NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR.410.015.02.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie
ul. Łobzowska 67, 30-038 Kraków
T +48 12 342 34 00, F +48 12 342 34 44
lkr@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/18/006 – *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Krakowie
Kontroler	Małgorzata Kram, specjalista kontroli państwowej, upoważnienie do kontroli nr LKR.130.2018 z 22 czerwca 2018 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Starostwo Powiatowe w Myślenicach, ul. Mikołaja Reja 13, 32-400 Myślenice (*Starostwo* lub *Urząd*)
Kierownik jednostki kontrolowanej	Józef Tomal – Starosta Myślenicki (*Starosta)* (dowód: akta kontroli str. 66)

II. Ocena kontrolowanej działalności

Ocena ogólna[1]

Najwyższa Izba Kontroli ocenia negatywnie działania Starosty w zakresie zarządzania bezpieczeństwem informacji w Urzędzie, w kontrolowanym okresie[2], pomimo podejmowania pewnych działań na rzecz zapewnienia bezpieczeństwa informacji.

W Starostwie nie zapewniono należytej organizacji bezpieczeństwa informacji, nie wprowadzono odpowiednich zabezpieczeń technicznych w celu zapewnienia ochrony przetwarzanych informacji, nie podjęto wystarczających działań mających na celu zapobieganie incydentom bezpieczeństwa.

Stwierdzone nieprawidłowości polegały w szczególności na:

- nieopracowaniu i niewdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w szczególności zaktualizowanej Polityki Bezpieczeństwa Informacji (PBI), co stanowiło naruszenie § 20 ust. 1 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[3];
- niezaktualizowaniu obowiązującej w Urzędzie dokumentacji w zakresie ochrony danych osobowych pod kątem dostosowania do wymogów wynikających z przepisów 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)[4], co było działaniem nierzetelnym;
- niezagwarantowaniu realizacji zadań Inspektora Ochrony Danych (IOD) w sposób niezależny, co było niezgodne z art. 38 ust. 3 rozporządzenia RODO,
- posiadaniu uprawnień administratora systemu nieadekwatnych do realizowanych zadań przez 7 z 10 pracowników Starostwa objętych badaniem NIK, co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia RM w sprawie KRI;

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

[2] Kontrolą objęto okres od 1 czerwca 2017 r. do dnia zakończenia kontroli.

[3] Dz. U. z 2017 r. poz. 2247, dalej: *rozporządzenie RM w sprawie KRI*.

[4] Dz. Urz. UE L119 z 4.05.2016, str. 1, ze zm., dalej: *rozporządzenie RODO*.

- nieustanowieniu procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co stanowiło naruszenie § 20 ust. 2 pkt 8 rozporządzenia RM w sprawie KRI;
- nieprzeprowadzaniu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co było niezgodne z § 20 ust. 2 pkt 3 rozporządzenia RM w sprawie KRI;
- nieprzeprowadzeniu analizy procesów przetwarzania danych, o której mowa w art. 32 rozporządzenia RODO.

Należy przy tym zauważyć, że inne zadania i obowiązki wykonywane przez osobę pełniącą w Urzędzie zarówno funkcję IOD i informatyka, jak i funkcję Administratora Systemów Informatycznych (ASI) mogą powodować konflikt interesów, o którym mowa w art. 38 ust. 6 rozporządzenia RODO.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

W Urzędzie nie opracowano i nie wdrożono SZBI. Obowiązujące w Starostwie: polityka bezpieczeństwa danych osobowych oraz *Instrukcja Zarządzania Systemami Informatycznymi* dotyczyły bezpieczeństwa danych osobowych. Wszyscy pracownicy Urzędu zaangażowani w proces przetwarzania danych osobowych zostali zapoznani z obowiązującą dokumentacją w zakresie ochrony danych osobowych podczas szkoleń przeprowadzonych w Starostwie. W zarządzeniach wprowadzających uregulowania w zakresie bezpieczeństwa danych osobowych zobowiązano wszystkich pracowników do stosowania zasad określonych w tych dokumentach.

(dowód: akta kontroli str. 3-9, 14-17, 19-48, 145-148, 205-206)

W związku z wejściem w życie przepisów rozporządzenia RODO, w Urzędzie nie przeprowadzono aktualizacji dokumentacji w zakresie ochrony danych osobowych pod kątem dostosowania do wymogów tego rozporządzenia.

