NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu

LWR.410.015.01.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

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

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura we Wrocławiu

Kontroler

Paweł Potempski – główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/133/2018 z dnia 30 maja 2018 r.

(dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miejski w Jaworze, Rynek 1, 59-400 Jawor (dalej: „Urząd").

Kierownik jednostki kontrolowanej

Emilian Bera – Burmistrz Miasta Jawora[1] (dalej: „Burmistrz").

(dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia negatywnie działalność kontrolowanej jednostki w zakresie zarządzania bezpieczeństwem informacji[2].

Uzasadnienie oceny ogólnej

Podstawą oceny ogólnej były negatywne oceny cząstkowe dotyczące wszystkich trzech badanych obszarów kontrolnych, tj. organizacji bezpieczeństwa informacji, wdrożenia i wykorzystania rozwiązań technicznych i organizacyjnych zapewniających bezpieczeństwo informacji, oraz działań podejmowanym w celu zapobiegania incydentom bezpieczeństwa informacji.

Stwierdzone w toku kontroli nieprawidłowości dotyczyły: [1] nieopracowania i niewdrożenia systemu zarządzania bezpieczeństwem informacji, w szczególności polityki bezpieczeństwa informacji (dalej: „PBI"), wymaganego w § 20 ust. 3 w związku z 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] (dalej: *„rozporządzenie KRI"*); [2] niepowołania do dnia 5 sierpnia 2018 r. Inspektora ochrony danych (dalej: *„IOD"*) wymaganego art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/79 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] (dalej: *„RODO"*); [3] nieprowadzenia inwentaryzacji zasobów informatycznych, która zawierałaby pełne i aktualne informacje w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, co było niezgodne z § 20 ust. 2 pkt 2 *rozporządzenia KRI*; [4] przyznania uprawnień administracyjnych wszystkim pracownikom Urzędu dla wykorzystywanych zestawów komputerowych, czym naruszono uregulowania wewnętrzne w zakresie stosowanych zabezpieczeń oraz § 20 ust. 2 pkt 4 *rozporządzenia KRI;* [5] nieprzestrzegania uregulowań

[1] Od dnia 1 grudnia 2014 r.
[2] W okresie objętym kontrolą, tj. od dnia 1 czerwca 2017 r. do dnia 2 sierpnia 2018 r.
[3] Dz. U. z 2017 r. poz. 2247.
[4] Dz. Urz. UE L 119, ze zm.

wewnętrznych w zakresie przyznawania/zmiany/pozbawiania uprawnień do przetwarzania danych osobowych oraz systemów informatycznych, [6] stosowania haseł dostępowych użytkowników do systemu informatycznego niezapewniających właściwej ochrony informacji przed nieuprawnionym dostępem, co naruszało § 20 ust. 2 pkt 7 *rozporządzenia KRI*; [7] nienależytego zabezpieczenia serwerowni, w której przechowywano również kopie zapasowe serwerów, co stanowiło naruszenie § 20 ust. 2 pkt 9 oraz § 20 ust. 2 pkt 12 lit. b i e *rozporządzenia KRI*; [8] braku zapisów zobowiązujących wykonawcę do zachowania tajemnicy informacji w zawartej umowie na dostawę i serwis zestawów komputerowych, co było niezgodne z § 20 ust. 2 pkt 10 *rozporządzenia KRI;* [9] użytkowania 38 zestawów komputerowych z zainstalowanym systemem operacyjnym, który nie posiadał wsparcia producenta, co naruszało § 20 ust. 2 pkt 12 lit. a i f *rozporządzenia KRI;* [10] sporządzania i przechowywania kopii zapasowych serwerów baz danych w sposób niezapewniający wystarczającej ochrony przed utratą informacji, co było niezgodne z § 20 ust. 2 pkt 12 lit. b i e *rozporządzenia KRI;* [11] nieprowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co było niezgodne z § 20 ust. 2 pkt 3 *rozporządzenia KRI*; [12] niezapewnienia szkoleń wszystkich osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem zagadnień określonych w § 20 ust. 2 pkt 6 *rozporządzenia KRI*, jak i zagadnień związanych z *RODO*.

