NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.005.02.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 53 08, F +48 22 444 52 52
kap@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontroler	Bartosz Tajer, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/56/2018 z 28 maja 2018 r. (dowód: akta kontroli str. 1)
Jednostka kontrolowana	Urząd Miasta i Gminy Góra Kalwaria, ul. 3 Maja 10, 05-530 Góra Kalwaria (dalej: Urząd)
Kierownik jednostki kontrolowanej	Dariusz Zieliński, Burmistrz Miasta i Gminy Góra Kalwaria (dalej: Burmistrz) (dowód: akta kontroli str. 2-3)
Okres objęty kontrolą	Od 1 czerwca 2017 r. do dnia zakończenia czynności kontrolnych w jednostce, tj. do 13 lipca 2018 r.

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 danych osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;

Administrator Systemów Informatycznych, ASI – osoba odpowiedzialna za funkcjonowanie systemu (-ów) lub sieci informatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci informatycznych;

aktywa informacyjne – zidentyfikowane zbiory danych Urzędu;

aktywa informatyczne – oprogramowanie, dane, sprzęt, dokumentacja, zasoby administracyjne fizyczne, komunikacyjne lub ludzkie związane z działalnością informatyczną Urzędu;

dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą);

---

[1] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1, ze zm. 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.

incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają prawdopodobieństwo zakłócenia działań Urzędu i zagrażają zachowaniu bezpieczeństwa informacji;

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;

podatność – słabość aktywów, która może być wykorzystana przez zagrożenia;

Polityka Bezpieczeństwa Informacji, PBI – zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w jednostce;

przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

ryzyko – jest scenariuszem opisującym zdarzenie i jego konsekwencje;

ryzyko związane z bezpieczeństwem informacji – potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów, powodując w ten sposób szkodę dla organizacji. Ryzyko mierzone jest jako kombinacja prawdopodobieństwa zdarzenia i jego wpływu;

System Zarządzania Bezpieczeństwem Informacji, SZBI – cześć całościowego systemu zarządzania, oparta na podejściu wynikającym ze zidentyfikowanego ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji;

zagrożenie bezpieczeństwa informacji – potencjalna przyczyna zdarzenia, incydentu naruszenia bezpieczeństwa informacji, którego skutkiem może być szkoda (strata) dla organizacji;

zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działania podejmowane w Urzędzie w zakresie zarządzania bezpieczeństwem informacji. Powyższą ocenę uzasadnia fakt, że pomimo przyjęcia i wdrożenia rozwiązań organizacyjno-technicznych w celu zapewnienia bezpieczeństwa informacji, w działalności Urzędu stwierdzono nieprawidłowości, które w ocenie NIK wpływały na zapewnienie bezpieczeństwa informacji.

Uzasadnienie oceny ogólnej

Pozytywnie należy ocenić, że w Urzędzie została opracowana dokumentacja składająca się na System Zarządzania Bezpieczeństwem Informacji, w tym Polityka Bezpieczeństwa Informacji oraz szczegółowe procedury i instrukcje. Pracownicy

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

Urzędu zostali zapoznani z obowiązującymi w Urzędzie wymogami w zakresie bezpieczeństwa informacji. Burmistrz, zgodnie z wymogami określonymi w RODO, powołał Inspektora Ochrony Danych i umożliwił mu realizację zadań w sposób niezależny. Osoba pełniąca tę funkcję, a także inni pracownicy odpowiedzialni za bezpieczeństwo informacji, posiadali odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. Komputery Urzędu zostały zabezpieczone przed szkodliwym oprogramowaniem oraz możliwością instalowania dowolnego oprogramowania przez użytkowników. Prowadzono aktualizację oprogramowania systemowego oraz sporządzano i weryfikowano prawidłowość kopii zapasowych. Spełniono również wymóg przechowywania kopii poza miejscem ich wytwarzania. W okresie objętym kontrolą przeprowadzono przegląd części dokumentacji SZBI, jednak w ocenie NIK, dokumentacja Urzędu wymaga dalszej aktualizacji, na co wskazują ustalenia kontroli oraz ujawnione w wyniku kontroli nieprawidłowości.

Stwierdzone nieprawidłowości polegały w szczególności na:
- nieprzeprowadzeniu w 2017 r. audytu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI;
- nieprzeprowadzeniu oceny procesów przetwarzania danych w Urzędzie, o której mowa w art. 32 RODO;
- braku aktualizacji obowiązującej w Urzędzie *Polityki bezpieczeństwa danych osobowych Urzędu Miasta i Gminy Góra Kalwaria*[4] pod kątem dostosowania do nowych wymogów w zakresie ochrony danych osobowych wynikających z przepisów RODO;
- nieuregulowaniu zasad i procedur korzystania przez pracowników ze sprzętu i urządzeń przenośnych Urzędu poza jego siedzibą, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI;
- braku pełnej informacji o wykorzystywanych zasobach informatycznych Urzędu, obejmującej ich rodzaj i konfigurację, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI;
- zastosowaniu zabezpieczeń fizycznych serwerowni, które w niewystarczającym stopniu chroniły to pomieszczenie, a także przechowywaniu w nim materiałów łatwopalnych, co było niezgodne z § 20 ust. 2 pkt 9 rozporządzenia KRI (nieprawidłowość została częściowo usunięta w trakcie kontroli);
- braku dokumentowania procesu nadawania uprawnień użytkowników do pracy w systemach informatycznych nie służących do przetwarzania danych osobowych, co było niezgodne z *Instrukcją postępowania w przypadku nadawania/cofania uprawnień do pracy w systemie informatycznym*[5];
- braku pełnej informacji o podstawowych aktywach informacyjnych Urzędu w zestawieniu opracowywanym na podstawie *Metodyki analizy ryzyka utraty integralności, dostępności lub poufności informacji*[6], w zakresie opisów zbiorów informacji Urzędu, sposobów ich zabezpieczenia, oceny ich wartości dla Urzędu i uzasadnienia tych ocen.

Ponadto, na podstawie wyników kontroli NIK sformułowała uwagi, dotyczące poprawy bezpieczeństwa informacji w Urzędzie.

---

[4] Wprowadzone zarządzeniem nr ROA.0050.210.2015 Burmistrza z 9 grudnia 2015 r. w sprawie wdrożenia polityki bezpieczeństwa danych osobowych i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie.

[5] Wprowadzona zarządzeniem nr ROA.0050.188.2016 Burmistrza z 28 października 2016 r. w sprawie wdrożenia instrukcji i zasad związanych z bezpieczeństwem informacji w Urzędzie Miasta i Gminy w Górze Kalwarii.

[6] Wprowadzona zarządzeniem nr ROA.0050.187.2016 Burmistrza z 28 października 2016 r. w sprawie wdrożenia metodyki analizy ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie Miasta i Gminy w Górze Kalwarii.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. Stosownie do § 20 ust. 1 rozporządzenia KRI, w Urzędzie zostały opracowane i zatwierdzone regulacje wewnętrzne, składające się na System Zarządzania Bezpieczeństwem Informacji. W Urzędzie została wdrożona Polityka Bezpieczeństwa Informacji[7], o której mowa w § 20 ust. 3 w związku z ust. 1 rozporządzenia KRI. Pracowników Urzędu zapoznano z dokumentami wchodzącymi w skład SZBI podczas przeprowadzonych w Urzędzie szkoleń z zakresu bezpieczeństwa informacji. W zarządzeniach wprowadzających uregulowania w zakresie bezpieczeństwa informacji zobowiązano wszystkich pracowników do stosowania zasad, określonych w tych dokumentach. W Urzędzie przechowywano oświadczenia pracowników i listy obecności na szkoleniach z zakresu polityki bezpieczeństwa informacji, potwierdzające zapoznanie się pracowników z dokumentacją bezpieczeństwa informacji.