(dowód: akta kontroli str. 3-17, 19-48)

W czasie kontroli NIK w Starostwie rozpoczęto audyt zewnętrzny (m.in. w zakresie inwentaryzacji procesów przetwarzania danych oraz zbiorów danych osobowych, analizy dokumentacji administracyjnej, analizy aktualnych zabezpieczeń, analizy zawartych umów dotyczących przetwarzania danych osobowych, analizy ryzyk i zagrożeń, wydania rekomendacji wdrożenia zabezpieczających środków technicznych i organizacyjnych) wykonywany przez kancelarię radcowską na podstawie umowy ZI.142.2.2018 z 10 lipca 2018 r. Audyt zaplanowano do 30 września 2018 r. (do zakończenia kontroli NIK nie otrzymano jego wyników).

(dowód: akta kontroli str. 3-9, 16-17, 149-159)

Starosta wyjaśnił, że przeprowadzono postępowanie konkursowe w celu wyłonienia zewnętrznego, niezależnego podmiotu, którego zadaniem byłoby przygotowanie i zaktualizowanie dokumentacji prawnej związanej z wdrożeniem przepisów rozporządzenia RODO. Zakończenie prac przewidziano do 30 września 2018 r.

(dowód: akta kontroli str. 160-164)

Starosta wyznaczył pracowników Urzędu na stanowiska odpowiedzialne za bezpieczeństwo informacji[5], tj. Administratora Bezpieczeństwa Informacji (ABI) – do 24 maja 2018 r., oraz IOD (od 25 maja 2018 r.). W zarządzeniach zostały określone podstawowe zakresy obowiązków na tych stanowiskach. Tylko w przypadku stanowiska ABI wskazano, że podlega bezpośrednio Staroście. Ponadto w Urzędzie funkcjonował Referat Informatyki, w zakresie którego leżały m.in. sprawy związane z rozwojem, wdrażaniem i eksploatacją

[5] 25 maja 2018 r., na podstawie art. 158 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1 000), funkcję IOD zaczął pełnić główny specjalista (informatyk) – od 2 sierpnia 2004 r. Administrator Bezpieczeństwa Informacji. Starosta powołał IOD 1 sierpnia 2018 r. (zarządzeniem nr 94/2018, przy czym w zarządzeniu zamiennie używano nazwy: *Inspektor Ochrony Danych* i *Inspektor Ochrony Danych Osobowych*, a w zakresie czynności skupiono się w zasadzie na działaniach dotyczących przetwarzania danych osobowych).

systemów informatycznych. Pracownicy Referatu dysponowali odpowiednimi kompetencjami (wykształcenie, praktyka zawodowa), umożliwiającymi prawidłowe wykonywanie powierzonych im zadań.

(dowód: akta kontroli str. 3-15, 101-114)

Zgodnie z art. 37 ust. 1 rozporządzenia RODO, zarządzeniem nr 94/2018 Starosty z 1 sierpnia 2018 r., został powołany IOD. Zgodnie z art. 37 ust. 5 rozporządzenia RODO wyznaczony IOD posiadał odpowiednie kwalifikacje zawodowe do pełnienia tej funkcji. Regulamin organizacyjny Urzędu nie uwzględniał stanowiska IOD i nie gwarantował niezależności jego działań poprzez bezpośrednią podległość Staroście. Osoba wyznaczona na IOD była jednocześnie zatrudniona na stanowisku informatyka oraz realizowała zadania ASI.

(dowód: akta kontroli str. 3-15, 101-114)

W Urzędzie zidentyfikowano zbiory przetwarzanych danych podlegające zabezpieczeniu. Posiadane zasoby baz danych obejmowały 24 zbiory, przy czym w formie elektronicznej prowadzono 7 z nich.

(dowód: akta kontroli str. 3-9, 16-17, 58-63, 119)

Jednostka posiadała aktualne informacje o zasobach informatycznych obejmujące ich rodzaj i konfigurację zgodnie z wymogami § 20 ust. 2 pkt 2 rozporządzenia RM w sprawie KRI. Zasoby teleinformatyczne Starostwa 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 elektronicznego. Badanie oparte o dobór celowy 15 użytkowanych urządzeń[6] wykazało, że system ten zawierał pełną informację o ww. zasobach teleinformatycznych.

