NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.010.03.2018
P/18/006

01462818

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	Wojciech Zambrzycki – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/75/2018 r. z 5 czerwca 2018 r. (dowód: akta kontroli str. 1-2) Dominika Jocz – inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/76/2018 z 5 czerwca 2018 r. (dowód: akta kontroli str. 3-4)
Jednostka kontrolowana	Starostwo Powiatowe w Augustowie, ul. 3 Maja 29, 16-300 Augustów (dalej *„Starostwo"* lub *„Urząd"*)
Kierownik jednostki kontrolowanej	Jarosław Szlaszyński – Starosta[2] (dowód: akta kontroli str. 5)

II. Ocena kontrolowanej działalności[3]

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, przyjęte i wdrożone rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa informacji przetwarzanych w Starostwie.

Uzasadnienie oceny ogólnej

Organizacja procesu zabezpieczania informacji została przeprowadzona właściwie. Stworzono szereg polityk i procedur traktujących o tych zagadnieniach, w tym ustanowiono System Zarzadzania Bezpieczeństwem Informacji. Dokumenty te były aktualizowane wraz ze zmieniającymi się przepisami prawa. Powołano też Administratora Bezpieczeństwa Informacji (dalej: *„ABI"*), a od 25 maja 2018 r. – Inspektora Ochrony Danych (dalej: *„IOD"*). Prowadzono działania zapobiegające incydentom bezpieczeństwa informacji, poprzez wykonywanie cyklicznych audytów wewnętrznych i analiz ryzyka utraty integralności, poufności lub dostępności. Prowadzono także szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych.

Stwierdzone nieprawidłowości polegały na:

- nieposiadaniu pełnych i aktualnych danych dotyczących użytkowanego sprzętu i oprogramowania oraz jego konfiguracji,
- stosowaniu przez jednego z pracowników zbyt krótkiego hasła dostępu do systemu informatycznego, w którym przetwarzane były dane osobowe,
- przekazaniu hasła dostępu do systemu operacyjnego komputera przez pracownika innemu pracownikowi,
- posiadaniu uprawnień administratora przez pracownika, który takich uprawnień nie powinien posiadać.

---

[1] Kontrolą objęto okres od 1 czerwca 2017 r. do 28 czerwca 2018 r.
[2] Funkcję pełni od 28 października 2014 r.
[3] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Starostwie opracowano, ustanowiono i z początkiem 2016 roku wdrożono System Zarządzania Bezpieczeństwem Informacji (dalej: *„SZBI"*), stosownie do wymogów § 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[4].

Zarządzeniem Starosty z 9 stycznia 2015 r.[5] powołano sześcioosobowy zespół ds. wdrożenia *SZBI*, wskazano zakres jego zadań oraz zobowiązano wszystkich pracowników do aktywnego uczestnictwa w pracach nad wdrażaniem *SZBI*. Następnie zarządzeniem Starosty z 8 maja 2015 r.[6] zatwierdzono dokumentację *SZBI*, ustalono termin zakończenia wdrożenia na 31 grudnia 2015 r. oraz wskazano osoby odpowiedzialne za wdrożenie. Dokumentacja *SZBI* składała się z: *„Polityki Bezpieczeństwa Informacji"*, *„Księgi SZBI"*, *„Deklaracji stosowania zabezpieczeń"*, *„Polityki bezpieczeństwa ochrony danych osobowych"* oraz procedur *SZBI*. W przyjętej dokumentacji wskazano, że kierownictwo Urzędu jest odpowiedzialne za ocenę, przegląd i modyfikację polityki *SZBI*.
(dowód: akta kontroli str. 6-255)

1.2. Sporządzenie dokumentacji w zakresie ochrony danych osobowych, uwzględniającej wymogi 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)[7], zostało przeprowadzone zgodnie z harmonogramem opracowanym przez ABI. Uwzględniono w nim szereg działań, realizowanych od stycznia do maja 2018 roku, obejmujących m.in. wykonanie przeglądów i analiz w poszczególnych komórkach organizacyjnych, weryfikację dotychczasowych i opracowanie nowych procedur oraz szkolenie pracowników z nowych przepisów prawa polskiego i europejskiego. Zarządzeniem Starosty z 24 maja 2018 r.[8] wprowadzono nową *„Politykę bezpieczeństwa ochrony danych osobowych"* wraz z załącznikami, *„Regulamin ochrony danych osobowych"*, wskazano zadania inspektora ochrony danych oraz uchylono dotychczas obowiązującą *„Politykę bezpieczeństwa"* z 27 czerwca 2017 r. Nowe zarządzenie zostało przekazane naczelnikom wydziałów, rozesłane pracownikom drogą elektroniczną oraz udostępnione kadrze Starostwa na stronie intranetowej. Ponadto na stronie internetowej Starostwa, w Biuletynie Informacji Publicznej, umieszczono zakładkę *„Ochrona danych osobowych"*, w której poinformowano o uprawnieniach wynikających z przepisów RODO, wskazując m.in. że każdej osobie fizycznej, której dane są przetwarzane, w określonych sytuacjach przysługuje prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody na przetwarzanie danych. Obok nowych regulacji dotyczących ochrony danych osobowych, w Starostwie obowiązywała również *„Polityka Bezpieczeństwa Informacji"* oraz procedury *SZBI* uchwalone zarządzeniem z 2015 roku. (dowód: akta kontroli str. 256-323)

1.3. W Starostwie dokonywano aktualizacji regulacji wewnętrznych stanowiących *SZBI* w zakresie dotyczącym zmieniającego się otoczenia, realizując w tym zakresie obowiązek wynikający z § 20 ust. 2 pkt 1 rozporządzenia KRI. Aktualizacja obejmowała m.in. *„Politykę bezpieczeństwa ochrony danych osobowych"* wraz z załącznikami, *„Wykaz zbiorów danych osobowych"* oraz poszczególne procedury wprowadzone w ramach *SZBI*. Opracowana została analiza ryzyka, co szerzej opisano w punkcie 3.1. niniejszego wystąpienia. Od września do grudnia 2017 roku przeprowadzono 14 audytów wewnętrznych, co szerzej

---

4 Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: *„rozporządzeniem KRI"*.

5 Zarządzenie Nr 2 Starosty Augustowskiego z dnia 9 stycznia 2015 r. w sprawie wdrożenia w Starostwie Powiatowym w Augustowie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy ISO 27001:2007.

