NAJWYŻSZA IZBA KONTROLI
Delegatura w Kielcach

LKI-4114-03-01/2012
I/12/010

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Kielcach
al. Tysiąclecia Państwa Polskiego 4, 25-520 Kielce
T +48 41 249 91 00, F +48 41 249 91 05
lki@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	I/12/010 - Informatyzacja administracji samorządowej.
Okres objęty kontrolą	Od 1 stycznia 2010 r. do 30 września 2012 r.
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Kielcach.
Kontrolerzy	1. Jerzy Stachowiak, główny specjalista kp., upoważnienie do kontroli nr 84672 z dnia 23.11.2012 r. 2. Piotr Bulski, inspektor kp., upoważnienie do kontroli nr 84671 z dnia 23.11.2012 r. (dowód: akta kontroli str. 1-4)
Jednostka kontrolowana	Starostwo Powiatowe w Starachowicach (Starostwo), ul. Borkowskiego 4, 27-200 Starachowice.
Kierownik jednostki kontrolowanej	Andrzej Matynia, Starosta Starachowicki. (dowód: akta kontroli str. 5)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie pomimo stwierdzonych nieprawidłowości[1] działalność kontrolowanej jednostki w zbadanym zakresie.

Uzasadnienie oceny ogólnej

Pozytywną ocenę uzasadnia:

- wykorzystywanie infrastruktury informatycznej do podnoszenia sprawności Starostwa i jakości wykonywanych przez niego zadań;
- opracowanie i wdrożenie *Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych (Polityka bezpieczeństwa)*;
- zapoznanie pracowników z *Polityką bezpieczeństwa* oraz *Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (Instrukcja)*;
- przestrzeganie zasad określonych w *Polityce bezpieczeństwa* Starostwa.

Stwierdzone nieprawidłowości dotyczą:

- nieustalenia w *Instrukcji* zasad i procedur dotyczących zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, pomimo obowiązku wynikającego z § 5 pkt 3-8 rozporządzenia z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[2];
- nieprzestrzegania warunków licencji oprogramowania WinRAR zainstalowanego na dwóch komputerach Starostwa;
- braku aktualizacji zakresów obowiązków dwóch pracowników Starostwa.

[1] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
[2] Dz. U. Nr 100, poz. 1024.

III. Opis ustalonego stanu faktycznego

1. Stan i jakość podstawowej infrastruktury informatycznej, sposób jej wykorzystania oraz wpływ informatyzacji na podnoszenie sprawności Starostwa i jakości wykonywanych zadań

Opis stanu faktycznego

Liczba komputerów osobistych i laptopów (komputerów) użytkowanych w Starostwie wzrosła ze 104 na koniec 2010 r. do 109 na 30 września 2012 r., tj. o 4,8%. Oznacza to, że na 10 pracowników zatrudnionych na stanowiskach urzędniczych przypadało dziewięć komputerów.
Analiza okresu eksploatacji ww. sprzętu wskazuje na stopniowe jego starzenie się. Na koniec 2010 r. komputery użytkowane pięć i więcej lat stanowiły 26% wszystkich komputerów, podczas gdy na 30 września 2012 r. – 48%. Zjawisko starzenia się komputerów następowało pomimo zakupu 27 komputerów w 2010 r. i w 2011 r., oraz otrzymania w 2011 r. jednego komputera w użytkowanie, przekazanego następnie w 2012 r. na własność (w 2012 r. – do 30 września – w Starostwie nie dokonano zakupu komputerów). (dowód: akta kontroli str. 140-155)
W okresie objętym kontrolą nie analizowano obszarów działania Starostwa w celu informatycznego usprawnienia realizowanych w nim procesów. Przeprowadzano analizy służące zabezpieczeniu w budżecie środków finansowych na niezbędne zakupy i ewentualne naprawy już użytkowanego sprzętu komputerowego oraz zakup licencji na użytkowanie programów. Spowodowane to było, jak wyjaśniła Sekretarz Powiatu Marlena Kostrzewa, trudną sytuacją finansową powiatu oraz udziałem w projektach: „e-świętokrzyskie – Rozbudowa Infrastruktury Informatycznej JST" i „e-świętokrzyskie – Budowa Systemu Informacji Przestrzennej Województwa Świętokrzyskiego". W związku z projektem „e-świętokrzyskie – Rozbudowa Infrastruktury Informatycznej JST", Starostwo ma otrzymać m.in. 43 zestawy komputerowe, po zakończeniu projektu, które zaplanowano na 2014 r. (dowód: akta kontroli str. 116-118)