(dowód: akta kontroli str. 3-9, 16-18, 73-79, 119-144, 165-198)

Ustalone nieprawidłowości

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

1. W Urzędzie nie opracowano i nie wdrożono SZBI, w szczególności nie wdrożono zaktualizowanej PBI.
Było to niezgodne z § 20 ust. 1 rozporządzenia RM w sprawie KRI, w myśl którego podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Z § 20 ust. 3 rozporządzenia RM w sprawie KRI wynika, że wymagania określone w ust. 1 tego paragrafu uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001[7], a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[8]. W pkt 5.1 Polskiej Normy PN-EN ISO/IEC 27002 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji.

Starosta wyjaśnił, że aktualizacja dokumentów dotyczących bezpieczeństwa informacji została zlecona firmie zewnętrznej w lipcu 2018 r. i ma zostać przygotowana do 30 września 2018 r.

(dowód: akta kontroli str. 160-164)

2. W Urzędzie nie przeprowadzono aktualizacji uregulowań wewnętrznych w zakresie ochrony danych osobowych, pod kątem ich dostosowania do wymogów w zakresie ochrony danych osobowych w związku z wejściem w życie przepisów rozporządzenia RODO, co było działaniem nierzetelnym.

---

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

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

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

Według wyjaśnień Starosty przed wejściem w życie przepisów rozporządzenia RODO osoba pełniąca funkcję ABI, dokonała oceny faktycznej procesów przetwarzania danych osobowych Starostwa i stwierdziła, że stosowane w Urzędzie w/w środki techniczne i organizacyjne były adekwatne do występujących ryzyk. Jednocześnie ABI zastrzegł, że ryzyka te powinny zostać zweryfikowane przez zewnętrzny, niezależny podmiot, z którym zostanie podpisana umowa na wdrożenie przepisów rozporządzenia RODO, ze względu na złożoność tego rozporządzenia, brak krajowych przepisów na dzień dokonania oceny (ustawa o ochronie danych osobowych ukazała się dzień przed wejściem w życie rozporządzenia RODO), a także brak szczegółowych wytycznych, co do sposobu przeprowadzenie oceny. Do tej pory nie było również dostępnych kodeksów postępowania, które zgodnie z art. 40 rozporządzenia RODO pomogłyby właściwie stosować rozporządzenie. Obecnie przedmiotem analizy w Urzędzie jest opracowany przez wykonawcę usługi wdrożenia rozporządzenia RODO dokument pn. *Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych w zakresie spełnienia wymagań europejskiego rozporządzenia o ochronie danych osobowych (RODO) w Starostwie Powiatowym w Myślenicach*.

(dowód: akta kontroli str. 160-164, 207-211)

3. W Starostwie nie zagwarantowano IOD wykonywania obowiązków w sposób niezależny, co było niezgodne z art. 38 ust. 3 rozporządzeniem RODO.
Zgodnie z tym przepisem IOD podlega bezpośrednio najwyższemu kierownictwu. Do regulaminu organizacyjnego Urzędu nie wprowadzono zapisów o utworzeniu stanowiska IOD i jego bezpośredniej podległości Staroście.

Starosta wyjaśnił, że nie dokonywano zmiany w regulaminie organizacyjnym, ale w zarządzeniu powołującym ABI, który następnie został IOD, wskazano, że podlega on bezpośrednio Staroście. Ponadto podał, że ponieważ drugi pracownik działu IT złożył w lipcu wypowiedzenie tymczasowo zlecił zadania IOD informatykowi, który zajmował się praktyczną częścią zapewnienia bezpieczeństwa informacji, natomiast cele przetwarzania danych były w gestii naczelników wydziałów i kierownictwa Urzędu. Z uwagi na wagę ochrony danych osobowych, nadzorowaną przez GIODO/UODO, skupiono się w dokumentach na ochronie danych osobowych, a przez przeoczenie użyto zamiennie nazwy IOD i Inspektor Ochrony Danych Osobowych. Obecnie przygotowywane jest zarządzenie prostujące omyłkowe użycie nazwy IOD oraz trwa przygotowanie do naboru na stanowisko informatyka pełniącego rolę koordynatora pracami IT w Starostwie.

(dowód: akta kontroli str. 160-164, 207-211)

4. W Urzędzie od 2004 r. nie przeprowadzono aktualizacji informacji o posiadanych i przetwarzanych aktywach informacyjnych, co było działaniem nierzetelnym.
Aktualizacji tej dokonano dopiero w trakcie kontroli NIK. Stosownie do pkt A.8.1.1 Polskiej Normy PN-EN ISO/IEC 27001 należy zidentyfikować informacje, aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów.

Starosta wyjaśnił, że w Urzędzie trwa aktualizacja dokumentacji.