6 Zarządzenie nr 17/2015 Starosty Augustowskiego z dnia 8 maja 2015 r. w sprawie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, zmienione zarządzeniem z 20 listopada 2017 r.

7 Dz. Urz. UE L z 2016.119.1. Rozporządzenie zwane dalej: *„RODO"*.

8 Zarządzenie nr 13/2018 Starosty Augustowskiego z dnia 24 maja 2018 roku w sprawie wprowadzenia Polityki Bezpieczeństwa dotyczącej ochrony danych osobowych w Starostwie Powiatowym w Augustowie oraz wyznaczenia inspektora ochrony danych.

opisano w punkcie 3.4. wystąpienia, w wyniku których nie stwierdzono nieprawidłowości. ABI (pełniący również funkcję Pełnomocnika ds. SZBI) dokonywał sprawdzeń zgodności przetwarzania danych osobowych z przepisami w trybie sprawdzenia planowego – w okresie objętym kontrolą sprawdzenia dokonano w Wydziale Spraw Obywatelskich od 19 do 20 października 2017 r. (w jego wyniku nie stwierdzono nieprawidłowości). ABI przeprowadził również okresowy przegląd, zakończony sprawozdaniem z działań związanych z wdrażaniem *SZBI*, sporządzonym 10 stycznia 2018 r. Prowadzony był również rejestr incydentów dotyczących bezpieczeństwa. ABI dokonywał regularnych przeglądów rejestru, co następnie raportował Staroście (w okresie objętym kontrolą sporządzono pięć raportów, w których opisano poszczególne zdarzenia sklasyfikowane jako incydenty istotne oraz wskazano spostrzeżenia i zalecenia na przyszłość). Wśród zaleceń Pełnomocnika ds. SZBI oraz czynności podejmowanych w celu zapobiegania podobnym incydentom w przyszłości znalazły się m.in.: monitorowanie temperatury w serwerowni w dni wolne od pracy poprzez kamerę internetową, czyszczenie radiatora oraz uzupełnianie czynnika chłodzącego w klimatyzatorach w serwerowni, naprawy posiadanego sprzętu w ramach gwarancji, wymiana dysku macierzy, zakup nowych klimatyzatorów, sporządzenie instrukcji dla pracowników dotyczącej korzystania z drukarek sieciowych.

(dowód: akta kontroli str. 324-331, 648-674)

1.4. W Urzędzie zostali wyznaczeni dwaj pracownicy odpowiedzialni za bezpieczeństwo informacji, zatrudnieni na stanowiskach informatyka i głównego specjalisty w Wydziale Organizacyjno-Prawnym, posiadający odpowiednie kwalifikacje i doświadczenie zawodowe. Każdy z nich odbył kilkanaście szkoleń z zakresu zagadnień informatycznych oraz związanych z ochroną danych osobowych. Ponadto obaj pracownicy posiadają kwalifikacje auditora wewnętrznego zgodnie z normą ISO 27001:2014. Zadania związane z bezpieczeństwem informacji zostały uwzględnione w zakresach ich czynności.

(dowód: akta kontroli str. 347-350, 648)

1.5. Stosownie do art. 37 ust. 1 lit. a) RODO, w Urzędzie 25 maja 2018 r. został wyznaczony IOD, który posiadał kwalifikacje do pełnienia tej funkcji, wskazane w art. 37 ust. 5 RODO. Osoba ta pełniła wcześniej funkcję ABI[9]. IOD ukończył studia podyplomowe z zakresu informatyki, odbył kursy i szkolenia w zakresie ochrony danych osobowych (11 szkoleń w latach 2015–2018), w tym uwzględniające zmiany przepisów wynikające z RODO. Został on zobowiązany do realizacji zadań określonych w art. 39 ust. 1 RODO.

(dowód: akta kontroli str. 347, 355-356)

1.6. W *„Regulaminie Organizacyjnym"*, obowiązującym od 25 maja 2018 r.[10], wyodrębniono IOD jako oddzielne stanowisko, podlegające bezpośrednio Staroście oraz wskazano zakres jego zadań. Spełniono tym samym wymóg art. 38 ust. 3 RODO. Osoba będąca IOD realizowała inne zadania w ramach zatrudnienia na stanowisku głównego specjalisty – zastępowała osobę zatrudnioną na stanowisku informatyka. Wykonywanie tych obowiązków nie wywoływało konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

(dowód: akta kontroli str. 351-361)

1.7. W ramach wdrożenia *SZBI* sporządzono dokumentację, zawierającą polityki i procedury, określające szczegółowe zasady wdrożenia zabezpieczeń technicznych. W *Księdze SZBI* wyodrębniono następujące polityki: [1] bezpieczeństwa dotyczącą ochrony danych osobowych, [2] zarządzania zmianami (dotyczącą zmian w systemach informatycznych, oprogramowaniu i urządzeniach), [3] zarządzania wymiennymi nośnikami informacji, [4] zarządzania relacjami z dostawcami, [5] zarządzania kluczami do pomieszczeń, [6] tworzenia kopii zapasowych, [7] przetwarzania i komunikacji mobilnej, [8] ochrony antywirusowej, [9] korzystania z usług sieciowych, [10] kontroli dostępu, [11] czystego ekranu i czystego biurka, [12] bezpieczeństwa zasobów ludzkich, [13] bezpieczeństwa fizycznego, [14] korzystania z sieci Internet i poczty e-mail. Ponadto integralną część *SZBI* stanowiło 10 procedur, tj. *„Inwentaryzacja aktywów i postępowania z ryzykiem"*, *„Postępowanie z incydentami bezpieczeństwa informacji"*, *„Audyt wewnętrzny"*,

[9] W zarządzeniu z 24 maja 2018 r. wprowadzającym nową politykę bezpieczeństwa Starosta ustalił, że zgodnie z art. 158 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[9], obowiązki IOD będzie pełnił dotychczasowy ABI.

[10] Uchwała nr 1010/126/2018 Zarządu Powiatu w Augustowie z dnia 23 maja 2018 r. w sprawie uchwalenia Regulaminu Organizacyjnego Starostwa Powiatowego w Augustowie.

