NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu

LWR.410.015.02.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu
ul. Marszałka J. Piłsudskiego 15/17, 50-044 Wrocław
T +48 71 711 83 00, F +48 71 711 83 50
lwr@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 we Wrocławiu

Kontroler

Waldemar Zimoch – główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/156/2018 z dnia 27 czerwca 2018 r.

(dowód: akta kontroli str. 1)

Jednostka kontrolowana

Urząd Miasta i Gminy w Kątach Wrocławskich (dalej: „Urząd"), ul. Rynek – Ratusz 1, 55-080 Kąty Wrocławskie.

Kierownik jednostki kontrolowanej

Pan Antoni Kopeć – Burmistrz Miasta i Gminy w Kątach Wrocławskich (dalej: „Burmistrz").

(dowód: akta kontroli str. 3-4)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości działalność kontrolowanej jednostki w zakresie zarządzania bezpieczeństwem informacji.

Uzasadnienie oceny ogólnej

Na treść oceny ogólnej wpłynęła ocena cząstkowa sformułowana dla obszaru dotyczącego wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji, który został oceniony pozytywnie mimo stwierdzonych nieprawidłowości. Pozostałe dwa badane obszary, tj. organizacja bezpieczeństwa informacji oraz działania w celu zapobiegania incydentom bezpieczeństwa informacji, zostały ocenione pozytywnie.

Stwierdzona nieprawidłowość dotyczyła posiadania uprawnień administracyjnych przez 14,3% badanych użytkowników niebędących pracownikami służb informatycznych, co stanowiło naruszenie § 20 ust. 2 pkt 4 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[1] (dalej: *„rozporządzenie KRI"*). W ocenie NIK w tym konkretnym przypadku nie wpłynęło to jednak w sposób zasadniczy na zachowanie bezpieczeństwa informacji w badanej jednostce.

W toku kontroli stwierdzono także, iż Urząd opracował i wdrożył system zarządzania bezpieczeństwem informacji (dalej: „SZBI"), w tym w szczególności politykę bezpieczeństwa informacji (dalej: „PBI"), wymagany przepisami *rozporządzenia KRI*. Prowadził także inwentaryzację posiadanych zasobów informatycznych, obejmującą ich rodzaj i konfigurację. W Urzędzie stosowano również politykę haseł dostępowych dla użytkowników do systemów informatycznych, zapewniającą właściwą ochronę informacji przed nieuprawnionym dostępem, prawidłowo zabezpieczono wszystkie

[1] Dz. U z 2017 r. poz. 2247.

serwerownie, jak również sporządzano i przechowywano kopie zapasowe baz danych w sposób zapewniający wystarczającą ochronę przed utratą informacji.

Ponadto należy podkreślić, że zgodnie z wymogami *rozporządzenia KRI*, w okresie objętym kontrolą, Urząd przeprowadził audyt wewnętrzny w zakresie bezpieczeństwa informacji oraz okresową analizę ryzyka utraty integralności, poufności lub dostępności informacji, a także szkolenia dla pracowników zaangażowanych w proces przetwarzania informacji.

Najwyższa Izba Kontroli sformułowała również uwagi dotyczące: [1] udostępnienia szczegółów technicznych stosowanych procedur i zabezpieczeń wszystkim pracownikom Urzędu; [2] ryzyka istnienia konfliktu interesu w przypadku osoby powołanej na stanowisko Inspektora Ochrony Danych (dalej: „IOD"); [3] przekroczenia zajętości przestrzeni dyskowej powyżej 80%.

Jednocześnie NIK pozytywnie ocenia działania podejmowane przez Urząd w związku z wejściem w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*[2] (dalej: „*RODO*").

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

W Urzędzie opracowano i wdrożono SZBI, w tym w szczególności PBI, wymagany § 20 ust. 3 w związku z ust. 1 *rozporządzenia KRI*.

Składał się on z wprowadzonej w dniu 6 lipca 2009 r.[3] częściowo nowej, a także zaktualizowanej dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne służące do przetwarzania tych danych. Następnie zarządzeniem 128/2015 z dnia 14 maja 2015 r. Burmistrza Miasta i Gminy Kąty Wrocławskie uzupełnioną ją procedurą zarządzania ryzykiem w ramach SZBI, a w związku z wejściem w życie *RODO*, dokonano aktualizacji dokumentacji PBI oraz procedur związanych z przetwarzaniem danych osobowych w Urzędzie[4].