(dowód: akta kontroli str. 160-164, 207-211)

Uwaga dotycząca kontrolowanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że inne zadania i obowiązki wykonywane przez osobę pełniącą w Starostwie funkcję IOD mogą powodować konflikt interesów, o którym mowa w art. 38 ust. 6 rozporządzenia RODO. W opinii NIK, osoba powołana na IOD w Starostwie, będąc jednocześnie informatykiem oraz ASI, uczestniczy w określaniu celów i sposobów przetwarzania danych osobowych w Urzędzie, zatem nie spełnia wymogu określonego w ww. przepisie. W myśl art. 38 ust. 6 rozporządzenia RODO, osoba wyznaczona na IOD może wykonywać inne zadania i obowiązki, jednak administrator danych musi zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Starosty w zakresie organizacji bezpieczeństwa informacji. Ocenę taką uzasadnia m.in. nieopracowanie i niewdrożenie w Urzędzie kompleksowego SZBI, w tym aktualizacji informacji o zbiorach danych podlegających zabezpieczeniu, oraz niezapewnienie dostosowania dokumentacji do wymogów wynikających z rozporządzenia RODO. Ponadto ustalono, że inne zadania

i obowiązki wykonywane przez osobę będącą równocześnie IOD oraz ASI mogą powodować konflikt interesów gdyż osoba ta jako informatyk uczestniczy w określaniu celów i sposobów przetwarzania danych osobowych w Urzędzie.

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

Opis stanu faktycznego

Uprawnienia użytkowników 7 z 10 komputerów objętych oględzinami pozwalały na zainstalowanie nieautoryzowanego oprogramowania. Było to niezgodne z § 20 ust. 2 pkt 4 rozporządzenia RM w sprawie KRI.

(dowód: akta kontroli str. 64-72, 115-118, 165-198)

Zasady obowiązujące przy nadawaniu, modyfikowaniu i odbieraniu uprawnień użytkownikom systemów informatycznych określono w § 3 *Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Myślenicach*[9] (*Instrukcja*).
Analiza zadań służbowych realizowanych przez 15 pracowników Starostwa[10] (w tym 5 na stanowiskach kierowniczych) wykazała, że każdy z nich, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia RM w sprawie KRI, uczestniczył w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań.

(dowód: akta kontroli str. 64-72, 80-96)

Kontrolą objęto uprawnienia do dostępu, do systemów informatycznych 15 wybranych osób, które w okresie od 1 czerwca 2017 r. do 31 lipca 2018 r. zakończyły zatrudnienie w Urzędzie i realizowały zadania z wykorzystaniem systemów informatycznych. Stwierdzono, że dostęp do systemów informatycznych dla 13 osób został zablokowany. Pozostałe 2 osoby zostały ponownie zatrudnione w Urzędzie od 1 sierpnia 2018 r., w związku z czym pozostawiono im uprawnienia do pracy w systemach informatycznych.

(dowód: akta kontroli str. 64-72, 80-96, 165-198)

Realizując wymogi § 20 ust. 2 pkt 7 rozporządzenia RM w sprawie KRI, jako zabezpieczenia techniczne wprowadzone w systemach informatycznych Urzędu w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem zastosowano:

- wprowadzenie unikalnych identyfikatorów użytkowników,
- haseł dostępu o wymuszanej przez Windows 10 złożoności i sile (8 znaków, przynajmniej jedna duża litera, przynajmniej jedna cyfra),
- centralne zarządzanie komputerami.

(dowód: akta kontroli str. 73-79, 165-198)

Oględziny wykazały, że ustawienie monitorów na 5 wybranych stanowiskach pracy obsługujących obywateli w zakresie rejestracji pojazdów i wydawania prawa jazdy zapewniało, że dane wyświetlane na ekranie nie były widoczne dla osób nieuprawnionych. Było to zgodne z § 20 ust. 2 pkt 7 rozporządzenia RM w sprawie KRI.

(dowód: akta kontroli str. 18, 165)

Pracownicy Urzędu korzystali z 14 komputerów przenośnych. W Urzędzie nie ustanowiono zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 9 rozporządzenia RM w sprawie KRI.

(dowód: akta kontroli str. 14-17, 19-48, 115-118)

W komputerach przenośnych, będących w posiadaniu Starostwa, nie stosowano szyfrowania dysków twardych.