Obowiązki w zakresie wdrożenia, oceny, przeglądu i modyfikacji PBI były przydzielone do dnia 24 maja 2018 r. pracownikowi pełniącemu funkcję ABI, a po 25 maja 2018 r. zostały przydzielone IOD.

(dowód: akta kontroli str. 4-6, 17-35, 44-45, 84-137, 196-228, 244-333, 543, 548, 551, 579-581, 587, 592, 640-642)

1.2. W związku z wejściem w życie przepisów RODO, w Urzędzie nie przeprowadzono aktualizacji *Polityki bezpieczeństwa danych osobowych Urzędu Miasta i Gminy Góra Kalwaria oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria,* pod kątem dostosowania do wymogów tego rozporządzenia (dalszy opis w części *Ustalone nieprawidłowości* w pkt 1 na str. 7).

W związku z wejściem w życie RODO, na tablicach informacyjnych Urzędu oraz w Biuletynie Informacji Publicznej zostały zamieszczone klauzule informacyjne dla kontrahentów (klientów, usługodawców), dotyczące przetwarzania i ochrony danych osobowych. Została uruchomiona skrzynka e-mail, służąca do kontaktu z powołanym w Urzędzie IOD[8]. Ponadto, opracowano wzory oświadczeń dla pracowników w zakresie przetwarzania danych osobowych, których podpisane egzemplarze przechowywano w aktach osobowych. Zostały przygotowane wzory umów z kontrahentami, zawierające uregulowania w zakresie administrowania danymi osobowymi, powierzenia ich przetwarzania oraz zabezpieczenia danych.

(dowód: akta kontroli str. 272-323, 463-485, 543-544, 548-549, 587, 592, 640-642)

1.3. W wyniku przeglądu w 2017 r.[9] dokumentacji bezpieczeństwa informacji zostały zaktualizowane jedynie zasady ochrony fizycznej pomieszczeń i budynków, wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe, wykaz i struktura zbiorów danych osobowych Urzędu oraz procedury tworzenia kopii zapasowych (dalszy opis w części *Ustalone nieprawidłowości* w pkt 1 na str. 7, pkt 4 na str. 8, pkt 4 na str. 14 oraz w części *Uwagi dotyczące kontrolowanej działalności* w pkt 1, 3 i 5 na str. 15-16).

(dowód: akta kontroli str. 321-323, 539, 584, 588)

---

7 Wprowadzona zarządzeniem nr ROA.0050.182.2016 Burmistrza z 19 października 2016 r.

8 iod@gorakalwaria.pl

9 Zarządzenie nr ROA.0050.24.2017 Burmistrza z dnia 9 lutego 2017 r. zmieniające zarządzenie nr ROA.0050.210.2015 z dnia 9 grudnia 2015 r.

1.4. Na podstawie zarządzeń Burmistrza[10] zostali wyznaczeni pracownicy Urzędu na stanowiska odpowiedzialne za bezpieczeństwo informacji, tj. Administratora Bezpieczeństwa Informacji (do 24 maja 2018 r.), Inspektora Ochrony Danych (od 25 maja 2018 r.), Administratora Systemów Informatycznych oraz Administratora Systemu Teleinformatycznego dla informacji niejawnych. W zarządzeniach zostały określone podstawowe zakresy obowiązków na tych stanowiskach. Powyższe stanowiska podlegały bezpośrednio Burmistrzowi. Wyznaczeni pracownicy posiadali niezbędne kompetencje do pełnienia powierzonych im zadań z zakresu bezpieczeństwa informacji, poparte wykształceniem, praktyką zawodową (w tym pełnienie obowiązków ABI), szkoleniami i kursami, obejmującymi również problematykę RODO.

(dowód: akta kontroli str. 43-83, 390-408, 557-564, 640-642)

1.5. Zgodnie z art. 37 ust. 1 lit. a) RODO, 25 maja 2018 r. w Urzędzie został wyznaczony Inspektor Ochrony Danych. Pracownik pełniący tę funkcję posiadał niezbędne kwalifikacje, wynikające z art. 37 ust. 5 RODO. Osoba ta pełniła wcześniej funkcję ABI.

(dowód: akta kontroli str. 391-394, 557-564)

1.6. W zmienionym w dniu 25 maja 2018 r. Regulaminie Organizacyjnym Urzędu[11] wyodrębniono IOD jako oddzielne stanowisko, podlegające bezpośrednio Burmistrzowi. Zakres zadań IOD został określony w zarządzeniu Burmistrza, dotyczącym wyznaczenia pracownika na to stanowisko. Spełniono tym samym wymóg z art. 38 ust. 1 RODO. Osoba będąca IOD realizowała inne zadania w ramach zatrudnienia na samodzielnym stanowisku do spraw obrony cywilnej i zarządzania kryzysowego, spraw wojskowych i obronnych oraz ochrony informacji niejawnych. Wykonywanie tych obowiązków, w ocenie NIK nie wywoływało konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO, gdyż osoba ta nie uczestniczyła w określaniu celów i sposobów przetwarzania danych osobowych.

(dowód: akta kontroli str. 43, 46-47, 391-394, 585, 589, 640-642)

1.7. W ramach wdrożenia PBI sporządzono niżej wskazaną dokumentację, zawierającą polityki i procedury, określające m.in. szczegółowe zasady wdrożenia zabezpieczeń technicznych:

- *Polityka bezpieczeństwa danych osobowych Urzędu Miasta i Gminy Góra Kalwaria* i *Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria*;
- *Metodyka analizy ryzyka utraty integralności, dostępności lub poufności informacji*;
- zasady zapewnienia ciągłości działania i plan zachowania ciągłości działania[12];
- dokumenty dotyczące ochrony informacji niejawnych;
- instrukcje: zarządzania zdalnym dostępem do usług i systemów teleinformatycznych, postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa informacji, postępowania w przypadku nadawania lub cofania

[10] 1. Zarządzenie nr ROA.0050.138.2015 z 20 sierpnia 2015 r. w sprawie wyznaczenia nieetatowego administratora systemu teleinformatycznego w Urzędzie Miasta i Gminy Góra Kalwaria; 2. Zarządzenie nr ROA.0050.147.2015 z 31 sierpnia 2015 r. w sprawie wyznaczenia nieetatowego administratora systemów informatycznych w Urzędzie Miasta i Gminy Góra Kalwaria; 3. Zarządzenie nr ROA 120.61.2012 z 14 maja 2012 r. w sprawie wyznaczenia Administratora Bezpieczeństwa Informacji; 4. Zarządzenie nr ROA.0050.96.2015 z 26 maja 2015 r. zmieniające zarządzenie w sprawie wyznaczenia Administratora Bezpieczeństwa Informacji; 5. Zarządzenie nr ROA.0050.87.2018 z 25 maja 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych.

[11] Zarządzenie nr ROA.0050.88.2018 Burmistrza z 25 maja 2018 r. zmieniające zarządzenie w sprawie wprowadzenia Regulaminu Organizacyjnego Urzędu Miasta i Gminy Góra Kalwaria.

[12] Obejmujące: instrukcję przeciwpożarową, instrukcję bezpieczeństwa pożarowego Urzędu Miasta i Gminy, instrukcję organizacji pracy na Głównym Stanowisku Kierowania Burmistrza w stałej siedzibie i zapasowym miejscu pracy.

uprawnień do pracy w systemach informatycznych, korzystania przez pracowników z zasobów informatycznych Urzędu[13];
- zasady gospodarowania kluczami i ochrony fizycznej budynków Urzędu[14].