Dokumentacja ta została zatwierdzona przez kierownika jednostki oraz przedstawiono ją do zapoznania się i stosowania wszystkim pracownikom Urzędu. Określono w niej jasno właściciela odpowiadającego za jej opracowanie, wdrożenie i ocenę, a także przegląd i modyfikację.

(dowód: akta kontroli str. 42-43)

W urzędzie sporządzono dokumentację w zakresie ochrony danych osobowych uwzględniającą wymogi *RODO*, obejmującą:

- ✓ Politykę Systemu Zarządzania Bezpieczeństwem Informacji;
- ✓ Deklarację Stosowania;
- ✓ Politykę Bezpieczeństwa Informacji;
- ✓ Politykę Bezpieczeństwa Danych Osobowych;
- ✓ Zasady Nadzorowania Danych Osobowych;
- ✓ Procedury Nadzorowania Danych Osobowych;

[2] Dz. Urz. UE L 119 z 04 maja 2016, str. 1, ze zm.

[3] Zarządzeniem 584/2009 Burmistrza Miasta i Gminy Kąty Wrocławskie w sprawie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych.

[4] Zarządzeniem 965/2018 Burmistrza Miasta i Gminy Kąty Wrocławskie z dnia 25 maja 2018 r.

- ✓ Zarządzanie Ryzykiem w ramach Systemu Zarządzania Bezpieczeństwem Informacji;
- ✓ Instrukcje Zarządzania Systemem Informatycznym;
- ✓ Regulamin Ochrony Danych Osobowych.

Powyższa dokumentacja została przedstawiona do zapoznania się wszystkim pracownikom jednostki.

(dowód: akta kontroli str. 45-199)

W okresie po 1 czerwca 2017 r dokumentacja techniczna stanowiąca SZBI została poddana formalnemu przeglądowi i aktualizacji[5], w związku z wejściem w życie nowych przepisów prawnych dotyczących *RODO*, co było zgodne z § 20 ust. 2 pkt 1 *rozporządzenia KRI*.

(dowód: akta kontroli str.45-199)

Zgodnie z obowiązującymi regulacjami dotyczącymi bezpieczeństwa, nadzór nad PBI i przestrzeganiem zasad w niej zawartych pełnił Administrator Bezpieczeństwa Informacji (dalej: „ABI"). Od dnia 7 kwietnia 2015 r. Urząd posiadał formalnie wyznaczonego pracownika pełniącego tę funkcję. Osoba ta według zakresu czynności miała za zadanie zapewnić przestrzeganie zasad i wymagań bezpieczeństwa dla systemów informatycznych, prowadzić nadzór nad realizacją wymogów określonych w polityce bezpieczeństwa informacji oraz wszelkich procedur i instrukcji bezpieczeństwa obowiązujących w Urzędzie, a także współpracować w zakresie aktualizacji instrukcji bezpieczeństwa systemów komputerowych i zapewnić poprawność i ciągłość działania tychże systemów. Osoba ta miała odpowiednie kompetencje wynikające z jej wykształcenia, praktyki zawodowej oraz odbytych szkoleń.

(dowód: akta kontroli str. 5-6)

W dniu 14 sierpnia 2018 r. zarządzeniem nr 1050/2018 Burmistrz Miasta i Gminy Kąty Wrocławskie wyznaczył IOD, co było zgodne z art. 37 ust. 1 *RODO*. W tym samym dniu jednostka przekazała informację o wyznaczeniu IOD do Prezesa Urzędu Ochrony Danych Osobowych, co było zgodne z art. 158 ust. 5 ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych*[6] (dalej: „*uodo*"), a jego prawa i obowiązki zostały określone w obowiązującej „Polityce Bezpieczeństwa Danych Osobowych".

(dowód: akta kontroli str. 7-8)

Osoba wyznaczona do pełnienia funkcji IOD posiadała doświadczenie zawodowe w zakresie ochrony danych osobowych, pełniła wcześniej funkcję ABI w Urzędzie oraz brała udział w licznych szkoleniach dotyczących ochrony danych osobowych i ukończyła w tym zakresie specjalistyczne kursy. IOD był pracownikiem etatowym, zatrudnionym w pełnym wymiarze na stanowisku głównego specjalisty ds. informatyki. W toku przeprowadzonej kontroli stwierdzono, iż pracownik wybrany do pełnienia funkcji IOD spełniał przepisy art. 38 ust. 3 *RODO* w zakresie niezależności, jednak ze względu na pełnioną wcześniej funkcję ABI istniało ryzyko konfliktu interesu.