Łączne wydatki na zakup sprzętu komputerowego i licencji na oprogramowanie oraz ich aktualizacji wnosiły: w 2010 r. – 134, 5 tys. zł, w 2011 r. – 131,6 tys. zł (tj. 0,4% wydatków ogółem w tych latach) oraz do 30 września 2012 r. – 32,6 tys. zł (tj. 0,2% wydatków). Powyższe zakupy sfinansowano: w 2010 r. wyłącznie ze środków własnych powiatu, w 2011 r. i 2012 r. ze środków własnych i z dotacji wojewody świętokrzyskiego na realizację zadań zleconych (środki z dotacji stanowiły odpowiednio – 2.785,00 zł i 429,00 zł). Ponadto w 2012 r. – w związku z realizacją projektu „As w samorządzie" współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego – Starostowo otrzymało nieodpłatnie komputer o wartości 3.499,97 zł. (dowód: akta kontroli str. 142-155)

Starostwo ponosiło również ze środków własnych wydatki wynikające z konieczności zapewnienia nadzoru nad utrzymaniem w ruchu systemu finansowo-księgowego i kadrowo-płacowego, dostarczania nowych wersji programów w przypadku zmian, usuwania awarii oraz udzielania konsultacji w powyższym zakresie. W 2010 r. wydatki te wyniosły 6,6 tys. zł (0,6% wydatków Starostwa na zakup usług pozostałych), w 2011 r. – 4,9 tys. zł (0,4% ww. wydatków) a w 2012 r. (do 30 września) – 5,3 tys. zł (0,6% ww. wydatków). (dowód: akta kontroli str. 332-349)

W Starostwie, zarówno kluczowe jak i wspomagające procesy, realizowane przez poszczególne komórki organizacyjne, np. Wydział Budownictwa i Gospodarki Komunalnej, Wydział Edukacji, Kultury Fizycznej i Sportu, Wydział Geodezji,

wspierane są przez specjalistyczne programy informatyczne. Użytkowany jest również zestaw do podpisu elektronicznego (po jednym stanowisku w Wydziałach: Organizacyjnym, Finansowym oraz Komunikacji i Dróg) oraz program Proton – elektroniczny obieg dokumentów (tylko w zakresie systemu elektronicznej skrzynki podawczej na BIP). Ponadto wykorzystywany jest system MS Windows, pakiety biurowe, programy antywirusowe, przeglądarki internetowe, programy narzędziowe oraz oprogramowanie bazodanowe (zapewniające funkcjonowanie specjalistycznych programów zaprojektowanych w architekturze klient-serwer). Żaden z ww. programów nie był dedykowany dla Starostwa. (dowód: akta kontroli str. 156-160, 172-206, 208-244)

W Starostwie prowadzone są 93 rejestry/ewidencje, z tego 63 w formie papierowej, 17 – elektronicznej, a 13 – równolegle w obu wersjach (ze względu na wymogi sprawozdawczości). Do prowadzenia rejestrów w wersji elektronicznej służą MS Word/Excel oraz programy specjalistyczne (EGB, EWMapa, Ośrodek, ProPublico, Kierowca/Pojazd – moduły systemu CEPIK). (dowód: akta kontroli str. 132-139)

Podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Starostwie, zgodnie z zarządzeniem Starosty Starachowickiego, jest system tradycyjny („papierowy"). Przy sporządzaniu przez pracowników Starostwa projektów pism, wykorzystywano narzędzia informatyczne jak również dla spraw o niskim stopniu złożoności opracowano szablony. Ponadto pracownicy mają dostęp do programu Lex oraz programu Bestia, który pozwala kontrolować ustawowe wskaźniki konieczne przy realizacji budżetu powiatu i wieloletniej prognozy finansowej. W Biuletynie Informacji Publicznej opublikowano wzory druków i formularzy właściwych do załatwienia sprawy w poszczególnych komórkach organizacyjnych. Wprowadzono również elektroniczną skrzynkę podawczą, Elektroniczną Platformę Usług Administracji Publicznej (e-PUAP), infomat[3], hot-spot[4]. Wg wyjaśnień Sekretarza Powiatu, Starostwo jest przygotowane pod względem oprogramowania do wprowadzenia elektronicznego obiegu dokumentów, jednak wdrożenie pełnej funkcjonalności zakupionego systemu „Proton" jest uzależnione od realizacji projektu „e-świętokrzyskie – Rozbudowa Infrastruktury Informatycznej JST" (pierwotnie realizacja projektu miała nastąpić w 2008 r.). Starostwo nie posiada narzędzia pozwalającego na zdalne kontrolowanie pracy poszczególnych pracowników na stanowiskach pracy. W 2012 r. podjęto działania zmierzające do rozpoznania rynku usług w tym zakresie oraz możliwości finansowych powiatu w celu ewentualnego zakupu oprogramowania. Zdaniem Sekretarza Powiatu nie zachodziła potrzeba opracowania i wdrożenia mierzalnych wskaźników do oceny efektów wdrożenia konkretnych programów informatycznych. (dowód: akta kontroli str. 116-120, 285-321)

W okresie objętym kontrolą osoby przystępujące do naboru na wolne stanowiska urzędnicze, zobowiązane były do posiadania umiejętności obsługi komputera w zakresie MS Windows i pakietu biurowego MS Office jak również programów wykorzystywanych do pracy w komórce organizacyjnej na konkretnym stanowisku. Dodatkowo pracownicy Starostwa delegowani byli na specjalistyczne szkolenia informatyczne. W okresie od 1 stycznia 2010 r. do 30 września 2012 r., w szkoleniach tych wzięło udział 36 pracowników. (dowód: akta kontroli str. 121-131, 322-331)

[3] Informator multimedialny.
[4] Punkt dostępu do internetu bezprzewodowego.

Ustalone nieprawidłowości

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

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w badanym obszarze.

2. Polityka bezpieczeństwa systemu informatycznego funkcjonującego w Starostwie

Opis stanu faktycznego

Polityka bezpieczeństwa, została ustalona zarządzeniem Starosty Starachowickiego w dniu 22 maja 2007 r. W zarządzeniu tym zawarto elementy wymagane § 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Zawiera bowiem wykaz budynków, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami oraz określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
W *Polityce bezpieczeństwa* określono również, że:

- wszystkie komputery podłączone są do wydzielonej sieci energetycznej i posiadają zasilacze czasowe podtrzymujące napięcie (UPS);
- hasła posiadają minimum 8 znaków i są różne od identyfikatorów;
- hasła przy wpisywaniu nie są wyświetlane na ekranie;
- komputery posiadają wygaszacze ekranu zabezpieczone hasłem, uruchamiające się po 5-minutowym czasie bezczynności;
- do ochrony antywirusowej należy stosować jednostanowiskowy program antywirusowy, w aktualnej wersji, pracujący w tle, tj. z włączoną ochroną plików w czasie rzeczywistym.