(dowód: akta kontroli str. 196-228, 244-332)

1.8. Regulacje wewnętrzne, stanowiące dokumenty wykonawcze PBI, były dostępne dla wszystkich pracowników Urzędu, nie tylko dla osób odpowiedzialnych za realizację poszczególnych czynności wymaganych tymi dokumentami, co zostało szczegółowo opisane w części *Uwaga dotycząca kontrolowanej działalności* na str. 9. W portalu intranetowym Urzędu były publikowane dokumenty SZBI, materiały szkoleniowe i praktyczne wskazówki dla pracowników, dotyczące problematyki bezpieczeństwa informacji.

(dowód: akta kontroli str. 217, 244, 263, 272, 321, 324, 550, 553)

1.9. Zgodnie z *Metodyką analizy ryzyka utraty integralności, dostępności lub poufności informacji*, w Urzędzie sporządzono zestawienie aktywów informacyjnych podlegających ochronie, opisujące: zbiory informacji Urzędu, ich właścicieli, formaty tych zbiorów (elektroniczne, papierowe, papierowo-elektroniczne) oraz lokalizacje przetwarzania i przechowywania informacji. Jednak jak ustalono, pozostałe informacje przewidziane w tym zestawieniu, tj. opisy zbiorów, sposoby ich zabezpieczenia, uzasadnienie wartości zbiorów z punktu widzenia Urzędu, nie zostały uzupełnione przez wyznaczonych właścicieli zbiorów (dalszy opis w części *Ustalone nieprawidłowości* w pkt 3 na str. 8).

(dowód: akta kontroli str. 217-243, 586-587, 591)

1.10. Jak ustalono, zasoby teleinformatyczne Urzędu zostały przypisane do osób, które odpowiadały za dany sprzęt. W Urzędzie prowadzono elektroniczny rejestr zasobów teleinformatycznych (tzw. baza konfiguracji). Rejestr prowadzony był z wykorzystaniem systemu *IT Manager.* W wyniku badania, opartego o dobór celowy 16 użytkowanych urządzeń[15] ustalono, że system ten nie zawierał pełnej informacji o wszystkich zasobach teleinformatycznych Urzędu (dalszy opis w części *Ustalone nieprawidłowości* w pkt 2 na str. 8).

(dowód: akta kontroli str. 5, 36, 535-538, 628, 632-633)

Ustalone nieprawidłowości

W działalności Urzędu w zakresie organizacji bezpieczeństwa informacji stwierdzono następujące nieprawidłowości:

1. W Urzędzie nie przeprowadzono aktualizacji *Polityki bezpieczeństwa danych osobowych Urzędu Miasta i Gminy Góra Kalwaria* oraz *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria,* pod kątem ich dostosowania do wymogów w zakresie ochrony danych osobowych w związku z wejściem w życie przepisów RODO. Jak ustalono, aktualizacja taka jest planowana po zakończeniu w sierpniu 2018 r. audytu bezpieczeństwa informacji, obejmującego również problematykę dostosowania do RODO. Jak wyjaśnił Burmistrz: *(…) ponieważ funkcjonujący w Urzędzie system bezpieczeństwa informacji sprawdził się w praktyce należy pozostawić opisującą go dokumentację wprowadzając w niej tylko niezbędne korekty polegające na zmianie nazewnictwa, uszczegółowieniu niektórych procedur, skorelowaniu zapisów w poszczególnych dokumentach (…) przy dokonywaniu zmian w dokumentacji*

[13] Zarządzenie nr ROA.0050.188.2016 Burmistrza z dnia 28 października 2016 r. w sprawie wdrożenia instrukcji i zasad związanych z bezpieczeństwem informacji w Urzędzie Miasta i Gminy w Górze Kalwarii.

[14] Zarządzenie nr ROA.0050.202.2016 Burmistrza z dnia 28 listopada 2016 r. w sprawie określenia zasad gospodarki kluczami i ochrony fizycznej budynków Urzędu Miasta i Gminy w Górze Kalwarii.

[15] Komputerów stacjonarnych oraz przenośnych, serwerów, sprzętu sieciowego i urządzeń peryferyjnych (drukarek).

należy uwzględnić wnioski i zalecenia z zewnętrznego audytu bezpieczeństwa informacji. Zdaniem NIK, zlecenie przez Urząd audytu w tym zakresie powinno nastąpić w terminie umożliwiającym dostosowanie dokumentacji Urzędu przed wejściem w życie przepisów RODO. Ponadto, wyrażenie przez Urząd zgody na przesunięcie terminu zakończenia audytu bezpieczeństwa o cztery miesiące, tj. z 30 kwietnia na 30 sierpnia 2018 r., uniemożliwiło wykorzystanie jego wyników przed wejściem w życie przepisów RODO. W rozporządzeniu tym przewidziano dwuletni okres, poprzedzający wejście w życie jego przepisów, który powinien być wykorzystany na niezbędne działania dostosowawcze.

(dowód: akta kontroli str. 8-16, 17-35, 43-45, 190-195, 272-323, 543-544, 548-549, 584, 588, 626-627, 630-631, 640-642)

2. Urząd nie posiadał pełnej informacji o wykorzystywanych zasobach informatycznych, obejmującej ich rodzaj i konfigurację, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI. Prowadzona elektroniczna ewidencja zasobów teleinformatycznych Urzędu i ich konfiguracji obejmowała wyłącznie komputery stacjonarne i przenośne, co stanowiło jedynie około 59% urządzeń[16]. W systemie nie rejestrowano informacji o konfiguracji takich urządzeń, jak serwery czy inny sprzęt sieciowy, drukarki itp. Burmistrz wyjaśnił m.in., że: *(…) Serwery nie są monitorowane (…) gdyż ich lokalizacja i ograniczony dostęp (…) uniemożliwia nieautoryzowane modyfikacje konfiguracji sprzętowej (…) Inne urządzenia takie jak drukarki, sprzęt sieciowy mają stałą, niezmienną konfigurację sprzętową i nie wymagają monitorowania w tym zakresie.* Zdaniem NIK, ograniczony zakres zgromadzonych informacji o zasobach teleinformatycznych stanowi ryzyko, że w przypadku katastrofy lub innego zdarzenia losowego ich odtworzenie, a tym samym możliwość świadczenia usług przez Urząd, mogą być utrudnione.

(dowód: akta kontroli str. 5, 36, 535-538, 628, 632-633)

3. Prowadzone przez Urząd zestawienie podstawowych aktywów informacyjnych (wersja z listopada 2017 r.) nie zawierało pełnych informacji, tj. brak było danych w zakresie opisów zbiorów informacji Urzędu, sposobów ich zabezpieczenia, oceny ich wartości dla Urzędu i uzasadnienia tych ocen. Działanie to było niezgodne z obowiązującą w Urzędzie *Metodyką analizy ryzyka utraty integralności, dostępności lub poufności informacji.* Jak wyjaśnił Burmistrz: *Wstępna analiza wykazała, że trudno będzie jednoznacznie określić mniej lub bardziej ważne aktywa w codziennej pracy. W związku z tym zostało przyjęte skonsolidowane podejście do ochrony aktywów, zapewniając im taki sam poziom ochrony.*

(dowód: akta kontroli str. 217-243, 586-587, 591)

4. Stanowiąca część dokumentacji zapewnienia ciągłości działania Urzędu *Instrukcja bezpieczeństwa pożarowego* z lipca 2014 r. nie została zaktualizowana. Było to niezgodne z § 6 ust. 7 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów[17] oraz skutkowało tym, że w *Instrukcji* jako odpowiedzialne za bezpieczeństwo były wykazywane osoby, które zakończyły pracę w Urzędzie. Burmistrz wyjaśnił, że: *Instrukcja bezpieczeństwa nie była aktualizowana, z powodu braku potrzeby*

---

[16] Według stanu na 7 czerwca 2018 r. w Urzędzie użytkowano łącznie 184 urządzenia (tj. komputery, serwery, macierze dyskowe, sprzęt sieciowy, drukarki, telefony, w tym z dostępem do poczty służbowej).