(dowód: akta kontroli str. 9-35)

Obowiązujące w Urzędzie regulacje w zakresie PBI zawierały między innymi takie procedury jak:

---

[5] Umowa OR.142.2.2018-8, zawarta w dniu 20 marca 2018 r. na wykonanie usługi polegającej na weryfikacji, aktualizacji i wdrożeniu dokumentacji oraz procedur związanych z przetwarzaniem danych osobowych w Urzędzie Miasta i Gminy Katy Wrocławskie.

[6] Dz. U. poz. 1000.

- ✓ realizacji szkoleń z ochrony danych osobowych;
- ✓ nadawania uprawnień w systemie informatycznym;
- ✓ złożenia przez pracownika wymaganych oświadczeń;
- ✓ zawierania i realizacji umów z podmiotami przetwarzającymi dane osobowe;
- ✓ przydziału haseł dla administratorów systemów, użytkowników oraz częstotliwość ich zmiany;
- ✓ postępowania z nośnikami informacji zawierającymi dane osobowe;
- ✓ korzystania z komputerów przenośnych;
- ✓ korzystania z poczty elektronicznej;
- ✓ sporządzania i przechowywania kopii zapasowych;
- ✓ zabezpieczeń systemu informatycznego przed oprogramowaniem złośliwym;
- ✓ kontrola eksploatowanego oprogramowania i wprowadzania zmian;
- ✓ uwiarygodnienie danych wejściowych;
- ✓ przymus alarmowania o zagrożeniach.

Przytoczone powyżej regulacje składały się wyłącznie z części deklaratywnej i były w całości dostępne dla wszystkich pracowników Urzędu. Pracownicy jednostki zostali zapoznani z tymi regulacjami.

(dowód: akta kontroli str. 45-199)

W związku z wejściem w życie przepisów *RODO* w Urzędzie zaktualizowano system zarządzania ryzykiem. W ramach przeprowadzonej analizy ryzyka, dokonano identyfikacji systemów/zbiorów, w których przetwarzane były dane. Dla potrzeb szacowania ryzyka zakwalifikowano je do następujących kategorii: systemy dziedzinowe, systemy EOD[7], strony internetowe, strony bankowości elektronicznej, systemy monitoringu, systemy powiadamiania mieszkańców. Dla wskazanych kategorii dokonano identyfikacji zagrożeń oraz wykonano szacowanie ryzyka.

(dowód: akta kontroli str. 200)

Urząd prowadził inwentaryzację zasobów informatycznych jednostki obejmującą ich rodzaj i konfigurację, wynikającą z § 20 ust. 2 pkt 2 *rozporządzenia KRI.* Do tego celu wykorzystywano oprogramowanie wspomagające zarządzanie systemem komputerowym, które pozwalało na stałe monitorowanie:

- ✓ stanu i rodzaju zainstalowanego oprogramowania na stacjach roboczych i komputerach przenośnych;
- ✓ aktualnej konfiguracji sprzętowej urządzeń oraz zmian w parametrach sprzętu;
- ✓ logowania się i aktywności użytkowników pracujących na komputerach.

(dowód: akta kontroli str. 201-206)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Uwaga dotycząca badanej działalności

NIK zwraca uwagę, że:

1. szczegóły techniczne stosowanych procedur i zabezpieczeń, zawarte w załącznikach do obowiązującej PBI, są częścią deklaratywną tego dokumentu i są dostępne dla wszystkich pracowników Urzędu. Udostępnienie tych dokumentów wszystkim pracownikom stwarza ryzyko, że informacje w nich zawarte zostaną wykorzystane do przełamania ustanowionych zabezpieczeń;
2. inne zadania i obowiązki wykonywane przez osobę pełniącą w Urzędzie funkcję IOD mogą powodować konflikt interesów, o którym mowa w art. 38 ust. 6 *RODO*, gdyż osoba powołana na tą funkcję, będąc jednocześnie głównym specjalistą ds. informatyki, uczestniczy w określaniu celów i sposobów