(dowód: akta kontroli str. 3-9, 16)

W serwerowni Urzędu zapewniono rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwerów i urządzeń sieciowych. Zastosowane

[9] Stanowiącej załącznik nr 2 do dokumentacji dotyczącej przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w Starostwie, ustalonej zarządzeniem nr 42/2004 Starosty z 27 października 2004 r.

[10] W badanym okresie nie było pracowników, którzy w okresie objętym kontrolą zmienili komórkę organizacyjną.

rozwiązania, służące zabezpieczeniu serwerowni, w wystarczającym stopniu chroniły pomieszczenie, co było zgodne z wymogami § 20 ust. 2 rozporządzenia RM w sprawie KRI.

(dowód: akta kontroli str. 16-18, 119-144)

Badanie umowy na zakup sprzętu informatycznego[11], wykazało, że w umowie tej nie zawarto zapisów mówiących o zobowiązaniu wykonawcy do zachowania w tajemnicy informacji, do jakich może mieć dostęp w związku z realizacją umowy.

(dowód: akta kontroli str. 157-158)

Starosta wyjaśnił, że w przypadku zakupu sprzętu komputerowego Starostwo nie przewidywało możliwości naprawy dysków twardych przez podmioty zewnętrzne. Stosowaną metodą naprawy nośników informacji był zakup nowego sprzętu i wymiana przez pracowników Zespołu Informatycznego.

(dowód: akta kontroli str. 160-164, 207-211)

W Urzędzie nie ustalono zasad dotyczących przekazywania sprzętu IT poza jednostkę (np. do serwisu lub zbycie sprzętu). Ustalono, że w dniu 26 sierpnia 2017 r. nastąpiło przekazanie 32 sztuk komputerów z systemem Windows XP, niewykorzystywanych w Starostwie i *zużytych ekonomicznie* do miasta partnerskiego w ramach umowy zawartej 18 stycznia 2017 r. pomiędzy Powiatem Myślenickim a Obwodem Wierchowińskim. Dane zapisane na dyskach tych komputerów zostały trwale pozbawione informacji na nich zgromadzonych. Ponadto 29 grudnia 2017 r. nastąpiło przekazanie 8 szt. serwerów do gmin Powiatu Myślenickiego w związku z realizacją projektu *E-powiat*. Serwery te znajdowały się w ww. gminach na podstawie wcześniejszych umów użyczenia.

(dowód: akta kontroli str. 16-17, 155-159)

W Starostwie przeprowadzano aktualizacje oprogramowania (systemów operacyjnych), o których mowa w § 20 ust. 2 pkt 12 lit. a i f rozporządzenia RM w sprawie KRI, w tym aktualizacji oprogramowania antywirusowego. Nie stwierdzono wykorzystywania systemów operacyjnych, nieobjętych wsparciem producenta (np. *Windows XP*).

(dowód: akta kontroli str. 115-144, 165-198)

W Urzędzie przeprowadzano regularne tworzenie i testowanie kopii zapasowych danych i oprogramowania aplikacyjnego, w którym przetwarzane były dane stosownie do § 20 ust. 2 pkt 12 lit. b i e oraz § 20 ust. 2 pkt 7 rozporządzenia RM w sprawie KRI. Sprawdzanie kopii zapasowych dokonywane było codziennie, a proces tworzenia kopii został zautomatyzowany poprzez zastosowanie skryptu. Codzienne kopie nagrywano na taśmę, Urząd dysponował dwoma serwerowniami, a ponadto raz na tydzień kopia była przenoszona poza miejsce jej wytworzenia, do archiwum w innym budynku poza bazą. W Instrukcji określono zasady testowania kopii zapasowych, przy czym kontrola ustaliła, że w tym zakresie wykorzystywano własny skrypt do weryfikacji poprawności procesu tworzenia kopii komputerów/serwerów. W okresie objętym kontrolą nie wystąpiły przypadki konieczności odtworzenia danych z kopii zapasowych lub przywracania systemów.

(dowód: akta kontroli str. 19-144)

W Urzędzie wdrożono zabezpieczenia przed instalacją szkodliwego oprogramowania na komputerach wykorzystywanych przez pracowników zgodnie z § 20 ust. 2 pkt 12 lit. f rozporządzenia RM w sprawie KRI. 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.

(dowód: akta kontroli str. 15-17, 165-198)

Pojemność nośników pamięci systemów Urzędu była na bieżąco monitorowana przez informatyków i nie przekraczała progu ostrzegawczego na poziomie 80% zajętości przestrzeni. Działanie pracowników Urzędu było zgodne z zaleceniem sformułowanym w pkt A.12.1.3 załącznika A Polskiej Normy PN-ISO/IEC 27001:2017.