[17] Dz. U. z 2010 r. Nr 109, poz. 719. Zgodnie z § 6 ust. 7 rozporządzenia, instrukcja bezpieczeństwa pożarowego jest poddawana okresowej aktualizacji, co najmniej raz na dwa lata, a także po takich zmianach sposobu użytkowania obiektu lub procesu technologicznego, które wpływają na zmianę warunków ochrony przeciwpożarowej.

aktualizacji treści merytorycznej. Instrukcja zostanie zmieniona do końca sierpnia w zakresie aktualności danych osób.

(dowód: akta kontroli str. 332, 629, 643-649)

Uwaga dotycząca kontrolowanej działalności

NIK zauważa, że opracowane w ramach PBI szczegółowe uregulowania, dotyczące zarządzania zdalnym dostępem do usług IT, nadawania/cofania uprawnień oraz zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, zostały udostępnione wszystkim pracownikom Urzędu. Zdaniem NIK, szczegółowe informacje w tym zakresie powinny być udostępniane wyłącznie pracownikom odpowiedzialnym za realizację zadań wynikających z uregulowań, a nie wszystkim pracownikom Urzędu, ponieważ stwarza to ryzyko, że informacje w nich zawarte mogą być wykorzystane do przełamania ustanowionych zabezpieczeń.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działania Burmistrza w zakresie organizacji bezpieczeństwa informacji. W Urzędzie została opracowana dokumentacja, składająca się na SZBI, w tym PBI oraz szczegółowe procedury i instrukcje. Pracownicy Urzędu zostali zapoznani z obowiązującymi w Urzędzie wymogami w zakresie bezpieczeństwa informacji. Burmistrz, zgodnie z wymogami określonymi w RODO, powołał IOD i umożliwił mu realizację zadań w sposób niezależny. Osoba pełniąca tę funkcję, a także inni pracownicy Urzędu odpowiedzialni za bezpieczeństwo informacji, posiadali odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe.

W okresie objętym kontrolą zapewniono przegląd dokumentacji SZBI, jednak w Urzędzie nie przeprowadzono aktualizacji *Polityki bezpieczeństwa danych osobowych Urzędu Miasta i Gminy Góra Kalwaria* oraz *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria,* pod kątem ich dostosowania do wymogów przepisów RODO. Prowadzone przez Urząd zestawienie podstawowych aktywów informacyjnych (wersja z 2017 r.) nie zawierało pełnych informacji, tj. brak było danych w zakresie opisów zbiorów informacji Urzędu, sposobów ich zabezpieczenia, oceny ich wartości dla Urzędu i uzasadnienia tych ocen. Działanie to było niezgodne z obowiązującą *Metodyką analizy ryzyka utraty integralności, dostępności lub poufności informacji.* Stwierdzono ponadto, że Urząd nie posiadał pełnej informacji o wykorzystywanych zasobach informatycznych obejmującej ich rodzaj i konfigurację.

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

Opis stanu faktycznego

2.1. W § 3 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria* zostały określone obowiązki, odpowiedzialność, zasady i ograniczenia, dotyczące instalacji i wykorzystania oprogramowania przez pracowników. Na podstawie oględzin 10 użytkowanych komputerów ustalono, że zalogowani do nich użytkownicy nie mieli przyznanych uprawnień administracyjnych, umożliwiających instalację dowolnego oprogramowania. Kontrola ustaliła również, że w wykorzystywanym w Urzędzie systemie *IT Manager* wprowadzono reguły, ograniczające możliwość podłączenia do komputerów Urzędu nieautoryzowanych pamięci przenośnych. W ocenie NIK, powyższe działania były zgodne z wymogami określonymi w § 20 ust. 2 pkt 4 rozporządzenia KRI.

(dowód: akta kontroli str. 302-303, 532-534, 587, 591, 628, 632, 637-639)

2.2. W Urzędzie określono zasady nadawania/cofania uprawnień do pracy w systemach informatycznych. Zasady te zostały opisane w dwóch dokumentach:

- w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria* – w zakresie uprawnień do systemów służących przetwarzaniu danych osobowych;
- w *Instrukcji postępowania w przypadku nadawania/cofania uprawnień do pracy w systemie informatycznym* – w zakresie uprawnień do wszystkich systemów informatycznych Urzędu, w tym do systemów służących przetwarzaniu danych osobowych.

Na podstawie badania próby uprawnień do systemów informatycznych 15 pracowników Urzędu ustalono, że wszyscy posiadali uprawnienia do pracy w systemach adekwatne do zakresu realizowanych zadań. Badaniem objęto także uprawnienia dwóch pracowników, którzy w okresie objętym kontrolą zmienili stanowiska pracy. Stwierdzono, że uprawnienia tych osób do pracy w systemach informatycznych zostały zmodyfikowane i były zgodne z nowym zakresem obowiązków. Powyższe działania były zgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI.

Ustalono, że w Urzędzie nie dokumentowano procesu nadawania uprawnień użytkownikom do pracy w systemach innych, niż służące przetwarzaniu danych osobowych, np. *BeSTi@, EDOŚ*[18] (dalszy opis w części *Ustalone nieprawidłowości* w pkt 1 na str. 13).

(dowód: akta kontroli str. 252-254, 293-309, 333-389, 505, 512-514, 627-628, 631-634)

2.3. W wyniku badania blokowania kont w systemach informatycznych, przeprowadzonego na próbie 12 z 17 osób, które w okresie objętym kontrolą zakończyły pracę w Urzędzie ustalono, że ich konta zostały zablokowane. Blokowanie kont odbywało się niezwłocznie po otrzymaniu przez ASI informacji od głównego specjalisty ds. kadrowych w Urzędzie, co było zgodne z *Instrukcją postępowania w przypadku nadawania/cofania uprawnień do pracy w systemie informatycznym*. Trzy zablokowane uprzednio konta były odblokowywane przez ASI, a proces ten nie był dokumentowany, co szczegółowo opisano w części *Uwagi dotyczące kontrolowanej działalności* w pkt 4 na str. 15.

Ustalono, że w przypadku jednego z pracowników objętych badaniem brak było dokumentacji potwierdzającej uprzednie nadanie mu uprawnień do pracy w systemach informatycznych. Było to niezgodne z obowiązującymi w Urzędzie uregulowaniami w zakresie nadawania/cofania uprawnień do pracy w systemach informatycznych (dalszy opis w części *Ustalone nieprawidłowości* w pkt 2 na str. 14).

(dowód: akta kontroli str. 505-531, 545, 550, 586, 590)

2.4. Komputery Urzędu były zarządzane centralnie w oparciu o mechanizm *Active Directory*. Wymogi dotyczące złożoności haseł do systemów informatycznych, zostały określone w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria*. W myśl tych zasad, każdy z użytkowników winien stosować hasła o wymaganej złożoności. Powyższe rozwiązania i wymogi określone w *Instrukcji* były zgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI.

[18] W badanej próbie dotyczącej uprawnień do pracy w systemach informatycznych 15 pracowników Urzędu, oprócz programów służących do przetwarzania danych osobowych pracownicy posiadali uprawnienia do innych programów, tj. *BeSTi@* (zarządzanie budżetem jednostki samorządu terytorialnego i sprawozdawczość), *EDOŚ* (ewidencja danych o dokumentach zawierających informację o środowisku i jego ochronie), itp.