[7] EOD - Elektroniczny obieg dokumentów - potoczne określenie systemu informatycznego do zarządzania obiegiem zadań oraz dokumentów działającego w oparciu o mechanizmy typu workflow.

przetwarzania danych osobowych w Urzędzie, a zatem nie spełnia wymogu określonego w ww. przepisie. W myśl art. 38 ust. 6 *RODO*, osoba wyznaczona na IOD może wykonywać inne zadania i obowiązki, jednak administrator danych (tj. Burmistrz) musi zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów. Zdaniem NIK, biorąc pod uwagę art. 158 ust. 1 *uodo* – gdzie wskazano, że osoba pełniąca w dniu 24 maja 2018 r. funkcję ABI staje się IOD i pełni swoją funkcję do dnia 1 września 2018 r. – po tym terminie funkcja IOD powinna być powierzona osobie, której podstawowe obowiązki (z racji wykonywanych zadań) nie będą powodować konfliktu interesów z zadaniami IOD.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie organizacji bezpieczeństwa informacji.

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

Opis stanu faktycznego

Uprawnienia użytkowników 14 komputerów objętych oględzinami nie pozwalały (poza dwoma przypadkami) na zainstalowanie nieautoryzowanego oprogramowania. Było to zgodne z § 20 ust. 2 pkt 4 *rozporządzenia KRI*.

(dowód: akta kontroli str. 207-224)

W Urzędzie obowiązywała procedura nadawania i odbierania uprawnień do systemów informatycznych. Uprawnienia dostępu do systemów informatycznych, ich zmiana lub cofnięcie następowało w formie pisemnej po akceptacji bezpośredniego przełożonego i ABI. Stosowany formularz[8] uwzględniał m.in. możliwość nadania uprawnień do wybranych z listy zasobów sieciowych, możliwość nadania uprawnień do poszczególnych programów lub ich modułów. Zakres tych uprawnień obejmował przeglądanie, drukowanie, modyfikacje, zmianę, wprowadzanie, dopisywanie, aktualizację, usuwanie, czy też archiwizowanie. Szczegółowe badanie uprawnień 15 pracowników Urzędu wykonujących zadania w systemach informatycznych, wykazało, że pracownicy ci posiadali uprawnienia do pracy w tych systemach informatycznych adekwatne do realizowanych zadań, co było zgodne z § 20 ust. 2 pkt 4 *rozporządzenia KRI*.

(dowód: akta kontroli str. 225-237, 271-327)

W okresie po 1 czerwca 2017 r. jedna osoba zakończyła pracę w Urzędzie. Osoba ta była pracownikiem obsługi i nie pracowała na stanowisku umożliwiającym dostęp do systemów informatycznych wymagających utworzenia konta.

(dowód: akta kontroli str. 238-240)

Komputery w Urzędzie były zarządzane centralnie w oparciu o mechanizmy Microsoft Active Directory[9]. W systemie komputerowym Urzędu dopuszczalne były następujące sposoby autoryzacji w trakcie logowania do zasobów komputerowych (komputerów stacjonarnych lub przenośnych) podłączonych do tej usługi:

- ✓ logowanie do konta użytkownika w usłudze Active Directory (dalej: „AD") z wykorzystaniem loginu i hasła (minimalna długość hasła: 8 znaków, hasło musiało zawierać duże i małe liter oraz cyfry lub znaki specjalne;
- ✓ logowanie do konta użytkownika w usłudze AD z wykorzystaniem karty mikroprocesorowej (certyfikatu) zabezpieczonej PIN (hasłem). Przeprowadzony

[8] Formularz – „Zlecenie nadania lub modyfikacji uprawnień użytkownika".

[9] Usługa ta używa strukturalnego magazynu danych jako podstawy dla logicznej i hierarchicznej organizacji informacji katalogowych, przechowuje informacje dotyczące obiektów w sieci i ułatwia administratorom i użytkownikom znaleźć i używać tych informacji.

test na próbie 14 użytkowników[10] polegający na oględzinach wybranych losowo stanowisk pod kątem złożoności stosowanych haseł i PIN, wykazał, że w 10 przypadkach hasło miało od 8 do 10 znaków, natomiast w czterech przypadkach hasło (PIN) przy logowaniu za pomocą karty kryptograficznej miało długość od 8 do 11 znaków.