Ponadto Najwyższa Izba Kontroli sformułowała uwagę dotyczącą udostępniania pełnej treści „Instrukcji zarządzania systemem informatycznym" zbyt szerokiemu gronu pracowników Urzędu.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

W Urzędzie nie opracowano i nie wdrożono systemu zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 w związku z ust. 3 *rozporządzenia KRI*.

W okresie objętym kontrolą w Urzędzie obowiązywały wewnętrzne regulacje dotyczące bezpieczeństwa przetwarzania danych osobowych. W tym zakresie weszło w życie zarządzenie Burmistrza z dnia 7 stycznia 2017 r.[5] *w sprawie wprowadzenie polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie*, w oparciu o które wprowadzono do stosowania:

- *Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie*;
- *Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie*

zwane w dalszym ciągu łącznie jako „*Polityka danych osobowych*".

Z treścią powyższych dokumentów zapoznali się wszyscy pracownicy Urzędu, którzy w ramach realizowanych zadań dokonywali przetwarzania danych osobowych.

(dowód: akta kontroli str. 8-24, 127-134, 191-208)

[5] Nr 559.2017, wydanego na podstawie art. 36 ustawy z dnia 27 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. z 2017 r. poz. 922) oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jaki powinny odpowiadać urządzenia i systemy informatyczne służące przetwarzaniu danych osobowych* (Dz. U. Nr 100 poz. 1024).

Zarządzeniem Burmistrza z dnia 25 maja 2018 r.[6] znowelizowano z tym dniem regulacje w sprawie przetwarzania danych osobowych w Urzędzie. Jako podstawę prawną zarządzenia podano art. 32 ust. 1 i 2 *RODO*. W treści zawarto wynikające z *RODO* obowiązki administratora do: ograniczenia przetwarzania (art. 18), powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19), ochrony danych osobowych w fazie projektowania, domyślnej ochrony danych (art. 25), rejestrowanie czynności przetwarzania (art. 30); bezpieczeństwa przetwarzania (art. 32), zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33), oceny skutków dla ochrony danych osobowych (art. 35). Wykonanie zarządzenia z dnia 25 maja 2018 r. Burmistrz powierzył Sekretarzowi, który przekazał drogą email pracownikom Urzędu upoważnionym do przetwarzania danych osobowych ww. dokumenty w dniu 30 maja 2018 r. celem zapoznania.

(dowód: akta kontroli str. 25-73, 127-134, 191-208)

Mimo określenia w zarządzeniach Burmistrza z dnia 7 stycznia 2017 r. i 25 maja 2018 r. obowiązku wyznaczenia IOD (obowiązek wynikający z art. 37 ust. 1 *RODO* (obowiązującej od 25 maja 2018 r.) oraz administratora systemu informatycznego (dalej: „ASI")[7], do dnia 2 sierpnia 2018 r. formalnie nie wyznaczono ww. osób. W tym okresie nie wyznaczono również, na podstawie art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych*[8], administratora bezpieczeństwa informacji (dalej: „ABI"). Burmistrz wskazał, iż osoby odpowiedzialne za realizację bezpieczeństwa informacji w zakresie danych osobowych (w tym również ABI), miały te zadania od dnia 22 czerwca 2016 r. w zakresie obowiązków[9].

Po zakończeniu czynności kontrolnych, z dniem 6 sierpnia 2018 r. obowiązki IOD powierzono firmie zewnętrznej[10], co było zgodne z art. 37 ust. 6 *RODO*.

(dowód: akta kontroli str. 4-7, 8-73)

W obowiązujących w Urzędzie dokumentach w zakresie bezpieczeństwa danych osobowych[11] zawarto obowiązki: administratora danych; IOD, ASI; osób upoważnionych do przetwarzania danych; kierujących komórką organizacyjną; oraz określono środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzania danych[12].

---

[6] Nr 958.2018.

[7] Wynikające z § 3 ust. 9 zarządzenia Burmistrza z dnia 25 maja 2018 r. nr 958/2018 oraz II pkt ust. 3 zarządzenia Burmistrza z dnia 9 stycznia 2017 r. nr 559/2017.