W wyniku badania trzech systemów informatycznych w Urzędzie ustalono, że wymogi wynikające z powyższej *Instrukcji* zostały wdrożone w dwóch systemach (tj. *eKANCELARIA* i *UmowyFV),* natomiast w systemie *odpadywgminie.com* do dnia 12 czerwca 2018 r. ustawienia dotyczące złożoności haseł dostępu nie spełniały tych wymogów (dalszy opis w części *Ustalone nieprawidłowości* w pkt 3 na str. 14*).* W trakcie kontroli zasady w systemie zostały dostosowane do wymogów *Instrukcji.*

(dowód: akta kontroli str. 296-298, 500-504, 544, 549, 591)

2.5. Na sześciu stanowiskach pracy, 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. 492)

2.6. W Urzędzie ustanowiono zasady zarządzania zdalnym dostępem pracowników lub kontrahentów zewnętrznych do usług i systemów teleinformatycznych Urzędu[19]. Określono w nich obowiązki, spoczywające na kontrahentach, kierownikach komórek organizacyjnych, a także na ABI oraz ASI, w związku z przydzielaniem zdalnego dostępu. Oprócz tych zasad, w Urzędzie nie wprowadzono innych szczegółowych uregulowań, dotyczących korzystania przez pracowników z posiadanego przez nich sprzętu informatycznego (tj. komputerów i pamięci przenośnych, telefonów komórkowych) poza siedzibą Urzędu (dalszy opis w części *Ustalone nieprawidłowości* w pkt 4 na str. 14).

(dowód: akta kontroli str. 244-262, 584-585, 588-589)

2.7. W Urzędzie nie zostało przyjęte jednolite podejście w zakresie szyfrowania urządzeń przenośnych, w celu minimalizowania ryzyka nieuprawnionego dostępu do informacji, o czym mowa w § 20 ust. 2 pkt 9 i 11 rozporządzenia KRI. Szyfrowaniem objęto część pamięci przenośnych oraz większość telefonów komórkowych. W sześciu komputerach przenośnych, będących w posiadaniu Urzędu, nie stosowano natomiast szyfrowania dysków twardych (dalszy opis w części *Uwagi dotyczące kontrolowanej działalności* w pkt 2 na str. 15).

(dowód: akta kontroli str. 532-534, 585, 588-589, 629, 633)

2.8. W serwerowni Urzędu zapewniono odpowiednie rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwerów i urządzeń sieciowych. W okresie objętym kontrolą testowano lub serwisowano znajdujące się w pomieszczeniu zasilacze awaryjne, klimatyzator i czujnik sygnalizacji pożaru. Część zastosowanych zabezpieczeń fizycznych serwerowni w niewystarczającym stopniu chroniła pomieszczenie, a ponadto w pomieszczeniu w trakcie badania były przechowywane materiały łatwopalne. Stanowiło to naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI (dalszy opis w części *Ustalone nieprawidłowości* w pkt 5 na str. 14).

Jak ustalono, w Urzędzie nie zostały zapewnione zapasowe źródła zasilania sprzętu komputerowego, co zostało opisane w części *Uwagi dotyczące kontrolowanej działalności* w pkt 5 na str. 15.

(dowód: akta kontroli str. 486-491, 541-542, 586, 590-591, 628-629, 633-634)

2.9. W wyniku badania siedmiu[20] z 28 obowiązujących w okresie objętym kontrolą umów z podmiotami zewnętrznymi, dotyczących świadczenia usług informatycznych

---

[19] W zarządzeniu nr ROA.0050.188.2016 Burmistrza z 28 października 2016 r.

[20] 1. umowa nr 851/2016 z 25 sierpnia 2016 r. z MGK Rafał Chmielewski na instalację, montaż, konfigurację i utrzymanie w sprawności technicznej bezprzewodowej sieci HotSpot m.in. w budynku Urzędu i Ratusza; 2. umowa nr 403/LW/2017/RSM z 3 kwietnia 2017 r. z MGK Rafał Chmielewski na wynajem i konserwację systemu monitoringu

na rzecz Urzędu, ustalono, że w pięciu z nich (w tym dwóch, dotyczących usługi poczty elektronicznej[21]) zostały zawarte wymogi, dotyczące zachowania poufności informacji, uzyskanych w związku z realizacją umowy. Było to zgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI.

W przypadku dwóch umów[22] nie zawarto takich postanowień, przy czym w przypadku jednej z nich nie było takiej konieczności, gdyż zainstalowana sieć bezprzewodowa typu *hotspot* nie miała punktu styku z siecią Urzędu (dalszy opis w części *Ustalone nieprawidłowości* w pkt 6 na str. 15).

(dowód: akta kontroli str. 409-458, 544, 549, 584, 587, 591, 629, 633, 650-658)

2.10. W Urzędzie zostały określone zasady, dotyczące postępowania w przypadku przekazywania sprzętu teleinformatycznego poza jednostkę, np. w celu wykonania napraw. W § 2 ust. 10 i 14 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria* przewidziano przed przekazaniem sprzętu m.in. demontaż nośników informacji, usuwanie danych oraz uszkadzanie lub niszczenie nośników w sposób uniemożliwiający odzyskanie danych. Ustanowienie tych zasad było zgodne z pkt A.11.2.7 załącznika A do normy PN-ISO/IEC 27001:2017.

(dowód: akta kontroli str. 298-300)

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

(dowód: akta kontroli str. 37-40, 533)

2.12. Zasady dotyczące tworzenia i przechowywania kopii zapasowych danych w Urzędzie zostały określone w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria.* W wyniku kontroli ustalono, że kopie wszystkich komputerów i serwerów oraz baz danych były wykonywane zgodnie z wymogami określonymi w *Instrukcji*. Proces tworzenia kopii został zautomatyzowany poprzez zastosowanie systemu informatycznego i skryptów. Kopie były przechowywane poza miejscem ich wytwarzania, tj. na macierzy dyskowej w drugiej serwerowni oraz na dyskach twardych i płytach DVD w szafie pancernej. Dostęp do tych pomieszczeń został ograniczony, tj. zastosowano zabezpieczenia fizyczne i ograniczenie kręgu osób uprawnionych do wstępu/pobrania kopii. W *Instrukcji* nie określono zasad testowania kopii zapasowych, przy czym kontrola NIK ustaliła, że w tym zakresie wykorzystywano oprogramowanie do weryfikacji poprawności procesu tworzenia kopii komputerów/serwerów oraz, że informatycy weryfikowali na bieżąco utworzone kopie. W okresie objętym kontrolą wystąpiły przypadki konieczności odtworzenia danych z kopii zapasowych, a proces odtwarzania zakończył się pomyślnie. Powyższe rozwiązania i działania zapewniały zgodność z § 20 ust. 2 pkt 7 oraz ust. 2 pkt 12 lit. b i e rozporządzenia KRI.

(dowód: akta kontroli str. 298-299, 321-323, 493-495, 628, 632)

---

miejskiego; 3. umowa nr 6/LW/2018/RGR z 10 stycznia 2018 r. z Profeko Sp. z o.o. ma aktualizację i serwis systemu odpadywgminie.com; 4. umowa nr 207/156/2018 z 15 lutego 2018 r. z Usługi informatyczne INFO-SYSTEM Roman i Tadeusz Groszek Spółka Jawna na dostarczenie oprogramowania Pakiet dla Administracji i jego serwisowania; 5. umowa nr 1/LW/2017/ROA z 2 stycznia 2017 r. z MTT Polska Sp. z o.o. na świadczenie usług serwisowych i naprawczych oraz dostawę tonerów do urządzeń biurowych, kserokopiarek oraz telefaksów stanowiących własność Urzędu; 6. umowa nr 4/BIP/WWW/2017 z 4 stycznia 2017 r. z Maxus Net Communications Sp. z o.o. na usługę hostingu (www, e-mail, BIP) i licencję na system CMS; 7. umowa nr 68/BIP/WWW/2018 z 31 grudnia 2017 r. z Maxus Net Communications Sp. z o.o. na usługę hostingu i licencję na system CMS.