W zależności od dostępnych opcji programy przypominają o terminie zmiany hasła lub wymuszają jego zmianę. Dla programów stosowanych do przetwarzania danych stosowano jednolitą politykę haseł[11]. Nie wszystkie programy w Urzędzie korzystały z pojedynczego logowania i były synchronizowane z usługą AD. W trakcie przeprowadzanej kontroli Urząd był jednak w trakcie wymiany kluczowych systemów informatycznych w ramach, której planowane było uruchomienie pojedynczego logowania wraz z synchronizacja nowych systemów z usługą AD. W toku przeprowadzonych weryfikacji trzech systemów informatycznych[12] stwierdzono, że nie pozwalały one z poziomu aplikacji, na zarządzanie ochroną przetwarzanych informacji przed nieautoryzowanym dostępem poprzez ustanawianie zasad złożoności hasła dostępowego oraz okresów, po jakim hasło użytkownika powinno być zmienione.

Oględziny 10 stanowisk pracy, w tym ośmiu realizujących zadania związane z obsługą klienta wykazały, że ich monitory były usytuowane w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione. Powyższe działania spełniały wymogi § 20 ust. 2 pkt 7 *rozporządzenia KRI*.

(dowód: akta kontroli str. 210-218)

Zasady pracy z komputerami przenośnymi w Urzędzie określał „Regulamin użytkowania komputerów przenośnych", stanowiący część „Instrukcji Zarządzania Systemem Informatycznym". Wymagał on od użytkownika przede wszystkim zabezpieczenia fizycznego użytkowanego komputera, nie pozostawiania go bez nadzoru, a także nie udostępniania go osobom trzecim. Procedura ta wymagała również chronienia wyświetlanych na monitorze informacji w trakcie pracy przed wglądem osób nieuprawnionych. W procedurze tej brak było natomiast regulacji dotyczących obowiązku podłączania tych urządzeń do sieci Urzędu w celu aktualizacji na nich oprogramowania. Należy jednak podkreślić, iż Urząd posiadał wdrożoną procedurę centralnego mechanizmu zarządzania aktualizacjami, co z punktu bezpieczeństwa nie stanowiło zagrożenia w zakresie bezpieczeństwa informacji.

Radni Rady Miejskiej w Kątach Wrocławskich oraz sołtysi i przewodniczący rad osiedli korzystali z 64 komputerów przenośnych[13], użyczonych im przez Urząd na czas pełnienia funkcji.

(dowód: akta kontroli str. 210-224, 241-244)

Dane zgromadzone na urządzeniach mobilnych były zabezpieczone (zaszyfrowane) w sposób uniemożliwiający dostęp do nich osób nieuprawnionych, co było zgodne z § 20 ust. 2 pkt 9 i 11 *rozporządzenia KRI*.

(dowód: akta kontroli str. 245)

Wszystkie serwerownie w Urzędzie były zlokalizowane w odrębnym zamykanym pomieszczeniu, wyposażonym m.in.: w klimatyzację, dedykowane zasilanie

[10] Osiem komputerów stacjonarnych i sześć laptopów.
[11] Minimalna długość hasła 8 znaków, poziom skomplikowania hasła: hasło musi zawierać duże i małe liter oraz z cyfr lub znaki specjalne.
[12] Sigid, Optiest, Kadry.
[13] Radni - 21 sztuk, sołtysi i przewodniczący rad osiedli - 43 sztuki.

elektryczne oraz system zasilania zapasowego i automatyczny system gaszenia, co zapewniało zabezpieczenie informacji wynikające z § 20 ust. 2 pkt 9 *rozporządzenia KRI*.

(dowód: akta kontroli str. 246-266)

W okresie objętym kontrolą Urząd zawarł łącznie osiem umów dotyczących zakupu i serwisowania sprzętu komputerowego, a także instalacji i aktualizacji oprogramowania. Wszystkie one zawierały zapisy gwarantujące zachowanie odpowiedniego poziomu bezpieczeństwa informacji. Powyższe było zgodne z wymogami § 20 ust. 2 pkt 10 *rozporządzenia KRI*.