Oględziny 13 stanowisk komputerowych Starostwa (11,9% stanu komputerów na 30 września 2012 r.) potwierdziły przestrzeganie powyższych wymogów *Polityki bezpieczeństwa*. (dowód: akta kontroli str. 6, 7, 24, 25, 26, 27, 251-263) Ustalono, że kopie zapasowe danych tworzono i przechowywano zgodnie z zasadami przyjętymi w *Polityce bezpieczeństwa*. (dowód: akta kontroli str. 24-27, 284)

Starosta Starachowicki jako administrator danych osobowych Starostwa, w dniu 20 października 2010 r. wyznaczył *[…]*[5] – inspektora w Zespole ds. Ochrony i Zarządzania Kryzysowego na „Administratora Bezpieczeństwa Informacji" (Administrator) dla danych zawartych w systemach informatycznych Starostwa. Administrator, zgodnie z *Polityką bezpieczeństwa*, przeprowadzał zaplanowane kontrole stanu bezpieczeństwa danych osobowych. (dowód: akta kontroli str. 24-27, 69, 74-75, 272-283)

Zarządzeniem Starosty Starachowickiego z dnia 22 maja 2007 r. została wprowadzona *Instrukcja*. Spełnia ona wymogi określone w § 5 pkt 1 i 2 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Zawiera bowiem

[5] Tajemnica ustawowo chroniona: art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 ze zm.), ze względu na prywatność osoby fizycznej.

procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności, a także stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem. (dowód: akta kontroli str. 11, 66-73)

Wszyscy pracownicy obsługujący komputery służące do przetwarzania danych osobowych zostali zapoznani z *Polityką bezpieczeństwa* i *Instrukcją* – każdy z nich podpisał stosowne oświadczenie w tym zakresie. Wszyscy pracownicy posiadają wydane na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[6] upoważnienia do przetwarzania danych osobowych określające zadania i czynności do wykonania, w tym *przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym.* (dowód: akta kontroli str. 109-113, 264, 265)

Starostwo stosowało zabezpieczenia programowe blokujące ingerencję z zewnątrz tzw. zaporę sieciową. Przyjęte rozwiązania okazały się skuteczne. (dowód: akta kontroli str. 250, 272-283)

W przypadku komputerów użytkowanych przez pracowników Wydziału Finansowego Starostwa, politykę bezpieczeństwa systemów informatycznych określa *Polityka rachunkowości* nadana przez Starostę Starachowickiego w dniu 29 grudnia 2010 r. W załączniku nr 8 do ww. zarządzenia określono m.in. system ochrony danych, w tym ochronę danych informatycznych, tj.: zarządzanie systemami haseł, zasady rejestrowania i wyrejestrowania użytkowników, procedury rozpoczęcia i zakończenia pracy, obsługę kopii bezpieczeństwa, nośników informacji oraz wydruków, zasady ochrony danych przed ich utratą z systemów informatycznych oraz przeglądy i konserwację systemów i zbiorów danych. Wg *Polityki rachunkowości* w sytuacjach naruszenia zasad ochrony systemów informatycznych należy postępować zgodnie z *Polityką bezpieczeństwa*. (dowód: akta kontroli str. 76-77, 78-83)

Do ochrony danych przetwarzanych w systemie finansowo-księgowym zastosowano zabezpieczenia wymienione w art. 71 ust. 2 ustawy z 29 września 1994 r. o rachunkowości[7] w zakresie sporządzania kopii zapasowych danych, ograniczanie dostępu do danych wyłącznie do użytkowników uprawnionych oraz zastosowanie zabezpieczeń sprzętowo-programowych, blokujących ingerencję z zewnątrz. Zastosowane w Starostwie środki ochrony fizycznej odpowiadały wymogom określonym w *Polityce rachunkowości*. (dowód: akta kontroli str. 76-83, 87, 88, 91)

Analiza programów zainstalowanych na 13 komputerach oraz dokumentacji potwierdzającej legalność użytkowania oprogramowania wykazała, że na 11 komputerach (85%) użytkowano wyłącznie programy licencjonowane (z zakupioną licencją na użytkowanie). (dowód: akta kontroli str. 172-248)

W Starostwie, w okresie objętym kontrolą, zorganizowano jedno szkolenie w zakresie ogólnych zasad bezpieczeństwa systemów informatycznych (w ramach projektu „AS w samorządzie"). W szkoleniu tym uczestniczyło piętnastu pracowników. Administrator *[…]*[8], wyjaśniając w jaki sposób odbywa się szkolenie pracowników w powyższym zakresie stwierdził, że pracownicy Starostwa są zapoznawani z ogólnymi zasadami bezpieczeństwa systemów informatycznych określonymi w *Polityce bezpieczeństwa* oraz w *Instrukcji*, oraz że na bieżąco w ramach swoich obowiązków służbowych udziela instruktażu z zakresu ogólnych