[21] Umowy: nr 4/BIP/WWW/2017 z 4 stycznia 2017 r. i nr 68/BIP/WWW/2018 z 31 grudnia 2017 r. z Maxus Net Communications Sp. z o.o.

[22] 1. umowa nr 851/2016 z 25 sierpnia 2016 r., 2. umowa nr 1/LW/2017/ROA z 2 stycznia 2017 r.

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.

(dowód: akta kontroli str. 532-534)

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 była na bieżąco monitorowana przez informatyków, określono próg ostrzegawczy na poziomie 80% zajętości przestrzeni oraz wdrożono narzędzie do automatycznego monitorowania pojemności dwóch macierzy dyskowych, służących do przechowywania kopii zapasowych.

(dowód: akta kontroli str. 244-262, 293-323, 496-499, 585, 589, 627, 631, 635, 641-644)

2.15. W uregulowaniach Urzędu z zakresu bezpieczeństwa informacji zostały uwzględnione działania, związane z zarządzaniem zmianami w wykorzystywanym oprogramowaniu. W § 2 ust. 14-17 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria* 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. W *Instrukcji* nie uwzględniono jednak niektórych elementów, ograniczających ryzyko wystąpienia problemów w działaniu systemów informatycznych Urzędu w związku z wprowadzanymi zmianami (dalszy opis w części *Uwagi dotyczące kontrolowanej działalności* w pkt 3 na str. 15).

(dowód: akta kontroli str. 301-302, 587, 591)

2.16. Stosownie do art. 30 ust. 1 RODO, Inspektor Ochrony Danych sporządził i prowadził rejestr czynności przetwarzania. Rejestr zawierał informacje, o których mowa w art. 30 ust. 1 RODO.

(dowód: akta kontroli str. 459-462, 544, 549, 592, 626, 630)

Ustalone nieprawidłowości

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

1. W Urzędzie nie dokumentowano procesu nadawania uprawnień do pracy w systemach informatycznych nie służących do przetwarzania danych osobowych, np. *BeSTi@, EDOŚ.* Było to niezgodne z *Instrukcją postępowania w przypadku nadawania/cofania uprawnień do pracy w systemie informatycznym*. W myśl tej *Instrukcji,* kierownik właściwej komórki organizacyjnej Urzędu występuje do ABI z wnioskiem o nadanie uprawnień, w którym należy wskazać dane pracownika, nazwę systemu, zakres wnioskowanych uprawnień i okres ich udzielenia; w przypadku, gdy dostęp do systemu nie wiąże się z przetwarzaniem danych osobowych, ABI przekazuje kopię wniosku do realizacji do ASI. Jak wyjaśnił Zastępca Burmistrza Pan Jan Wysokiński: *W przypadku systemów nie zawierających danych osobowych (…) uprawnienia są nadawane, modyfikowane oraz usuwane zwyczajowo na ustny wniosek kierownika (właściciela) danego systemu.*

(dowód: akta kontroli str. 252-254, 293-309, 333-389, 512-514, 545, 550, 582-583, 629, 633-634)

2. W związku z badaniem blokowania uprawnień do systemów informatycznych 12 osób, które zakończyły pracę w Urzędzie, ustalono, że w przypadku jednej z tych osób brak było dokumentacji, potwierdzającej nadanie jej uprawnień do pracy w systemach informatycznych. Było to niezgodne z obowiązującymi w Urzędzie procedurami nadawania/cofania uprawnień do pracy w systemach informatycznych. Jak wyjaśnił Zastępca Burmistrza Pan Jan Wysokiński, pracownik ten został zatrudniony 8 września 2015 r., a 9 września 2015 r. uzyskał dostęp do systemów informatycznych na podstawie ustnego oświadczenia kierownika właściwej komórki organizacyjnej.

   (dowód: akta kontroli str. 505-531, 545, 550)

3. Ustawienia systemu *odpadywgminie.com* w zakresie złożoności haseł dostępu nie spełniały wymogów, określonych w § 2 ust. 4 *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria*. Jak wyjaśnił Zastępca Burmistrza Pan Jan Wysokiński: *Procedury zostały wdrożone, lecz nie były należycie przetestowane. W konsekwencji funkcjonowało mylne przeświadczenie o wdrożonych regułach dotyczących złożoności haseł, które po wykryciu zostało natychmiast skorygowane.* W trakcie kontroli NIK wdrożono dla tego systemu wymogi w zakresie złożoności haseł zgodne z *Instrukcją.*

   (dowód: akta kontroli str. 296-298, 500-504, 544, 549)

4. W Urzędzie nie określono szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych poza jego siedzibą, gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI. Burmistrz wyjaśnił, że brak szczegółowych regulacji wynika z charakteru używania na co dzień komputerów przenośnych, tj. komputery wykorzystywane przez Burmistrza i Zastępców służyły jako urządzenia stacjonarne, natomiast pozostałe komputery przenośne były wypożyczane przez informatyków na krótkie okresy, głównie do dokonywania prezentacji na spotkaniach. Burmistrz wyjaśnił ponadto, że szczegółowe regulacje w tym zakresie zostaną opracowane przy najbliższej aktualizacji polityk bezpieczeństwa. Zdaniem NIK, podstawową funkcją urządzeń przenośnych jest praca w dowolnym miejscu z wykorzystaniem technik komunikacyjnych, nie można zatem wykluczyć, że praca może być niekiedy wykonywana również poza siedzibą Urzędu, co może powodować zagrożenia dla bezpieczeństwa danych na nich zgromadzonych (np. kradzież, zgubienie). Biorąc pod uwagę możliwość wynoszenia sprzętu poza siedzibę Urzędu, warto rozważyć zastosowanie rozwiązania polegającego na szyfrowaniu dysków twardych komputerów przenośnych, dzięki czemu w przypadku ich kradzieży lub zagubienia osoby postronne nie będą miały dostępu do danych na nich zgromadzonych.

   (dowód: akta kontroli str. 244-262, 584-585, 588-589)

5. Część zastosowanych zabezpieczeń fizycznych serwerowni, w niewystarczającym stopniu chroniła to pomieszczenie[23], co zwiększało ryzyko ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji, będących w posiadaniu Urzędu. Ponadto, w pomieszczeniu w trakcie jego badania były przechowywane materiały łatwopalne. Było to niezgodne z § 20 ust. 2 pkt 9 rozporządzenia KRI. W trakcie kontroli została usunięta część materiałów łatwopalnych z pomieszczenia. Burmistrz poinformował również o planowanych działaniach, dotyczących poprawy zabezpieczeń fizycznych serwerowni.

   (dowód: akta kontroli str. 486-491, 540, 586, 590-591, 628-629)

[23] Szczegółowe ustalenia w tym zakresie zostały przekazane w trakcie czynności kontrolnych Burmistrzowi.