(dowód: akta kontroli str. 165-198)

[11] Umowa nr ZI.2600.22.2017 z 18 grudnia 2017 r.

W Starostwie nie przewidziano formalnych rozwiązań związanych z ryzykiem wystąpienia zakłóceń w normalnym funkcjonowaniu środowiska informatycznego w związku z wdrażaniem nowych wersji oprogramowania (dotyczących tzw. zarządzania zmianą).

(dowód: akta kontroli str. 16-48)

W Urzędzie, do września 2018 r. nie prowadzono rejestru czynności przetwarzania danych spełniającego wymogi art. 30 ust. 1 rozporządzenia RODO. Rejestr ten sporządzono dopiero w trakcie kontroli NIK.

(dowód: akta kontroli str. 16-17)

Starosta wyjaśnił, że dane osobowe w Starostwie Powiatowym w Myślenicach były usystematyzowane zgodnie z *Jednolitym Rzeczowym Wykazem Akt*, który prowadzony był odrębnie dla każdego z wydziałów. W chwili obecnej IOD dokonał konsolidacji danych zawartych w wykazie akt i dostosował ten dokument do wymogów rozporządzenia RODO, tworząc rejestr czynności przetwarzania danych osobowych.

(dowód: akta kontroli str. 160-164, 207-211)

Ustalone nieprawidłowości

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

1. Oględziny 10 stanowisk komputerowych w Urzędzie wykazały, że 7 pracowników posiadało uprawnienia administracyjne na użytkowanych przez nich komputerach. Było to niezgodne z § 20 ust. 2 pkt 4 rozporządzenia RM w sprawie KRI, w myśl którego zarządzanie bezpieczeństwem informacji jest realizowane między innymi przez podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.
Praktyka taka była niezgodna także z załącznikiem A Polskiej Normy PN-ISO/IEC 27001:2014-12 - punktem A.9.2.3, który stanowi, że przydzielanie i wykorzystywanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować.

Starosta wyjaśnił, że instalacji oprogramowania dokonywali wyłącznie informatycy poprzez zainstalowany program inwentaryzacyjny, zatem mieli oni możliwość bieżącego monitorowania zainstalowanych programów.

(dowód: akta kontroli str. 160-164, 207-211)

2. W Starostwie nie ustanowiono zasad (procedury) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia RM w sprawie KRI. Na komputerach przenośnych wykorzystywanych w Urzędzie nie stosowano rozwiązania polegającego na szyfrowaniu danych zgromadzonych na tych komputerach, co stanowiło naruszenie § 20 ust. 2 pkt 9 rozporządzenia RM w sprawie KRI.

(dowód: akta kontroli str. 238-333)

Starosta wyjaśnił, że ponieważ nie przewidywano zgody na wykorzystywanie urządzeń przenośnych poza terenem urzędu nie ustalano zasad posługiwania się takim sprzętem. Zakupiono szyfrowane pamięci przenośne do użytkowania dla poszczególnych wydziałów. W polityce bezpieczeństwa określono zakaz podłączania urządzeń mobilnych typu smartfon, tablet i żadne z tych urządzeń będących w posiadaniu Starostwa nie było podłączone do systemu informatycznego Starostwa.

(dowód: akta kontroli str. 160-164, 207-211)

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 Starostwa 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.

3. W Urzędzie w okresie do września 2018 r. nie prowadzono rejestru czynności przetwarzania danych spełniającego wymogi określone w art. 30 ust. 1 rozporządzenia RODO.

Starosta wyjaśnił, że rejestr został założony w trakcie kontroli NIK przez firmę wyłonioną do wdrożenia przepisów rozporządzenia RODO, a jego brak w Urzędzie wynikał ze skupienia się na ochronie newralgicznych danych osobowych.

(dowód: akta kontroli str. 160-164, 207-211)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działalność Starosty w zakresie funkcjonujących w Urzędzie rozwiązań organizacyjnych i technicznych, służących zapewnieniu bezpieczeństwa informacji. Negatywna ocena wynika z charakteru stwierdzonych nieprawidłowości, które dotyczyły:

- posiadania przez 7 pracowników (z 10 przypadków objętych kontrolą) uprawnień administracyjnych na użytkowanych przez nich komputerach, co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia RM w sprawie KRI;
- nieustaleniu szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych poza siedzibą Urzędu, gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 ww. rozporządzenia;
- nieprowadzenia rejestru czynności przetwarzania danych spełniającego wymogi określone w art. 30 ust. 1 rozporządzenia RODO (nieprawidłowość została usunięta w trakcie kontroli).