(dowód: akta kontroli str. 328-373)

Obowiązująca w badanym okresie „Procedura wykonywania przeglądów i konserwacji" wymagała naprawy dysków twardych w miejscu użytkowania. Wszystkie kluczowe urządzenia (serwery, macierze dyskowe) oraz stacje robocze i komputery przenośne wykorzystywane w Urzędzie kupowane były z polisami serwisowymi gwarantującymi serwis i naprawę sprzętu w miejscu eksploatacji oraz zapewniającymi pozostawienie dysku twardego w posiadaniu Urzędu w przypadku konieczności jego wymiany. W przypadku konieczności naprawy urządzeń w serwisie autoryzowanym producenta sprzętu dyski twarde były wymontowywane (i pozostawały zabezpieczone w Urzędzie) przed przekazaniem sprzętu do serwisu.

(dowód: akta kontroli str. 190-191, 197-198, 374)

Aktualizacja oprogramowania systemowego realizowana była z wykorzystaniem usługi Windows Update. Komputery automatycznie pobierały aktualizacje bezpośrednio z serwerów aktualizacji. Aktualizacja poprawek obywała się automatycznie przy wyłączeniu komputera. Według stanu na dzień 23 sierpnia 2018 r. do systemu informatycznego Urzędu podłączonych było 79 stanowisk komputerowych, z czego: 68 komputerów stacjonarnych i 11 laptopów. Na użytkowanych przez pracowników Urzędu stanowiskach komputerowych zainstalowane były systemy w wersjach posiadających wsparcie producenta. Wyjątkiem było jedno stanowisko, które posiadało nieobsługiwane serwisowo oprogramowanie Windows XP PRO SP3.

(dowód: akta kontroli str. 210-212, 216-217, 375-377)

Obowiązek tworzenia kopii zapasowej w Urzędzie został uregulowany w „Procedurze tworzenia kopii zapasowych", stanowiącej część „Instrukcji Zarządzania Systemem Informatycznym". Kopie zapasowe danych i aplikacji zlokalizowanych na serwerach Urzędu tworzone były w sposób zautomatyzowany w oparciu o harmonogramy określone w wyspecjalizowanym oprogramowaniu do tworzenia kopii bezpieczeństwa. Jak stwierdzono w toku przeprowadzonych oględzin zapasowe kopie danych wykonywane były w modelu dwustopniowym – pierwszą kopię sporządzano na dysku, a drugą na taśmie. Pierwsze kopie zapasowe umieszczane były na zasobie dyskowym w wydzielonej sieci. Kopie wykonywane były według planów (harmonogramów) zdefiniowanych dla danych rodzajów serwerów (fizyczne, wirtualne) oraz w zależność od typów i zakresów danych przechowywanych na serwerach. Zestawy taśm zawierające kopie dzienne i tygodniowe przechowywane były w innym budynku. Taśmy zawierające kopie miesięczne przechowywane były przez okres 12 miesięcy w ognioodpornym sejfie w innej do powyżej lokalizacji. Dostęp do kopii zgodnie z procedurą posiadali: ABI, ASI a także pracownicy Urzędu mający w zakresie czynności wpisany nadzór nad sejfem w danej lokalizacji.

Urząd nie prowadził w badanym okresie testów związanych z odtwarzaniem zapisanych danych systemów informatycznych i traktuje te dane, jako zbiór danych

historycznych. Należy podkreślić jednak, że na potrzeby Urzędu stworzono trzy niezależne maszyny wirtualne, które posiadały bieżące dane online i w razie awarii jednej z nich system przełączał się na inną drugą lub trzecią maszynę, co zapewnia przestrzeganie wymogów określonych w § 20 ust. 2 pkt 7 oraz pkt 12 lit. b i e *rozporządzenia KRI*.

(dowód: akta kontroli str. 246-262, 378-380)

Urząd dla ochrony swoich zasobów informacyjnych stosował oprogramowanie antywirusowe. W toku przeprowadzonych w dniu 19 lipca 2018 r. i dniu 9 sierpnia 2018 r. oględzin 14 komputerów stwierdzono, że we wszystkich badanych przypadkach oprogramowanie to posiadało definicje wirusów pochodzące z dnia badania, co było zgodne z § 20 ust. 2 pkt 12 lit. f *rozporządzenia KRI*.

(dowód: akta kontroli str. 210-212, 216-217)

W Urzędzie nie obowiązywały procedury dotyczące monitorowania pojemności nośników pamięci systemów urzędu, a także nie stosowano oprogramowania automatyzującego monitorowanie pojemności pamięci masowych (dysków twardych) wykorzystywanych w serwerach. Monitoring taki był prowadzony ręcznie przez Informatyka. W toku przeprowadzonych w dniu 17 lipca 2018 r. oględzin wszystkich serwerów wykorzystywanych przez tą jednostkę ustalono, że ich dyski twarde lub partycje na dyskach były zajęte od 6% do 96% pojemności.