[6] Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.
[7] Dz. U. z 2009 r. Nr 152, poz. 1223 ze zm.
[8] Tajemnica ustawowo chroniona: art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 ze zm.), ze względu na prywatność osoby fizycznej.

zasad bezpieczeństwa systemów informatycznych. (dowód: akta kontroli str. 98-101, 108)

Ustalone nieprawidłowości

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

1. W *Instrukcji*, pomimo obowiązku wynikającego z § 5 pkt 3-8 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, nie ustalono:

- procedur zawieszenia pracy przeznaczonych dla użytkowników systemu;
- procedur tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
- sposobu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia, tj. oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- sposobu realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4, tj. odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;
- procedur wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Odpowiedzialny za powyższą nieprawidłowość Starosta Starachowicki Andrzej Matynia, wyjaśnił, że elementy, które nie zostały ujęte w *Instrukcji* reguluje *Polityka bezpieczeństwa* a *Instrukcja* stanowi jej integralną część. Oba ww. dokumenty potraktowane zostały jako dokumenty spójne, względnie się uzupełniające.

Powyższe wyjaśnienie nie może zostać uwzględnione, ponieważ z przepisów rozporządzenia jednoznacznie wynika jakie elementy powinna zawierać *Polityka bezpieczeństwa,* a jakie *Instrukcja* a zatem nie można tych wymogów dowolnie traktować.

Starosta wyjaśnił również, że sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia zapewniono poprzez dokumentowanie udostępniania danych osobowych, w rejestrze udostępnienia prowadzonym przez komórki organizacyjne, które przetwarzają właściwe zbiory.

Stanowisko takie nie jest uzasadnione, ponieważ dane te, zgodnie z ww. przepisem, powinny zostać odnotowanie w systemie informatycznym. (dowód: akta kontroli str. 69-73, 104-108)

2. Na dwóch komputerach Starostwa zaewidencjonowanych jako „Inwestycje" i „geo101xp", nie odinstalowano testowej wersji programu WinRAR, pomimo upływu 40-dniowego okresu testowego (usunięcia programu dokonano podczas kontroli NIK). Oprogramowanie to na komputerze „Inwestycje" zainstalowano w grudniu 2011 r. natomiast na komputerze „geo101xp" we wrześniu 2009 r. Zaniechaniem tym naruszono art. 17 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[9], stanowiący, że twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim na wszystkich polach eksploatacji oraz do wynagrodzenia za korzystanie z utworu oraz pkt 2 i 12 warunków licencji WinRAR, w których określono, że każdy może korzystać z oprogramowania przez okres testowy 40 dni, a po jego upłynięciu należy dokonać zakupu licencji, oraz że brak akceptacji warunków licencji oznacza konieczność zaprzestania użytkowania

[9] Dz. U. z 2006 r. Nr 90, poz. 631 ze zm.