„Działania korygujące i zapobiegawcze", „Nadzór nad dokumentami", „Nadzór nad zapisami", „Przegląd SZBI", „Zarządzanie ciągłością działania", „Bezpieczeństwo sieci", „Kontrola dostępu do informacji w formie elektronicznej" (obowiązuje od 1 grudnia 2017 r.).
(dowód: akta kontroli str. 6-255)

1.8. Regulacje wewnętrzne stanowiące dokumenty wykonawcze wymagane przez PBI były dostępne dla osób odpowiedzialnych za realizację poszczególnych czynności wymaganych tymi dokumentami. Na stronie intranetowej Starostwa, dostępnej dla wszystkich pracowników, umieszczono dokumentację Systemu Zarządzania Bezpieczeństwem Informacji oraz zarządzenie Starosty wprowadzające nową *„Politykę bezpieczeństwa"*, uwzględniającą wymagania wynikające z rozporządzenia RODO, wraz z załącznikami. Na stronie tej w zakładce „SZBI" umieszczono: *„Politykę Bezpieczeństwa Informacji"*, *„Księgę SZBI"*, *„Deklarację stosowania zabezpieczeń"*, *„Politykę bezpieczeństwa ochrony danych osobowych"*, procedury *SZBI*, plany awaryjne, materiały dotyczące audytów i przeprowadzonych szkoleń. W zakładce „RODO" (Regulamin ochrony danych osobowych) umieszczono przepisy wewnętrzne (*„Politykę bezpieczeństwa"* wprowadzoną 24 maja 2018 r. wraz z załącznikami) oraz materiały ze szkoleń i praktyczne wyjaśnienia. Dokumenty te zawierały ogólne regulacje dotyczące bezpieczeństwa informacji. Szczegółowe zagadnienia dotyczące technicznych zabezpieczeń systemów informatycznych, określone w załączniku nr 1 do *„Polityki bezpieczeństwa"*, nie zostały udostępnione pracownikom Starostwa. Informacje te dostępne były wyłącznie dla informatyków. Dodatkowo na stronie intranetowej zamieszczono klauzulę o przeznaczeniu dokumentów wyłącznie pracownikom Urzędu oraz o zakazie ujawniania ich treści osobom trzecim. Część procedur zawierała informacje dotyczące szczegółowych zasad zarządzania środowiskiem informatycznym i z tych względów nie powinna być udostępniana wszystkim pracownikom, co omówiono dalej, w sekcji *„Uwagi dotyczące badanej działalności"*. (dowód: akta kontroli str. 260, 362-367)

1.9. W Urzędzie zidentyfikowano zbiory danych podlegające zabezpieczeniu. Prowadzono wykaz zbiorów danych osobowych, stanowiący załącznik B do *„Polityki bezpieczeństwa"* z 26 czerwca 2017 r. Ujęto w nim 102 zbiory danych osobowych. Załącznikiem do Polityki bezpieczeństwa wprowadzono rejestr czynności przetwarzania, szczegółowo omówiony w punkcie 2.16. niniejszego wystąpienia. W rejestrze na dzień 25 maja 2018 r. ujęto 119 czynności przetwarzania. (dowód: akta kontroli str. 200-218, 368-425, 592-596)

1.10. Starostwo posiadało system do zarządzania zasobami informatycznymi Urzędu. Nie zawierał on jednak pełnych informacji o posiadanym sprzęcie i oprogramowaniu, co szerzej omówiono poniżej, w sekcji *„Ustalone nieprawidłowości"*. Posiadane urządzenia informatyczne przypisane były (w prowadzonej ewidencji) do osób, które odpowiadają za dany sprzęt. Jak wyjaśnił IOD, *„prowadzone są protokoły przekazania sprzętu dla użytkownika z informacją, że może je stosować tylko do celów służbowych. Dokument ten jest przechowywany w aktach osobowych"*. (dowód: akta kontroli str. 426-471)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość, polegającą na niewywiązaniu się z obowiązku utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, określnego w § 20 ust. 2 pkt 2 rozporządzenia KRI. Prowadzona przez Starostwo (z wykorzystaniem systemu informatycznego) ewidencja nie zawierała pełnych i aktualnych danych dotyczących użytkowanego sprzętu i oprogramowania. Stwierdzono bowiem, że:

- system ten nie zawierał bieżących danych o sześciu (z 14 objętych badaniem) komputerach – ostatnia inwentaryzacja ich zawartości i parametrów była przeprowadzona w dwóch przypadkach w 2016 roku, a w kolejnych czterech w 2017 roku,
- lokalizacja dwóch komputerów (z 14 badanych) była inna niż wskazana w systemie,
- w systemie nie zinwentaryzowano 24 (z 47) posiadanych przez Starostwo drukarek.

IOD wyjaśnił, że brak automatycznej aktualizacji danych o sprzęcie i oprogramowaniu spowodowany był problemami technicznymi. Dodał, że jeden laptop nie był używany w lokalnej sieci (w trakcie kontroli zapewniono, że jego użytkownik zostanie zobowiązany

do zaktualizowania oprogramowania). Natomiast odnośnie dwóch komputerów wykazywanych przez system w innej lokalizacji niż rzeczywista, IOD wyjaśnił, że wynikało to z przeniesienia jednego z wydziałów do innego budynku i dodał, że na podstawie ewidencji papierowej informatycy są w stanie zlokalizować dany sprzęt. Wyjaśnił też, że wszystkie drukarki sieciowe (21 sztuk) nie inwentaryzują się automatycznie i muszą być ręcznie wprowadzone do oprogramowania, natomiast trzy drukarki lokalne są przestarzałe i przeznaczone do utylizacji. Dodał, że wszystkie drukarki były ujęte w ewidencji papierowej.

(dowód: akta kontroli str. 426-471)

Uwagi dotyczące badanej działalności

Najwyższa Izba Kontroli zwraca uwagę, że wszelkie szczegółowe informacje dotyczące zabezpieczeń informatycznych zawarte w Procedurze nr 9 – *„Bezpieczeństwo sieci"* oraz w odnoszącym się do ww. procedury *„Planie ciągłości działania na wypadek awarii systemów informatycznych"* (w części dotyczącej działania systemów i bezpieczeństwa sieci) powinny być udostępnione jedynie osobom odpowiedzialnym za bezpieczeństwo informacji, a nie – wszystkim pracownikom Starostwa na stronie intranetowej.