(dowód: akta kontroli str. 246-257)

W okresie objętym kontrolą w Urzędzie nie funkcjonowały procedury zarządzania zmianą w zakresie oprogramowania. Jednakże w „Instrukcji Zarzadzania Systemem Informatycznym", w części „Procedura wykonywania przeglądów i konserwacji" zapisano, że ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz dostępną wiedzą co do bezpieczeństwa i stabilności nowych wersji, a także odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych. W dokumencie „Deklaracja stosowania[14]" aby zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji wyszczególniono proces zarządzania zmianami, jednak nie został on szczegółowo opisany.

Zarządzanie zmianami w systemie teleinformatycznym Urzędu, jak wyjaśnił ABI, z uwagi na brak środowiska testowego, w praktyce realizowane było poprzez wstępną instalację nowego oprogramowania bądź aktualizacji (takich jak np. nowych wersji oprogramowania antywirusowego) na kilku wybranych stanowiskach przed ich instalacją na wszystkich stacjach roboczych.

(dowód: akta kontroli str.190-191, 381)

W Urzędzie był prowadzony rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania w imieniu administratora. Dla każdego z 53 zidentyfikowanych podzbiorów, zawartych w „Rejestrze czynności przetwarzania" określono zgodnie z wymaganiami art. 30 ust. 1 *RODO*: nazwę administratora i jego dane kontaktowe, dane inspektora danych osobowych, cel przetwarzania danych, kategorię osób, kategorię danych osobowych; kategorię odbiorców, którym dane osobowe zostaną ujawnione, planowane terminy usunięcia poszczególnych kategorii danych; opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 *RODO*.

(dowód: akta kontroli str. 382-388)

---

[14] Celem tego dokumentu jest określenie, które zabezpieczenia zostaną zastosowane w organizacji, jakie są cele tych zabezpieczeń, jak zostaną one wdrożone jak również zatwierdzenie ryzyk szczątkowych oraz formalne zatwierdzenie wdrożenia odnośnych zabezpieczeń.

Ustalona nieprawidłowość

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

W przypadku dwóch z 14 poddanych oględzinom stanowisk komputerowych stwierdzono, że pracownicy Urzędu posiadali uprawnienia administratora, mimo iż nie byli administratorem systemów informatycznych. Pracownikom tym, wbrew wymogom § 20 ust. 2 pkt 4 *rozporządzenia KRI*, umożliwiono instalowanie dowolnego oprogramowania. Z wyjaśnień ABI wynika, że *prawa te były nadane historycznie użytkownikom na potrzeby poprawnego działania i uruchamiania starszych wersji aplikacji mapowych EDIOM oraz MapView.* W trakcie oględzin uprawnienia do instalacji oprogramowania na obu komputerach zostały odebrane użytkownikom, nadano im uprawnienia standardowe.

(dowód: akta kontroli str. 207-224)

Uwaga dotycząca badanej działalności

NIK zwraca uwagę, że zajętość przestrzeni dyskowej nie powinna przekraczać 80%. Odpowiednia wolna zawartość dyskowa umożliwia sprawną pracę systemu, a jego skuteczne monitorowanie pozwala na wcześniejsze przygotowanie się do zwiększenia dostępnej pojemności.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości wdrożone i wykorzystywane przez Urząd rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

W okresie objętym kontrolą Urząd nie prowadził samodzielnie okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji. Jedynie w roku 2017 zgodnie z planem sprawozdań ochrony danych osobowych ABI przeprowadził samodzielnie dwa sprawdzenia związane z przetwarzaniem danych osobowych. W ich ramach weryfikowano prawidłowość funkcjonowania mechanizmów kontroli do zbiorów danych, a także poprawność upoważnień i uprawnień nadanych do przetwarzania danych osobowych pracownikom Urzędu.

Jednocześnie w dniach 3-5 kwietnia 2017 r. firma zewnętrzna na podstawie zawartej z Urzędem umowy przeprowadziła audyt bezpieczeństwa informacji. Jednym z jego elementów było zweryfikowanie ryzyka utraty integralności, poufności i dostępności, o których mowa w § 20 ust. 2 pkt 3 *rozporządzenia KRI*.