3. Realizacja działań w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

W Starostwie nie prowadzono okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia RM w sprawie KRI.

(dowód: akta kontroli str. 16-48)

W Urzędzie wskazano jako rejestr incydentów naruszenia bezpieczeństwa informacji, tj. realizacji obowiązku wynikającego z § 20 ust. 2 pkt 13 rozporządzenia RM w sprawie KRI, zapisy w § 7 obowiązującej w Starostwie od 2004 r. PBI, w której zamieszczono instrukcję postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 16-48, 164)

Urząd zapewnił szkolenia pracowników zaangażowanych w proces przetwarzania informacji stosownie do wymogów § 20 ust. 2 pkt 6 rozporządzenia RM w sprawie KRI. W okresie objętym kontrolą zorganizowano dwukrotnie (w styczniu 2017 r. i maju 2018 r.) szkolenia wewnętrzne dla pracowników w zakresie obowiązujących w Starostwie przepisów bezpieczeństwa informacji, bezpiecznej pracy w systemach informatycznych, ochrony danych i budynków, a także przepisów rozporządzenia RODO. Szkolenia były prowadzone przez ABI i ASI. Z zakresu bezpieczeństwa informacji zostali przeszkoleni wszyscy pracownicy Urzędu, co zostało potwierdzone podpisem na liście obecności. W okresie objętym kontrolą ABI i ASI uczestniczyli indywidualnie w szkoleniach zewnętrznych, obejmujących szczegółowe zagadnienia związane z wejściem w życie przepisów RODO.

(dowód: akta kontroli str. 16-17, 64-72, 145-148)

W Starostwie w 2017 r. przeprowadzono okresowy audyt wewnętrzny z zakresu bezpieczeństwa informacji stosownie do § 20 ust. 2 pkt 14 rozporządzenia RM w sprawie KRI, który wskazał m.in. na konieczność aktualizacji PBI. Do czasu kontroli NIK aktualizacja taka nie została przeprowadzona.

(dowód: akta kontroli str. 16-17, 49-57, 207)

W Urzędzie nie przeprowadzono analiza procesów przetwarzania danych, o której mowa w art. 32 ust. 1 rozporządzenia RODO.

(dowód: akta kontroli str. 16-48)

Ustalone nieprawidłowości

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

1. W Urzędzie nie przeprowadzano okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co było niezgodne z § 20 ust. 2 pkt 3 rozporządzenia RM w sprawie KRI, który stanowi, że zarządzanie bezpieczeństwem informacji jest realizowane m.in. poprzez przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

(dowód: akta kontroli str. 3-9, 16-48)

Starosta wyjaśnił, że przed wejściem w życie przepisów rozporządzenia RODO, Starostwo dokonało kontroli oraz wdrożyło w sposób faktyczny, we wszystkich swoich wydziałach, środki techniczne i organizacyjne zapewniające adekwatny do wymogów rozporządzenia RODO stopień bezpieczeństwa przetwarzanych danych osobowych. W Starostwie stosowane są m.in. następujące środki techniczne i organizacyjne:

- szyfrowanie danych osobowych na komputerach przenośnych pracowników;
- codzienne wykonywanie kopii zapasowych danych przetwarzanych w systemach informatycznych zapewniające integralność, dostępność i odporność przetwarzanych danych osobowych;
- przydział indywidualnych kont użytkowników systemu informatycznego;
- cykliczna (co 30 dni) zmiana indywidualnych haseł użytkowników systemów informatycznych;
- poinformowano pracowników o sposobie postępowania w przypadkach naruszenia ochrony danych osobowych (incydenty naruszenia danych osobowych).

