dotyczących bezpieczeństwa informacji, bezpiecznej pracy w systemach informatycznych, ochrony danych i budynków, a także przepisów RODO. Szkolenia były prowadzone przez ABI lub firmy zewnętrzne. Z zakresu bezpieczeństwa informacji zostali przeszkoleni wszyscy pracownicy Urzędu. Każdy pracownik składał stosowne oświadczenie o zaznajomieniu z przepisami i uregulowaniami dotyczącymi ochrony danych.
W okresie objętym kontrolą ABI, Sekretarz Gminy i Miasta Szadek i Pełnomocnik ds. informacji niejawnych uczestniczyli indywidualnie w szkoleniach zewnętrznych, obejmujących szczegółowe zagadnienia związane z wejściem w życie RODO lub bezpieczeństwem teleinformatycznym. Ponadto Sekretarz posiadała ukończone studia podyplomowe z ww. zakresu, ABI posiadał potwierdzenie bezpieczeństwa, dokument ukończenia szkolenia w zakresie ochrony informacji niejawnych oraz szkolenia w zakresie ww. informacji w systemie teleinformatycznym.
Na portalu internetowym Urzędu opublikowano materiały informacyjne z zakresu ochrony danych osobowych.

(dowód: akta kontroli str. 3-35, 113-126, 183-192, 193-226)

3.4. Zarządzeniem Nr 26/2017 z dnia 22 marca 2017 r. Burmistrza Gminy i Miasta Szadek wprowadzony został harmonogram przeprowadzenia audytu i kontroli w jednostkach organizacyjnych Urzędu, w tym UGiM. Pracownicy mieli działać na podstawie pisemnych upoważnień, a wykonanie zadania powierzono Sekretarzowi Gminy i Miasta Szadek. W wyniku kontroli ustalono, że w okresie objętym kontrolą nie wystawiono upoważnień w ww. zakresie, nie przedłożono dokumentów w postaci protokołów kontroli lub wniosków oraz zaleceń mających na celu eliminacje zagrożeń bądź też wskazujących na konieczność zmiany przepisów wewnętrznych (opisano w części *Ustalone nieprawidłowości*). Stosownie do zasad określonych w Polityce bezpieczeństwa danych osobowych (rozdział IV), ABI sprawował nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych osobowych, a z kontroli należało sporządzić protokoły, które przechowuje ABI.

(dowód: akta kontroli str. 35-58, 303-304)

3.5. W związku z wejściem w życie przepisów RODO w Urzędzie dokonano analizy procesów przetwarzania danych osobowych i oceny stopnia zapewnienia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk – zgodnie z wymogami art. 32 ust. 1 RODO.

(dowód: akta kontroli str. 159-168)

3.6. W związku z wejściem w życie RODO w Urzędzie zapewniono szkolenie w tym zakresie dla wszystkich pracowników w dniu 24 maja 2018 r. (na liście

podpisało się 25 z 27 osób, pozostałe dwie osoby złożyły oświadczenia o zapoznaniu się z obowiązującymi zasadami).

(dowód: akta kontroli str. 183-192)

Ustalone nieprawidłowości

W działalności Urzędu w zakresie podejmowanych działań w celu zapobiegania incydentom bezpieczeństwa informacji stwierdzono następującą nieprawidłowość:

W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI oraz zarządzeniem Nr 26/2017 Burmistrza Gminy i Miasta Szadek z dnia 22 marca 2017 r. w sprawie audytu i monitoringu systemów teleinformatycznych w zakresie bezpieczeństwa informacji.
Sekretarz UGiM wyjaśniła m.in., że audytu i kontroli systemów dokonał zgodnie z harmonogramem informatyk Urzędu, który zawsze zajmował się kontrolą informatyczną w Urzędzie i jednostkach. W związku z tym nie udzielono mu osobnego upoważnienia. Wynikłe nieprawidłowości polegające na technicznych usterkach usuwano na bieżąco. Ze względu na bardzo duże obciążenie pracą oraz bieżące naprawy, aktualizacje, nie zostały sporządzone protokoły z przeprowadzonej kontroli. Taka sytuacja wystąpiła jednorazowo i już nie będzie miała miejsca.
Najwyższa Izba Kontroli nie podziela stanowiska przedstawionego w wyjaśnieniach i wskazuje, że tego rodzaju czynności wykonywanych przez Informatyka Urzędu nie można uznać za audyt, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI. Audyt jest niezależną działalnością doradczą i weryfikacyjną, której celem jest usprawnienie działania jednostki. Przeprowadzanych przez Informatyka Urzędu czynności nie można zatem uznać za audyt, ponieważ jest on osobą bezpośrednio zaangażowaną w zarządzanie środowiskiem informatycznym Urzędu, które podlegało sprawdzeniu, więc nie został zachowany atrybut niezależności osoby wykonującej czynności sprawdzające.

(dowód: akta kontroli str. 65, 280-287, 288, 303-304)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Burmistrza w zakresie zapobiegania incydentom bezpieczeństwa informacji, ze względu na nieprzeprowadzenie w 2017 r. audytu bezpieczeństwa informacji.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[6], wnosi o:

1. Opracowanie i wdrożenie kompletnego systemu zarządzania bezpieczeństwem informacji uwzględniającego zalecenia normy PN-EN ISO/IEC 27001 i norm z nią związanych (PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, PN-EN ISO/IEC 24762).
2. Wdrożenie rozwiązań zapewniających odpowiednie zabezpieczenie pomieszczenia serwerowni.
3. Zapewnienie prowadzenia co najmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji.
4. Stosowanie haseł dostępu do systemów informatycznych zgodnych z zasadami określonymi w polityce haseł oraz wdrożenie rozwiązań wymuszających cykliczną zmianę haseł w odpowiednich odstępach czasu.

[6] Dz. U. z 2017 r., poz. 524, ze zm.

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 Łodzi.

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.

Łódź, dnia 14 września 2018 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Arkadiusz Kałużny
Starszy inspektor k. p.

podpis

Dyrektor
Przemysław Szewczyk

podpis