(dowód: akta kontroli str. 131-148, 235-255)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonej nieprawidłowości, organizację systemu bezpieczeństwa informacji w Starostwie. Wdrożone rozwiązania w zakresie organizacji bezpieczeństwa informacji były właściwe, z wyjątkiem nieutrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.

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

Opis stanu faktycznego

2.1. Użytkownicy 14 (z 15) objętych oględzinami komputerów[11] nie posiadali uprawnień i możliwości zainstalowania oprogramowania. Jeden użytkownik, z uwagi na nadane uprawnienia w systemie, posiadał możliwość instalacji oprogramowania, chociaż nie był administratorem systemów informatycznych. Kwestia ta szerzej została omówiona w dalszej części wystąpienia, w sekcji *„Ustalone nieprawidłowości"*. (dowód: akta kontroli str. 472-475)

2.2. Analiza realizowanych zadań służbowych 15 z 64 pracowników Starostwa (w tym pięciu kierowników wydziałów i jednego pracownika, który w okresie objętym kontrolą zmienił stanowisko pracy) wykazała, że posiadali oni uprawnienia do systemów informatycznych i zbiorów danych zgodne z zakresami obowiązków, czym wypełniono obowiązek wskazany w § 20 ust. 2 pkt 4 rozporządzenia KRI.

W Urzędzie prowadzony był rejestr upoważnień do przetwarzania danych osobowych, w którym ewidencjonowano datę nadania i ustania upoważnienia, zakres i identyfikator w systemie informatycznym, jeśli zbiór danych był przetwarzany za pomocą takiego narzędzia. Procedura nadawania uprawnień opisana została w rozdziale VI. pkt 4 *„Polityki bezpieczeństwa dotyczącej ochrony danych osobowych"* i w pkt 6 *„Regulaminu ochrony danych osobowych w Starostwie Powiatowym w Augustowie"* (przed 25 maja 2018 r. – w § 3 *„Instrukcji zarządzania systemami informatycznymi"*[12]), a fakt posiadania przez pracowników uprawnień tylko do wybranych systemów informatycznych i niektórych zbiorów wskazuje, że działania Starostwa były zgodne z zapisami ww. polityki i regulaminu.

(dowód: akta kontroli str. 224-234, 261-277, 312-321, 476-577, 647, 751-771)

2.3. W okresie objętym kontrolą w Starostwie pracę zakończyło 11 osób. Każdej z nich uniemożliwiono dostęp do systemów informatycznych poprzez blokadę lub usunięcie konta na użytkowanym komputerze, a także uniemożliwiono dostęp do poczty elektronicznej i systemu elektronicznego obiegu dokumentów dostępnych online[13].

(dowód: akta kontroli str. 578-579)

---

[11] 10 komputerów stacjonarnych i pięć laptopów.

[12] Wprowadzona Zarządzeniem Nr 26/2016 Starosty Augustowskiego z dnia 4 października 2016 r. w sprawie aktualizacji Instrukcji Zarządzania Systemami Informatycznymi w Starostwie Powiatowym w Augustowie. Przestała obowiązywać po wejściu w życie 25 maja 2018 r. *„Polityki bezpieczeństwa dotyczącej ochrony danych osobowych"*.

[13] W Urzędzie nie funkcjonowało zarządzanie siecią poprzez system Microsoft Active Directory, czyli centralne zarządzanie tożsamością i dostępem użytkowników do komputerów. Poprzez usunięcie albo blokadę konta użytkownika na komputerze automatycznie blokowany był dostęp do programów zainstalowanych na tych jednostkach operacyjnych.

Według zapisów pkt 1.1 ppkt 20 Procedury nr 10 *„Kontrola dostępu do informacji w formie elektronicznej"* – obowiązującej od 1 grudnia 2017 r. – wnioski o likwidację konta składają naczelnicy wydziałów lub uprawnione komórki organizacyjne, w ciągu siedmiu dni od wystąpienia zdarzenia powodującego likwidację konta[14] użytkownika. W analizowanej grupie osób, które zakończyły zatrudnienie w czasie obowiązywania ww. procedury, wnioski takie zostały złożone, jednak nie ewidencjonowano daty ich wpływu do służb informatycznych – nie było zatem możliwe ustalenie, czy wnioski wpłynęły w wymaganym terminie i czy usunięcie konta następowało niezwłocznie. IOD wyjaśnił, że były to dokumenty wewnętrzne, a zatem nie nanoszono na nich daty wpływu, jednak od 12 czerwca 2018 r. poleceniem Starosty informatycy zostali zobligowani do nanoszenia daty wpływu wniosku o założenie lub likwidację konta użytkownika.
(dowód: akta kontroli str. 149-172, 580-585)

2.4. W celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem, zgodnie z rozdziałem VI, pkt 5 ppkt 3 *„Polityki bezpieczeństwa dotyczącej ochrony danych osobowych"* (przed 25 maja 2018 r. – w § 4 pkt 3 *„Instrukcji zarządzania systemami informatycznymi"*), użytkownicy systemów informatycznych Starostwa powinni stosować hasła o wymaganej złożoności. Każdy z 15 użytkowników komputerów poddanych oględzinom stosował się do tej zasady dla haseł do systemu operacyjnego, co było zgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI. Jednocześnie jeden z tych pracowników używał hasła o nieodpowiedniej liczbie znaków do oprogramowania dziedzinowego[15], a inny dysponował hasłem dostępu do sytemu operacyjnego pracownika długotrwale nieobecnego w pracy, co szerzej zostało omówione w dalszej części wystąpienia, w sekcji *„Ustalone nieprawidłowości"*. (dowód: akta kontroli str. 224-234, 261-277, 472-475)

2.5. Usytuowanie sześciu monitorów komputerowych objętych badaniem w Wydziale Komunikacji uniemożliwiało interesantom wgląd do danych wyświetlanych na tych monitorach. Działania te spełniały wymogi § 20 ust. 2 pkt 7 rozporządzenia KRI.
(dowód: akta kontroli str. 586)