6. W obowiązującej w 2017 r. umowie nr 1/LW/2017/ROA z MTT Polska Sp. z o.o., obejmującej m.in. świadczenie usług serwisowych i naprawczych kserokopiarek Urzędu, nie uwzględniono zapisów o zachowaniu w tajemnicy informacji uzyskanych/przetwarzanych w związku z realizacją tej umowy. Było to niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI. NIK zauważa, że większość objętych umową urządzeń została wyposażona w pamięć i dyski twarde, umożliwiające przechowanie dokumentów przeznaczonych do druku. Stwarza to ryzyko uzyskania nieautoryzowanego dostępu do informacji przechowywanych w tych urządzeniach. Burmistrz wyjaśnił, że: *Brak zapisów o zachowaniu poufności w części umów wynika z odnawiania umów na wsparcie w kolejnych latach bez wnoszenia zmian do aktualnych uwarunkowań. Odnawiając umowy zwrócona zostanie uwaga na aspekt zachowania poufności.*

(dowód: akta kontroli str. 409-411, 428-458, 629, 633)

Uwagi dotyczące kontrolowanej działalności

1. NIK zauważa, że w Urzędzie funkcjonowały równolegle dwie instrukcje, które opisywały proces nadawania/cofania uprawnień do systemów informatycznych, a zapisy tych instrukcji nie były spójne w zakresie zadań ABI/ASI w związku z nadawaniem/cofaniem uprawnień oraz ich dokumentowaniem. Zdaniem NIK, zasady w tym zakresie powinny być ujednolicone dla wszystkich systemów informatycznych użytkowanych w Urzędzie.
2. W Urzędzie nie stosowano jednolitego podejścia w zakresie szyfrowania danych, zgromadzonych na nośnikach i urządzeniach przenośnych. Szyfrowaniu podlegała część pamięci przenośnych i większość telefonów komórkowych, natomiast nie szyfrowano dysków komputerów przenośnych. Zdaniem NIK, w celu zminimalizowania ryzyka nieuprawnionego dostępu do informacji w przypadku kradzieży lub zagubienia urządzenia/nośnika przenośnego, zasadne jest stosowanie szyfrowania pamięci wszystkich urządzeń mobilnych i nośników pamięci wykorzystywanych w Urzędzie.
3. W *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria* w zakresie zarządzania zmianą nie uregulowano takich zagadnień, jak: szacowanie potencjalnego wpływu zmian na działanie środowiska informatycznego i bezpieczeństwo informacji, zasad formalnego zatwierdzania zmian oraz wytycznych na wypadek niepomyślnych zmian lub nieprzewidzianych zdarzeń. Stosownie do pkt. 12.1.2 załącznika A do normy PN-ISO/IEC 27001:2017, w procesie zarządzania zmianą w oprogramowaniu należy także uwzględnić wyżej opisane kwestie. W odniesieniu do powyższego, Burmistrz wyjaśnił m.in., że w przypadku niepomyślnych zmian lub nieprzewidzianych zdarzeń przywracany jest stan z kopii bezpieczeństwa, wykonanej przed rozpoczęciem zmian lub zagadnienie jest konsultowane ze służbami wsparcia danego oprogramowania. Podał również, że szczegółowe regulacje w powyższym zakresie powstaną przy najbliższej aktualizacji powyższej *Instrukcji*.
4. NIK zauważa, że trzy spośród badanych 12 zablokowanych kont pracowników, którzy zakończyli pracę w Urzędzie, były odblokowywane przez ASI. Wynikało to z konieczności uzyskania przez kierowników komórek organizacyjnych Urzędu dostępu do informacji, zgromadzonych przez pracowników w systemach informatycznych. Czynność dostępu do konta osoby, która zakończyła zatrudnienie w Urzędzie nie była dokumentowana. Zdaniem NIK, w celu zapewnienia właściwego nadzoru nad dostępem do zasobów i danych Urzędu, tego typu operacje powinny być dokumentowane.
5. Pomimo, że zastosowanie odrębnego zasilania sprzętu komputerowego przewidziano w § 6 ust. 1 *Polityki bezpieczeństwa danych osobowych Urzędu*

Miasta i Gminy Góra Kalwaria, Urząd nie posiadał takiego rozwiązania. Z wyjaśnień Burmistrza wynika, że nie ma obecnie możliwości podłączenia dodatkowej linii zasilania. W związku z powyższym, zapisy *Polityki* w tym zakresie powinny zostać odpowiednio skorygowane.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, wdrożone i wykorzystywane w Urzędzie rozwiązania organizacyjne i techniczne, zapewniające bezpieczeństwo informacji. Komputery Urzędu zostały zabezpieczone programem antywirusowym przed szkodliwym oprogramowaniem oraz przed możliwością instalowania dowolnego oprogramowania przez użytkowników. W Urzędzie prowadzono na bieżąco aktualizację oprogramowania systemowego oraz sporządzano i weryfikowano prawidłowość kopii zapasowych. Spełniono również wymóg przechowywania kopii poza miejscem ich wytwarzania.

W powyższym zakresie stwierdzono nieprawidłowości, które dotyczyły m.in:

- niedokumentowania procesu nadawania uprawnień do pracy w systemach informatycznych nie służących do przetwarzania danych osobowych;
- nieuregulowania zasad i procedur korzystania przez pracowników ze sprzętu i urządzeń przenośnych Urzędu poza jego siedzibą;
- zastosowania do zabezpieczenia serwerowni rozwiązań, które w niewystarczającym stopniu chroniły to pomieszczenie, a także przechowywania w nim materiałów łatwopalnych (nieprawidłowość została częściowo usunięta w trakcie kontroli);
- niedostosowania ustawień systemu *odpadywgminie.com* w zakresie złożoności haseł użytkownika do wymogów, określonych w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Góra Kalwaria* (nieprawidłowość została usunięta w trakcie kontroli)*;*
- nieuwzględnienia w jednej z siedmiu badanych umów z podmiotami zewnętrznymi, świadczącymi usługi informatyczne dla Urzędu, zapisów o zachowaniu w tajemnicy informacji uzyskanych/przetwarzanych w związku z jej realizacją.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. Stosownie do § 20 ust. 2 pkt 3 rozporządzenia KRI, w Polityce Bezpieczeństwa Informacji Urzędu został uregulowany obowiązek przeprowadzania cyklicznej analizy ryzyka związanego z bezpieczeństwem informacji. Szczegółowe zasady, tj. etapy i czynności w procesie analizy ryzyka utraty integralności, poufności i dostępności, zasady dokumentowania przeprowadzonej analizy oraz odpowiedzialności, zostały określone w *Metodyce analizy ryzyka utraty integralności, dostępności lub poufności.* Jak ustalono, analiza ryzyka w powyższym zakresie była przeprowadzana corocznie, tj. zgodnie z pkt 9.1 *Metodyki.* W ramach analizy przeprowadzano aktualizację opracowanych na podstawie *Metodyki* dokumentów, opisujących:

- aktywa informacyjne Urzędu,
- podatności i potencjalne zagrożenia,
- zidentyfikowane ryzyka,
- ocenę ryzyka,
- sposoby reakcji na ryzyka,
- plany postępowania z ryzykiem.

(dowód: akta kontroli str. 217-243, 586-587, 591, 593-625)

3.2. Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI, w Urzędzie została opracowana *Instrukcja postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa informacji*[24]. Pracownicy Urzędu zostali zapoznani z *Instrukcją* i zobowiązani do stosowania jej zasad. Zgodnie z *Instrukcją,* w Urzędzie był prowadzony rejestr incydentów. W okresie objętym kontrolą zostało w nim zarejestrowane jedno zdarzenie, dotyczące możliwości nieuprawnionego dostępu do serwerowni.

W odniesieniu do problematyki zgłaszania zdarzeń i naruszeń bezpieczeństwa informacji Burmistrz wyjaśnił, że: *Na każde podejrzenia incydentu użytkownik otrzymuje informację zwrotną, czy zgłaszana sytuacja jest zagrożeniem, czy też nie. W przypadku, gdy jest to sytuacja niepożądana – dodawane są instrukcje co ma w tej sytuacji uczynić.*

W portalu intranetowym Urzędu służby informatyczne publikowały komunikaty ostrzegawcze i zalecenia dla pracowników, w związku z występującymi zagrożeniami bezpieczeństwa informacji.