(dowód: akta kontroli str. 160-164, 207-211)

Najwyższa Izba Kontroli wskazuje, że konieczność dokonywania cyklicznych analiz ryzyka utraty poufności, integralności i rozliczalności informacji wynika z przepisów rozporządzenia RM w sprawie KRI. Czynność ta powinna być udokumentowana. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od istotności informacji podlegających ochronie, będących w posiadaniu lub przetwarzaniu Urzędu. Rodzaj zastosowanych zabezpieczeń technicznych, jak i ich poziom wynika zatem z szacowania ryzyka. Proces zarządzania ryzykiem składa się z następujących etapów: identyfikacja ryzyka, analiza ryzyka, w tym określenie poziomu ryzyka, ocena ryzyka (czy ryzyko jest akceptowalne lub tolerowane, a jeżeli nie, to określenie sposobu postępowania z ryzykiem).
Dokumentem procesu zarządzania ryzykiem jest plan postępowania z ryzykiem, na który składa się wyliczenie ryzyk, celów stosowania zabezpieczeń oraz zabezpieczeń. Plan postępowania z ryzykiem jest podstawowym dokumentem wykonawczym do podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy. Po zastosowaniu zabezpieczeń wynikających z planu postępowania z ryzykiem pozostaje ryzyko szczątkowe podlegające akceptacji przez kierownictwo Urzędu.

2. W Starostwie nie zrealizowano zalecenia związanego z przeprowadzonym w 2017 r. audytem wewnętrznym, dotyczącego aktualizacji posiadanej dokumentacji w zakresie bezpieczeństwa informacji.
Starosta wyjaśnił, że brak wykonania ww. zalecenia był uchybieniem w wykonywaniu obowiązków pracowniczych osoby zajmującej się dokumentacją.

(dowód: akta kontroli str. 160-164, 207-211)

3. W Urzędzie nie przeprowadzono analizy procesów przetwarzania danych, o której mowa w art. 32 rozporządzenia RODO.
Z wyjaśnień Starosty wynika, że taka analiza została zlecona zewnętrznemu wykonawcy w ramach realizowanego przez niego w 2018 r. audytu bezpieczeństwa informacji i ma powstać do końca września 2018 r.

(dowód: akta kontroli str. 160-164, 207-211)

Uwaga dotycząca kontrolowanej działalności

Należy zauważyć, że ustanowiona w Starostwie procedura zarządzania incydentami związanymi z bezpieczeństwem informacji zamieszczona była w nieaktualizowanej od

czasu zatwierdzenia w 2004 r. PBI. Zdaniem NIK ustalone w § 20 ust 2 pkt 13 rozporządzenia RM w sprawie KRI zarządzanie bezpieczeństwem informacji, realizowane w szczególności przez zapewnienie możliwości bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób (umożliwiający szybkie podjęcie działań korygujących) wymaga aktualizacji dokumentów zgodnie ze zmianami środowiska.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Starosty w zakresie zapobiegania incydentom bezpieczeństwa informacji ze względu na nieprowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także braku aktualizacji procedury bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji. W Urzędzie nie przeprowadzono także analizy procesów przetwarzania danych, o której mowa w art. 32 rozporządzenia RODO oraz nie zrealizowano wniosku z audytu wewnętrznego w zakresie bezpieczeństwa informacji.

W Urzędzie przeprowadzono okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, co było zgodne z wymogiem § 20 ust. 2 pkt 14 rozporządzenie KRI, a także zapewniono szkolenia pracownikom zaangażowanym w proces przetwarzania danych osobowych.

IV. Uwagi i 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[12], wnosi o:

1) opracowanie i wdrożenie SZBI uwzględniającego zalecenia normy PN-EN ISO/IEC 27001 i norm z nią związanych (PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, PN-EN ISO/IEC 24762),
2) dostosowanie obowiązującej w Urzędzie dokumentacji w zakresie danych osobowych do wymogów rozporządzenia RODO;
3) aktualizację regulaminu organizacyjnego Starostwa i zapewnienie niezależności IOD;
4) odebranie użytkownikom niebędących pracownikami służb informatycznych uprawnień administratora systemu;
5) ustanowienie szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych;
6) prowadzenie okresowych analiz utraty integralności, dostępności lub poufności informacji i podejmowanie działań minimalizujących stwierdzone ryzyko;
7) przeprowadzenie analizy procesów przetwarzania danych w Urzędzie, o której mowa w art. 32 rozporządzenia RODO;
8) zapewnienie realizacji rekomendacji wynikających z okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji;
9) zaktualizowanie informacji o posiadanych i przetwarzanych aktywach informacyjnych.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Dyrektora Delegatury NIK w Krakowie.

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.

[12] Dz. U. z 2017 r. poz. 524 ze zm., dalej: *ustawa o NIK*.

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.

Kraków, dnia 12 października 2018 r.

p.o. Dyrektor
Delegatury Najwyższej Izby Kontroli
w Krakowie

z up.

Jan Kosiniak
p.o. Wicedyrektor

Kontroler

Małgorzata Kram
Specjalista kontroli państwowej