2.6. Starostwo dysponowało 15 komputerami przenośnymi. Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI, w Urzędzie ustanowiono zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. W załączniku nr 3 do *„Polityki bezpieczeństwa dotyczącej ochrony danych osobowych"* wskazano, że korzystanie z nich poza miejscem pracy wymaga pisemnej zgody Starosty lub upoważnionego pracownika i może być wykonywane tylko w związku z realizacją zadań służbowych. Ustalono w tym dokumencie również zasady użytkowania tego sprzętu takie, jak: [1] stosowanie hasła o określonej złożoności, [2] szyfrowanie nośnika z danymi kluczem o określonej długości znaków, [3] ograniczenie do niezbędnego minimum podłączenie laptopa do sieci Internet, [4] zachowanie szczególnej odpowiedzialności podczas transportu. Wcześniej (przed wejściem w życie 25 maja 2018 r. *„Polityki bezpieczeństwa [...]"*) w § 11 *„Instrukcji zarządzania systemami informatycznymi"* wskazano, że urządzenia i nośniki zawierające dane osobowe przekazane poza siedzibę Urzędu zabezpiecza się w sposób zapewniający poufność i integralność danych, w postaci zaszyfrowanej i wyłącznie za zgodą administratora danych osobowych (Starosty) lub ABI. Jednocześnie w punkcie A.6.2 *„Deklaracji Stosowania Zabezpieczeń"* i w pkt 1.3. ppkt 7) Procedury 10 – *„Kontrola Dostępu do Informacji w Formie Elektronicznej"* wskazano, że nie stosuje się urządzeń mobilnych do realizacji zadań poza Urzędem i nie stosuje się telepracy. Dokumenty zawierające powyższe instrukcje były zamieszczone na wewnętrznej stronie internetowej Starostwa (omówionej w punkcie 1.8. wystąpienia) i w ten sposób zakomunikowane pracownikom.
(dowód: akta kontroli str. 49-69, 224-234, 149-172, 261-277, 303-304)

2.7. IOD wyjaśnił, że na dzień kontroli na laptopach stosowane było oprogramowanie, które tworzyło wirtualny szyfrowany dysk. Zalecane było przechowywanie na nim wszelkich plików zawierających dane osobowe. Dyski nie były szyfrowane, ale w przypadku zaistnienia potrzeby pracy na laptopach poza siedzibą Urzędu, IOD był gotowy zaszyfrować dysk przed rozpoczęciem świadczenia pracy na zewnątrz. (dowód: akta kontroli str. 472-475, 605-607)

---

[14] Przed obowiązywaniem tej procedury wnioski składano ustnie.
[15] Weryfikowano hasła do systemów: EZD Smart Doc, Vera Crypt, QWANT, EWMapa, Ośrodek.

2.8. Starostwo, realizując wymóg § 20 ust. 2 pkt 9 rozporządzenia KRI, wprowadziło w serwerowni rozwiązania zabezpieczające przed wstępem do niej osób nieuprawnionych i możliwością ujawnienia, modyfikacji lub zniszczenia danych. Serwerownia znajdowała się w nieoznakowanym pomieszczeniu wyposażonym w czujnik antywłamaniowy. Prowadzony był stały monitoring tego pomieszczenia. Wyposażona była w klimatyzatory, miała dedykowane łącze elektryczne, a na wypadek przerw w dostawie energii – serwery podłączone były do zasilaczy awaryjnych. Dostęp do pomieszczenia serwerowni posiadali informatycy Starostwa oraz inne upoważnione osoby (prowadzony był rejestr pracowników upoważnionych do wstępu do serwerowni). (dowód: akta kontroli str. 472, 588-589)

2.9. Stosownie do zapisów pkt A.15.1.2 i pkt A.15.1.3 *„Deklaracji stosowania zabezpieczeń"*, w umowach i porozumieniach z dostawcami i innymi stronami trzecimi świadczącymi usługi na rzecz Starostwa – wprowadza się m.in. zapisy dotyczące zachowania poufności, wskazuje się ryzyka bezpieczeństwa informacji związane z technicznymi usługami informacyjnymi, komunikacyjnymi i łańcuchem dostaw.
(dowód: akta kontroli str. 49-69)

Analizie poddano dwie umowy. W jednej z nich, na utrzymanie oprogramowania księgowego, zamieszczono zapis o zobowiązaniu się do zachowania w tajemnicy wszelkich danych i informacji uzyskanych wzajemnie[16], czym wypełniono obowiązek wskazany w § 20 ust. 2 pkt 10 rozporządzenia KRI i zapisy pkt A.15.1.2 i pkt A.15.1.3 *„Deklaracji stosowania zabezpieczeń"*. Z kolei w umowie na zakup oprogramowania do obsługi naboru do szkół nie było takich zapisów, jednakże każdorazowo jednostki oświatowe zawierały umowy powierzenia przetwarzania danych, w treści których zawarto takie zapisy[17].
(dowód: akta kontroli str. 678-739)

2.10. Postępowanie związane z przekazaniem sprzętu IT poza Starostwo opisano w pkt 11 *„Polityki bezpieczeństwa dotyczącej ochrony danych osobowych"* (przed 25 maja 2018 r. – w § 10 *„Instrukcji zarządzania systemami informatycznymi"*). Wskazano w nim, że jeśli naprawy muszą odbyć się poza Urzędem, wymontowuje się nośniki danych przed przekazaniem sprzętu na zewnątrz, a jeśli nie jest to możliwe – informatyk lub osoba upoważniona udaje się wraz ze sprzętem i nadzoruje jego naprawę poza Urzędem. W przypadku wymiany nośników zawierających dane osobowe – dane należało zarchiwizować lub nośnik zniszczyć magnetycznie, mechanicznie, termicznie bądź chemicznie, a jeśli wymieniany nośnik należało zwrócić dostawcy – uprzednio bezpiecznie usunąć dane, stosując metody wielokrotnego nadpisania. W okresie objętym kontrolą nie zachodziła konieczność zastosowania ww. regulacji i – jak wyjaśnił IOD – na dzień kontroli komputery były składowane do czasu ogłoszenia przetargu na ich utylizację.
(dowód: akta kontroli str. 224-234, 261-277, 605-607)

2.11. Systemy operacyjne wszystkich 15 objętych kontrolą komputerów posiadły zainstalowane bieżące aktualizacje. Aktualizacja systemów operacyjnych odbywała się według harmonogramów ustalonych przez dostawcę oprogramowania i była wykonywana automatycznie bez udziału pracowników. Jednocześnie w Starostwie nie wykorzystywano sprzętu komputerowego z systemem operacyjnym nieobjętym wsparciem producenta[18].
(dowód: akta kontroli str. 587)