(dowód: akta kontroli str. 248-250, 545-546, 550, 555-556, 626, 630, 636)

3.3. Stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI, w PBI określono wymogi, dotyczące realizacji szkoleń z zakresu bezpieczeństwa informacji. Jak wyjaśniła Sekretarz Gminy Pani Beata Kisiel, szkolenia w Urzędzie są organizowane 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 w Urzędzie przepisów bezpieczeństwa informacji, bezpiecznej pracy w systemach informatycznych, ochrony danych i budynków, a także przepisów RODO. Szkolenia były prowadzone przez Administratora Bezpieczeństwa Informacji, Administratora Systemów Informatycznych, Sekretarza Gminy i Kierownika Referatu Organizacyjno-Administracyjnego. Z zakresu bezpieczeństwa informacji zostali przeszkoleni wszyscy pracownicy Urzędu za wyjątkiem dwóch osób, przebywających na długotrwałych zwolnieniach i urlopach. Jak wyjaśnił Burmistrz, w sierpniu 2018 r. po zakończeniu zewnętrznego audytu bezpieczeństwa informacji, zostanie przeprowadzone kolejne szkolenie dla pracowników z tego zakresu.

W okresie objętym kontrolą Administrator Bezpieczeństwa Informacji, Sekretarz Gminy, Kierownik Referatu Organizacyjno-Administracyjnego i główny specjalista ds. kadrowych uczestniczyli indywidualnie w szkoleniach zewnętrznych, obejmujących szczegółowe zagadnienia związane z wejściem w życie przepisów RODO.

Na portalu intranetowym Urzędu opublikowano materiały informacyjno-szkoleniowe z zakresu bezpieczeństwa informatycznego i oszustw komputerowych.

(dowód: akta kontroli str. 17-31, 211, 546, 551-581, 626, 630)

3.4. W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI (dalszy opis w części *Ustalone nieprawidłowości* w pkt 1 na str. 18).

Umową z 1 marca 2018 r. Urząd zlecił przeprowadzenie audytu bezpieczeństwa informacji[25], w którego zakresie ujęto zagadnienia zgodności z RODO, tj.:

– analizę zgodności prowadzonych procesów przetwarzania danych osobowych z RODO, identyfikację i wycenę ryzyk;

[24] Przyjęta zarządzeniem nr ROA.0050.188.2016 Burmistrza z 28 października 2016 r.

[25] Na podstawie umowy nr 393/LW/2018/INF z dnia 1 marca 2018 r.

– sformułowanie zaleceń oraz wariantów budżetów w celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji i spełnienia wymogów RODO.

W dniu 23 kwietnia 2018 r. wydłużono termin zakończenia audytu z 30 kwietnia do 30 sierpnia 2018 r.[26] Jak wyjaśnił Zastępca Burmistrza Pan Jan Wysokiński, rozmowy w sprawie przeprowadzenia audytu z wybranym oferentem były prowadzone od połowy 2017 r., a oferta wpłynęła w sierpniu 2017 r. Ze względu na inne zobowiązania, oferent mógł przystąpić do audytu dopiero w marcu 2018 r. Urzędowi zależało na wybranym oferencie, ze względu na opinie o wysokiej jakości prowadzonych przez niego audytów.

Zgodnie z § 9 *Polityki bezpieczeństwa danych osobowych Urzędu Miasta i Gminy Góra Kalwaria,* w 2017 r. zostało przeprowadzone przez ABI planowe sprawdzenie zgodności z przepisami przetwarzania danych osobowych w dwóch komórkach organizacyjnych Urzędu[27]. Zalecenia sformułowane w wyniku tego sprawdzenia zostały zrealizowane.

(dowód: akta kontroli str. 4-16, 144-195, 543-544, 548-549, 554, 584, 588)

3.5. W Urzędzie nie została przeprowadzona ocena procesów przetwarzania danych, o której mowa w art. 32 RODO. Z wyjaśnień wynika, że została ona zlecona zewnętrznemu wykonawcy w ramach realizowanego przez niego w 2018 r. audytu bezpieczeństwa informacji (dalszy opis w części *Ustalone nieprawidłowości* w pkt 2 na str. 18).

(dowód: akta kontroli str. 543-544, 548-549, 584, 588)

Ustalone nieprawidłowości

W działalności Urzędu w zakresie podejmowanych działań w celu zapobiegania incydentom bezpieczeństwa informacji stwierdzono następujące nieprawidłowości:

1. W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. Zastępca Burmistrza Pan Jan Wysokiński wyjaśnił, że spełniając zapisy rozporządzenia KRI, w Urzędzie zostały przeprowadzone audyty bezpieczeństwa systemów IT i bezpieczeństwa informacji w 2015 i 2016 r. Ponadto, podał że: *(…) Ponieważ nieprawidłowości stwierdzone podczas audytu w 2015 roku zostały usunięte, co zostało wskazane podczas audytu w roku 2016, w roku 2017 nie zaplanowano i nie przeprowadzono audytu, zaś do audytu wytypowane zostały inne obszary wymagające sprawdzenia.* Zdaniem NIK, rozporządzenie KRI w § 20 ust. 2 pkt 14 określa wprost wymóg zapewnienia przez kierownictwo podmiotu publicznego przeprowadzenia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok.

   (dowód: akta kontroli str. 4-16, 543, 548)

2. W Urzędzie nie przeprowadzono oceny procesów przetwarzania danych, o której mowa w art. 32 RODO. Z wyjaśnień Burmistrza wynika, że: *Analizę procesów przetwarzania danych, w związku z wejściem w życie przepisów RODO, zlecono firmie zewnętrznej, która nie przedstawiła jeszcze końcowych wyników w tym zakresie. Na podstawie wyników audytu będą, w razie potrzeby wdrażane stosowne zabezpieczenia lub też modyfikowane obecnie istniejące.*

   (dowód: akta kontroli str. 8-16, 190-195, 543-544, 548-549, 584, 588)

[26] Na podstawie aneksu nr 1 do umowy nr 393/LW/2018/INF z 30 kwietnia 2018 r.

[27] Referat Gospodarki Komunalnej oraz Referat Rolnictwa i Ochrony Środowiska.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Urzędu w zakresie zapobiegania incydentom bezpieczeństwa informacji, ze względu na nieprzeprowadzenie w 2017 r. audytu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI, a także ze względu na brak przeprowadzenia oceny procesów przetwarzania danych w Urzędzie, o której mowa w art. 32 RODO.

W Urzędzie natomiast prawidłowo realizowano zadania, dotyczące cyklicznej analizy ryzyka związanego z bezpieczeństwem informacji, postępowania w przypadku naruszenia bezpieczeństwa informacji oraz prowadzenia szkoleń z zakresu 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[28] wnosi o:

1) dostosowanie obowiązującej w Urzędzie Polityki bezpieczeństwa danych osobowych do wymogów RODO;
2) prowadzenie aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację;
3) zapewnienie pełnej informacji o podstawowych aktywach informacyjnych Urzędu;
4) zapewnienie dokumentowania procesu nadawania uprawnień użytkowników w odniesieniu do wszystkich systemów informatycznych w Urzędzie;
5) ustanowienie szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych;
6) wdrożenie rozwiązań umożliwiających odpowiednie zabezpieczenie pomieszczenia serwerowni;
7) zawieranie w umowach z podmiotami zewnętrznymi, świadczącymi usługi informatyczne dla Urzędu, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
8) zapewnienie przeprowadzenia co najmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji;
9) przeprowadzenie oceny procesów przetwarzania danych w Urzędzie, o której mowa w art. 32 RODO.

[28] 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 Departamentu Administracji Publicznej Najwyższej Izby Kontroli.

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.

Warszawa, dnia 30 lipca 2018 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej
Dyrektor
Bogdan Skwarka

.....
podpis

Kontroler:
Bartosz Tajer
Główny specjalista k.p.

.....
podpis