programu WinRAR i usunięcia ze swoich nośników danych wszystkich powiązanych z nim plików.
Zgodnie z zakresem czynności odpowiedzialność za powyższą nieprawidłowość ponosi *[…]*[10] – główny specjalista w Wydziale Organizacji, Kadr i Spraw Obywatelskich, któremu przydzielono zabezpieczenie przestrzegania prawa autorskiego i ochrony danych osobowych przy używaniu oprogramowania informatycznego w Starostwie oraz inwentaryzację sprzętu komputerowego i oprogramowania zainstalowanego w wydziałach.
[…][11] wyjaśnił, że przez przeoczenie nie sprawdził oprogramowania zainstalowanego na komputerze „Inwestycje" po przejęciu go na własność od Akademii Przedsiębiorczości sp. z o.o., organizatora szkolenia w ramach projektu „AS w samorządzie" w kwietniu 2012 r. W zakresie komputera „geo101xp" podał, że użytkownikiem tego komputera był i jest pracownik zatrudniony na stanowisku informatyka w Wydziale Geodezji, Ochrony Środowiska i Rolnictwa *[…]*[12], któremu w zakresie czynności służbowych powierzono m.in. obsługę informatyczną Wydziału Geodezji, Ochrony Środowiska i Rolnictwa oraz instalację i wdrażanie nowych wersji systemów operacyjnych, przez co to on ponosi odpowiedzialność za nieodinstalowanie tego oprogramowania. Dodał ponadto, że z jego obowiązków wyłączono zabezpieczenie przestrzegania prawa autorskiego w Wydziale Geodezji, Ochrony Środowiska i Rolnictwa, pomimo iż nie zostało to odnotowane w zakresie czynności.
Starosta Starachowicki wyjaśnił, że zgodnie z przyjętą praktyką w Starostwie obsługą informatyczną Wydziału Geodezji, Ochrony Środowiska i Rolnictwa zajmował się pracownik zatrudniony na stanowisku informatyka w tym Wydziale.
W zakresie czynności *[…]*[13] nie zawarto obowiązku zabezpieczenia przestrzegania prawa autorskiego i ochrony danych osobowych przy używaniu oprogramowania informatycznego w Wydziale Geodezji, Ochrony Środowiska i Rolnictwa oraz inwentaryzacji sprzętu komputerowego i oprogramowania zainstalowanego w tym Wydziale. (dowód: akta kontroli str. 165-171, 190-193, 207, 227-229, 237, 247, 267, 269, 356-360, 362-367)
Z powyższego wynika, że ustalone na piśmie zakresy czynności *[…]*[14] i *[…]*[15] nie były dostosowane do przewidzianych dla nich zadań w zakresie zapewnienia przestrzegania prawa autorskiego przy używaniu oprogramowania informatycznego w Starostwie. NIK zwraca uwagę, że zgodnie ze standardami kontroli zarządczej[16] każdy pracownik powinien mieć określony w formie dokumentu aktualny zakres obowiązków, uprawnień i odpowiedzialności, który wchodzi w skład dokumentacji systemu kontroli zarządczej (standard nr 3 i 10). Jednocześnie, zdaniem NIK, precyzyjne określenie zadań jest warunkiem koniecznym dla zapewnienia przestrzegania prawa autorskiego przy używaniu oprogramowania informatycznego w Starostwie.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, działalność kontrolowanej jednostki w badanym obszarze.

[10] Tajemnica ustawowo chroniona: art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 ze zm.), ze względu na prywatność osoby fizycznej.
[11] Tajemnica ustawowo chroniona: art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 ze zm.), ze względu na prywatność osoby fizycznej.
[12] Tajemnica ustawowo chroniona: art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 ze zm.), ze względu na prywatność osoby fizycznej.
[13] Tajemnica ustawowo chroniona: art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 ze zm.), ze względu na prywatność osoby fizycznej.
[14] Tajemnica ustawowo chroniona: art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 ze zm.), ze względu na prywatność osoby fizycznej.
[15] Tajemnica ustawowo chroniona: art. 5 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 ze zm.), ze względu na prywatność osoby fizycznej.
[16] Określonymi w Komunikacie Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF Nr 15, poz. 84).

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[17], wnosi o:

1. Dostosowanie *Instrukcji* do wymogów rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
2. Przestrzeganie warunków licencji oprogramowania zainstalowanego na komputerach Starostwa.
3. Zaktualizowanie zakresów czynności pracowników w celu zapewnienia przestrzegania prawa autorskiego przy używaniu oprogramowania informatycznego w Starostwie.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 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 Kielcach.

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.

Kielce, dnia stycznia 2013 r.

Najwyższa Izba Kontroli
Delegatura w Kielcach

Kontrolerzy
Jerzy Stachowiak
główny specjalista kp.

.....
podpis

Piotr Bulski
inspektor kp.

.....

Dyrektor
Tadeusz Poddębniak

.....
podpis

[17] Dz. U. z 2012 r., poz. 82 ze zm.

podpis