2.12. Do tworzenia i testowania kopii zapasowych (backup) stosowany był program Ferro Backup. Kopie zapasowe dokumentów znajdujących się na poszczególnych komputerach wykonywane były dwa razy w tygodniu (różne dni dla różnych wydziałów), a raz w tygodniu kopia poczty elektronicznej (różne dni dla różnych wydziałów). Backup serwera bazodanowego wykonywany był we wtorek, czwartek i sobotę, a serwera aplikacyjnego w poniedziałek, środę i piątek. Kopie przechowywane były na oddzielnym serwerze wykorzystywanym wyłącznie do tego celu, zlokalizowanym w innym pomieszczeniu w Urzędzie. Częstotliwość wykonywania kopii zapasowych była zgodna z zasadami

---

[16] Zapis o treści: „Obie Strony zobowiązują się zachować wszelkie dane i informacje uzyskane wzajemnie w związku z wykonaniem niniejszej Umowy w ścisłej tajemnicy przed stronami trzecimi chyba, że druga Strona udzieliłaby pisemnej zgody na ich ujawnienie".

[17] Zapis o treści: „Wykonawca zobowiązuje się do przetwarzania danych osobowych zgodnie z Ustawą, przy użyciu urządzeń i systemów informatycznych zapewniających zastosowanie wysokiego poziomu bezpieczeństwa [...]".

[18] Przykładem takiego systemu operacyjnego jest Windows XP, dla którego wsparcie techniczne ustało 8 kwietnia 2014 r.

opisanymi załączniku nr 4 do *„Polityki bezpieczeństwa dotyczącej ochrony danych osobowych"* (przed 25 maj 2018 r. zasady te były opisane w § 6 *„Instrukcji zarządzania systemami informatycznymi"*). Raz do roku służby informatyczne wykonywały testowe odtworzenie kopii zapasowych (w okresie objętym kontrolą wykonano 10 odtworzeń, wszystkie zakończyły się wynikiem pozytywnym). Powyższe działania wypełniały obowiązki wskazane w § 20 ust. 2 pkt 12 lit. b i e oraz § 20 ust. 2 pkt 7 rozporządzenia KRI.
(dowód: akta kontroli str. 224-234, 261-277, 472-475, 590-591)

2.13. Wszystkie 15 komputerów (w tym pięć laptopów) poddanych oględzinom miało zainstalowane oprogramowanie antywirusowe z aktualną bazą wirusów. Wypełniono tym samym wymagania § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI. Jednocześnie, zgodnie z pkt 5 ppkt 1 *„Regulaminu ochrony danych osobowych w Starostwie Powiatowym w Augustowie"*, pracownicy byli zobowiązani do skanowania za pomocą programu antywirusowego plików wprowadzanych z zewnętrznych nośników.
(dowód: akta kontroli str. 312-321, 472-475)

2.14. Oględziny trzech serwerów wykazały, że każdy z nich dysponował wolną przestrzenią dyskową, odpowiednio 55%, 93% i 98%. IOD wyjaśnił, że sprawdzał co najmniej raz w tygodniu takie dane. (dowód: akta kontroli str. 472-475)

2.15. Nie była opracowana procedura opisująca wprowadzanie zmian w oprogramowaniu wykorzystywanym w Urzędzie. IOD wyjaśnił, że oprogramowanie dziedzinowe pobierane było z serwera plikowego, wykonywana była kopia bazy na wypadek, gdyby po instalacji wystąpiły błędy. Aktualizacja była testowana przed instalacją, a następnie instalowana sieciowo. (dowód: akta kontroli str. 605-607)

2.16. Zgodnie z obowiązkiem wskazanym w art. 30 RODO, IOD prowadził od 25 maja 2018 r. (w formie elektronicznej) rejestr czynności przetwarzania danych. Według stanu na 11 czerwca 2018 r. rejestr ten liczył 119 pozycji, zawierających wszystkie wymagane dane takie, jak:

- nazwa czynności przetwarzania,
- nazwa zbioru,
- komórka merytoryczna, w której prowadzony jest zbiór oraz inne komórki organizacyjne, w których może zajść konieczność korzystania ze zbioru,
- cel przetwarzania danych,
- kategorie osób, których dane są w zbiorze,
- kategorie danych,
- podstawa prawna przetwarzania,
- źródło danych,
- planowany termin usunięcia,
- nazwa współadministratora i dane kontaktowe,
- podmiot przetwarzający na podstawie powierzenia,
- kategorie odbiorców, inne niż podmiot przetwarzający,
- w jakiej postaci przetwarzane są dane (papierowej czy elektronicznej),
- system informatyczny lub oprogramowanie służące do przetwarzania,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO,
- operacje przetwarzania na zbiorze[19],
- ocena skutków dla ochrony danych (Data Protection Impact Assessment),
- czy podlega transferowi do kraju trzeciego lub organizacji międzynarodowej – jeśli dotyczy,

[19] Np. zbieranie, wprowadzanie, przechowywanie, przeglądanie, opracowywanie, organizowanie, porządkowanie, analizowanie, kopiowanie (ksero, skan), drukowanie, kopie bezpieczeństwa, archiwizowanie, modyfikowanie, udostępnianie, ograniczanie.

– opis dokumentacji odpowiednich zabezpieczeń, jeśli dane podlegały transferowi i sytuacji opisanej w art. 49 ust. 1 akapit drugi RODO,

– miejsce przetwarzania. (dowód: akta kontroli str. 592-596)

Ustalone nieprawidłowości

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

1. Jeden z 15 pracowników do autoryzacji w systemie informatycznym *Ośrodek*[20] stosował hasło o nieodpowiedniej długości (trzy znaki). Dane gromadzone w tym systemie były również danymi osobowymi (imię, nazwisko, adres) osób fizycznych występujących o uzgodnienie dokumentacji dotyczącej prowadzonej inwestycji (np. budowy przyłącza do sieci).