(dowód: akta kontroli str. 416-513, 549-554)

W Urzędzie opracowano i wprowadzono procedury dotyczące zgłaszania wszelkich incydentów związanych z bezpieczeństwem, zapoznano z nimi również pracowników. Według informacji udzielonych przez ABI, a także rejestru incydentów bezpieczeństwa (naruszeń) w Urzędzie w badanym okresie nie wystąpiły incydenty związane z bezpieczeństwem informacji.

(dowód: akta kontroli str. 389-396)

W latach 2017-2018 w Urzędzie prowadzono szkolenia wewnętrzne i zewnętrzne pracowników zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem zagrożenia bezpieczeństwa informacji, skutków naruszenia tych zasad, w tym odpowiedzialności prawnej za te czyny oraz stosowania środków zapewniających bezpieczeństwo informacji. Wszyscy pracownicy Urzędu zostali przeszkoleni przez firmę zewnętrzną z bezpieczeństwa pracy w systemach teleinformatycznych, co było zgodne z § 20 ust. 2 pkt 6 *rozporządzenia KRI*.

(dowód: akta kontroli str. 397-415)

W latach 2017-2018 w Urzędzie przeprowadzono dwa audyty, weryfikacje zewnętrzne z zakresu bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt 14 *rozporządzenia KRI*. Zalecenia jakie zostały wskazane po audycie w roku 2017 zostały przez Urząd zrealizowane, dotyczyły one m.in.: przeprowadzania regularnych szkoleń dla pracowników z legalności oprogramowana, czy też bezpieczeństwa informatycznego oraz stosowania prawidłowych procedur zakupu i rozprowadzania oprogramowania. W roku 2018 dokonano natomiast weryfikacji, aktualizacji i wdrożeniu dokumentacji związanych z przetwarzaniem danych osobowych w zakresie wymogów *RODO*.

(dowód: akta kontroli str. 416-513)

Realizując wymogi określone w art. 32 ust. 1 *RODO* Urząd dokonał analizy ryzyk istniejących w procesach przetwarzania danych osobowych w jednostce.

(dowód: akta kontroli str. 543-548)

W toku przeprowadzonej analizy stwierdzono, że w Urzędzie w okresie objętym kontrolą wszyscy nowo zatrudnieni pracownicy przechodzili obowiązkowe szkolenie wstępne realizowane wewnętrznie przez ABI z zakresu ochrony danych osobowych, zagrożeń występujących przy przetwarzaniu danych i sposobów im przeciwdziałania w ramach organizacji. Pracownik po takim szkoleniu składał oświadczenie, że zapoznał się z dokumentacją ochrony danych osobowych, regulaminem ochrony danych osobowych, zasadami bezpiecznej pracy i obowiązkiem informacyjnym. Ponadto dla wszystkich pracowników Urzędu realizowane były rokrocznie szkolenia przeprowadzane przez podmioty zewnętrzne. W roku 2017 dla 59 pracowników zostało zrealizowane szkolenie z zakresu bezpieczeństwa pracy w systemach teleinformatycznych, a w roku 2018 dla 65 pracowników firma zewnętrzna wykonała szkolenie w temacie wymagań oraz stosowanych procedur i regulacji w Urzędzie w kontekście zmian, jakie w tym zakresie wnosi wdrożenie przepisów *RODO*.

(dowód: akta kontroli str. 397-415, 515-533)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działania Urzędu podejmowane w celu zapobiegania incydentom bezpieczeństwa informacji.

IV. Wnioski

Wnioski pokontrolne

Najwyższa Izba Kontroli, mając na uwadze postanowienia art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. *o Najwyższej Izbie Kontroli*[15] (dalej: „*ustawa o NIK*"), odstępuje od formułowania wniosków pokontrolnych ze względu na usunięcie stwierdzonej nieprawidłowości jeszcze w toku niniejszej kontroli.

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 we Wrocławiu.

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag

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.

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.

Wrocław, dnia 06 września 2018 r.

Kontroler:
Waldemar Zimoch
Główny specjalista kontroli państwowej

podpis

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
Dyrektor

DYREKTOR
Delegatura Najwyższej Izby Kontroli
we Wrocławiu
z up.
podpis
Zdzisław Florkowski
Wicedyrektor