   Zgodnie z zapisami rozdziału VI, pkt 5 ppkt 3 *„Polityki bezpieczeństwa dotyczącej ochrony danych osobowych"*, w systemach informatycznych służących do przetwarzania danych osobowych, w których następuje uwierzytelnienie za pomocą hasła, ustala się to hasło z zachowaniem wymogów złożoności. W trakcie kontroli NIK hasło zostało zmienione i dostosowane do przytoczonych wymogów.
   (dowód: akta kontroli str. 224-234, 261-277, 472-475, 597-599)

   Pracownik, który stosował hasło o nieodpowiedniej długości wyjaśnił, że znał procedury dotyczące ustawania haseł dostępu, ale system nie wymagał od niego ustalenia hasła zawierającego więcej znaków. IOD wyjaśnił z kolei, że oprogramowanie to nie ma możliwości ustawienia długości i złożoności hasła.
   (dowód: akta kontroli str. 600, 605-607)

2. Jeden z 15 pracowników Starostwa był w posiadaniu i wykorzystywał hasło dostępu do systemu operacyjnego komputera innego pracownika (długotrwale nieobecnego w pracy) oraz wykonywał czynności służbowe, będąc zalogowanym na jego koncie użytkownika. Według pkt 1.1 ppkt 13 Procedury nr 10 *„Kontrola dostępu do informacji w formie elektronicznej"* – użytkownik komputera powinien zachować w tajemnicy wszelkie hasła do systemów informatycznych i nikomu ich nie ujawniać.
   (dowód: akta kontroli str. 149-172, 472-475)

   Naczelnik Wydziału Organizacyjnego wyjaśnił, że pilność spraw, które toczyły się w Wydziale w związku z obsługą Rady i Zarządu Powiatu nie pozwoliła uregulować tych spraw wcześniej. Informatykom zgłaszana była potrzeba założenia drugiego konta na tym komputerze, ale z uwagi na inne, niecierpiące zwłoki sprawy, nie zostało to zrobione do czasu przeprowadzania badania przez NIK. Powtórne oględziny tego komputera (przeprowadzone 15 czerwca 2018 r.) wykazały, że sprawa została już uregulowana, poprzez założenie dodatkowego konta użytkownika na omawianym komputerze. IOD wyjaśnił, że pracownicy wspominali mu, że należałoby na tym komputerze założyć nowe konto użytkownika, ale nie wpłynął do niego formalny wniosek o założenie dodatkowego konta[21]. Nie wiedział również, że ktoś korzysta z komputera, przy użyciu hasła nieobecnego pracownika. (dowód: akta kontroli str. 601-607, 740)

3. Jeden z 15 pracowników, których komputery poddano oględzinom, posiadał uprawnienia administratora, dające mu możliwość instalacji oprogramowania. Posiadanie takich uprawnień nie wynikało z jego zakresu obowiązków. Zgodnie zaś z zapisami pkt 1.1 ppkt 14 Procedury nr 10 *„Kontrola dostępu do informacji w formie elektronicznej"*, użytkownik nie powinien dysponować dostępem administracyjnym do systemu operacyjnego komputera. Było to również niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, według którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez podejmowania 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.
   (dowód: akta kontroli str. 149-172, 472-475, 507-509)

---

[20] Był to system dla Ośrodków Dokumentacji Geodezyjnej i Kartograficznej, ułatwiający ewidencjonowanie i zarządzanie dokumentami państwowego zasobu geodezyjnego i kartograficznego.

[21] Regulowała to Procedura nr 10 *„Kontrola dostępu do informacji w formie elektronicznej"*.

IOD wyjaśnił, że system księgowy QNT musiał być podniesiony do nowej wersji. Na każdym komputerze należało przeprowadzić prace instalacyjne, będąc zalogowanym na koncie użytkownika o uprawnieniach administratora. Po wykonaniu tych prac przez przeoczenie nie powrócono do ustawień pierwotnych i pozostały uprawnienia administratora. Uprawnienia użytkownika zostały zmienione w trakcie kontroli NIK.
(dowód: akta kontroli str. 472-473, 605-607)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, wdrożenie i wykorzystywanie rozwiązań technicznych oraz stosowanie i egzekwowanie rozwiązań organizacyjnych związanych z zapewnieniem bezpieczeństwa informacji w Starostwie.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Starostwie prowadzono okresowe analizy ryzyka utraty integralności, poufności lub dostępności, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI. W okresie objętym kontrolą przeprowadzono jedną analizę (od 5 do 7 lutego 2018 r.). Przeprowadzał je Pełnomocnik ds. SZBI oraz informatyk. W zatwierdzonych 12 stycznia 2016 r. przez Starostę dokumentach pn. *Szacowanie ryzyka System teleinformatyczny Starostwa Powiatowego* oraz *Szacowanie ryzyka EZD SP Augustów* określone zostały potencjalne zagrożenia dla systemu teleinformatycznego i systemu elektronicznego zarządzania dokumentami. Opracowane zostały macierze ryzyka, w których do każdego potencjalnego zagrożenia przypisano podatność na wystąpienie ryzyka (w skali 0–10) i skutek jego wystąpienia (w tej samej skali). Iloczyn podatności i skutków określał poziom ryzyka. Przyjęto, że poziom akceptowalny wynosił 35 pkt. Ryzyko w postaci niewspierania systemu operacyjnego Windows XP przez producenta zostało ocenione na 40 pkt i było jedynym przekraczającym poziom akceptowalny. Na 7 czerwca 2018 r. żaden z komputerów nie posiadał już tego systemu operacyjnego. Po ustaleniu w 2016 roku macierzy ryzyka, kolejne analizy ryzyka utraty integralności, poufności lub dostępności przeprowadzone zostały od 16 do 18 stycznia 2017 r. i od 5 do 7 lutego 2018 r., kiedy to analizowano m.in. audyty przeprowadzone w ramach *SZBI* i incydenty bezpieczeństwa. Analizy te nie wykazały, aby nastąpiły zmiany powodujące konieczność ponownego szacowania ryzyk, a te już zidentyfikowane były na poziomie akceptowalnym.
(dowód: akta kontroli str. 608-624)

3.2. Realizując wymaganie określone w § 20 ust. 2 pkt 13 KRI, na wewnętrznej stronie Internetowej Starostwa (omówionej szerzej w punkcie 1.8 wystąpienia) udostępniony był formularz do zgłaszania incydentów bezpieczeństwa. Pracownik, podając swoje dane (imię i nazwisko oraz adres e-mail), mógł wybrać z listy temat zgłoszenia i w kolejnym polu opisać szczegóły incydentu bezpieczeństwa. Wiadomość ze zgłoszeniem trafiała na panel administratora – w tym przypadku IDO, w celu podjęcia dalszych działań. Jednocześnie prowadzona była papierowa lista incydentów bezpieczeństwa, na której IDO rejestrował zgłaszane mu incydenty (również przekazane osobiście lub telefonicznie). Zdarzenia kwalifikowane jako incydenty bezpieczeństwa zostały opisane w załączniku nr 5 do *„Polityki bezpieczeństwa dotyczącej ochrony danych osobowych"* (przed 25 maja 2018 r. – w Procedurze nr 2 *„Postępowania z incydentami bezpieczeństwa informacji"*), która była umieszczona na stronie intranetowej Starostwa i w ten sposób zakomunikowana pracownikom. Sposób postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa opisywała Procedura nr 2 *„Postępowania z incydentami bezpieczeństwa informacji"*. W okresie objętym kontrolą wystąpiło sześć incydentów bezpieczeństwa. Podjęte zostały działania zaradcze. (dowód: akta kontroli str. 77-88, 261-277, 332-346, 472-475)

3.3. Od 20 do 24 listopada 2017 r. 55 (z 64) pracowników Starostwa odbyło szkolenie z zakresu obejmującego m.in. zagrożenia bezpieczeństwa informacji i zabezpieczanie przed nimi, zmiany w procedurze kontroli dostępu do informacji, politykę bezpieczeństwa fizycznego, politykę zarządzania wymiennymi nośnikami informacji. Pracownicy nieobecni w tych dniach w pracy (zaplanowany urlop, choroba, wyjazd służbowy) szkolenie przeprowadzali w formie e-learningu, wykorzystując materiały publikowane na wewnętrznej stronie internetowej Starostwa. Szkolenie połączone było z zagadnieniami dotyczącymi RODO, co szerzej omówiono w punkcie 3.6. wystąpienia. Nowi pracownicy Starostwa byli

szkoleni z wybranych zagadnień ustawy o ochronie danych osobowych, 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, polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi[22], *SZBI* i regulaminu ochrony danych osobowych. Realizując powyższe działania, Starostwo wypełniło obowiązek wskazany w § 20 ust. 2 pkt 6 rozporządzenia KRI. (dowód: akta kontroli str. 625-647, 741-742)

3.4. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, w Starostwie prowadzono okresowy audyt z zakresu bezpieczeństwa informacji. Przedmiotem audytów realizowanych od września do grudnia 2017 roku była m.in.:

- weryfikacja szkoleń pracowników wydziałów z zakresu ochrony danych osobowych, incydentów bezpieczeństwa,
- umiejętność korzystania z wewnętrznej strony internetowej Urzędu i wiedza o jej zawartości,
- długość stosowanych haseł do systemu operacyjnego,
- umiejętność praktycznego zgłoszenia incydentu bezpieczeństwa poprzez wewnętrzną stronę internetową Starostwa.

Weryfikowano również m.in. działanie narzędzi i usług do wychwytywania zagrożeń na połączeniu z Internetem i wykonywanie analiz ryzyka utraty integralności, poufności lub dostępności.

Audyty przeprowadzono we wszystkich 14 komórkach organizacyjnych Starostwa. Dokumentowano je poprzez wypełnienie tzw. *Karty Audytu Wewnętrznego* i szczegółowego opisu przebiegu audytu. W żadnej kontrolowanej komórce organizacyjnej nie stwierdzono nieprawidłowości. Kolejny audyt wewnętrzny – według zatwierdzonego przez Starostę harmonogramu – zaplanowano na grudzień 2018 roku. Forma przeprowadzania audytów wewnętrznych bezpieczeństwa informacji była zgodna z zapisami Procedury nr 3 *„Audyt wewnętrzny"*. (dowód: akta kontroli str. 89-99, 648-674)

3.5. W związku z art. 32 ust. 1 RODO, według stanu na 15 czerwca 2018 r. Starostwo było w trakcie analizowania zachodzących procesów przetwarzania danych osobowych i dokonywania oceny stopnia zapewnienia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk. (dowód: akta kontroli str. 605-607)

3.6. Między 20 a 24 listopada 2017 r. 55 (z 64) pracowników Starostwa odbyło szkolenie z zakresu ochrony danych osobowych według zmian, jakie niesie za sobą wejście w życie RODO. Obejmowało ono m.in. takie zagadnienia, jak: [1] podstawowe pojęcia i terminy, [2] pseudonimizacja[23], [3] przenoszenie danych, [4] legalność przetwarzania danych, [5] obowiązek informacyjny według RODO, [6] sankcje. Kolejne szkolenie związane z wejściem RODO przeprowadzono od 19 do 27 kwietnia 2018 r. Wzięło w nim udział 60 osób. Pracownicy nieobecni na szkoleniach (zaplanowany urlop, choroba, wyjazd służbowy) przeprowadzali je w formie e-learningu, wykorzystując materiały publikowane na wewnętrznej stronie internetowej Starostwa. (dowód: akta kontroli str. 625-647, 741-750)

Ustalone nieprawidłowości

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

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie podjęte przez Starostwo działania w celu zapobiegania incydentom bezpieczeństwa informacji.

---

[22] Dz. U. Nr 100 poz. 1024.

[23] Jest to proces, który polega na zmianie identyfikatorów, które są danymi osobowymi na takie, które nimi nie są (np. imiona i nazwiska osób fizycznych zastępowane są liczbami). Pseudonimizacja jest procesem odwracalnym. Najważniejszym jej aspektem jest utajnienie powiązania – reguły – starych identyfikatorów z nowymi. Dane osobowe zostaną zabezpieczone, natomiast można je odzyskać jeżeli zna się regułę zamiany starych identyfikatorów.

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[24], wnosi o prowadzenie aktualnej i kompletnej inwentaryzacji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden kierownikowi 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 Białymstoku.

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.

Białystok, 13 lipca 2018 r.

Kontrolerzy
Wojciech Zambrzycki
starszy inspektor kontroli państwowej

podpis

Dominika Jocz
inspektor kontroli państwowej

podpis

DYREKTOR DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. WICEDYREKTOR
Robert Skwarko

podpis

[24] Dz. U. z 2017 r. poz. 524, ze zm. Ustawa zwana dalej „*ustawą o NIK*".