[8] Dz. U. z 2016 r. poz. 922, ze zm.

[9] W tym m.in.: monitorowanie regulacji prawnych w zakresie ochrony danych osobowych i dostosowanie wewnętrznych regulacji do wprowadzonych zmian; prowadzenie rejestru osób upoważnionych do przetwarzania danych; zapewnienie zapoznania osobom upoważnionym do przetwarzania danych z obowiązującymi regulacjami (prowadzenie szkoleń wstępnych, opracowanie i wdrożenie programu szkoleń z zakresu ochrony danych osobowych).

[10] Burmistrz przekazał umowę już po zakończeniu czynności kontrolnych, nie podlegała ona badaniu w toku prowadzonych czynności kontrolnych w Urzędzie.

[11] Zarządzenie nr 559.2017 z dnia 7 stycznia 2017 r. oraz nr 958.2018 z dnia 25 maja 2018 r. Burmistrza w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie wraz z załącznikami.

[12] Tj. środki: ochrony fizycznej; sprzętowe infrastruktury informatycznej i telekomunikacyjnej; ochrony w ramach narzędzi programowych i baz danych; oraz procedury: nadawania upoważnień do przetwarzania danych; rejestrowania czynności przetwarzania; inwentaryzacji zbiorów danych (czynności przetwarzania). Dodatkowo wskazano: obowiązek informacyjny; prawa osób, których dane dotyczą; ocenę skutków dla ochrony danych; zasady: powierzenia przetwarzania danych; przetwarzania a publicznego dostępu do dokumentów urzędowych oraz pseudoanonimizację danych; szkoleń; incydentów i naruszenia ochrony danych. W Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie określono procedury: nadawania i zmiany uprawnień do przetwarzania danych; zarządzania i użytkowania metodami oraz środki uwierzytelniania; rozpoczęcia, zawieszenia i zakończenia pracy w systemie; tworzenia kopii zapasowych; wykonywania przeglądów i konserwacji systemu; oraz zasady: przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruki; i sposób odnotowywania w systemie informacji

(dowód: akta kontroli str. 8-73)

Zgodnie z obowiązującą polityką bezpieczeństwa, w Urzędzie zidentyfikowano zbiory danych (w tym dane osobowe) podlegające zabezpieczeniu, oraz określono zakres ich przetwarzania.

(dowód: akta kontroli str. 4-7, 94-98)

W Urzędzie nie posiadano kompletnej informacji o zasobach informatycznych jednostki obejmujących ich rodzaj i konfigurację, do czego zobowiązywały postanowienia § 20 ust. 2 pkt 2 *rozporządzenia KRI.*

W Urzędzie sprzęt komputerowy nie przypisano osobom go używającym oraz za niego odpowiedzialnym. W prowadzonej ewidencji odnotowywano jedynie pomieszczenia, w którym je przechowywano. W trakcie przeprowadzonych oględzin, w przypadku czterech z 10 skontrolowanych zestawów komputerowych stwierdzono inne niż wskazano w prowadzonej ewidencji parametry sprzętowe. Dodatkowo w kontrolowanych pomieszczeniach występowały trzy zestawy komputerowe niewystępujące w prowadzonej ewidencji, a pozostałe cztery zestawy występowały w innej lokalizacji niż wynikało z prowadzonej ewidencji.

(dowód: akta kontroli str. 4-7, 99-107, 207-208)

Ustalone nieprawidłowości

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

1. W Urzędzie nie opracowano i nie wdrożono systemu zarządzania bezpieczeństwem informacji, w szczególności PBI. Było to niezgodne z § 20 ust. 3 w związku z ust. 1 *rozporządzenia KRI*, według którego wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli zostały opracowane na podstawie Polskiej Normy PN-ISO/IEC 27001 „*Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania"* (dalej: „ISO 27001") oraz powiązanej z nią Polskiej Normy PN-ISO/IEC 27002 „*Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji" (dalej: „*ISO 27002")[13]. W okresie objętym kontrolą obowiązywało Zarządzenie Burmistrza *w sprawie polityki bezpieczeństwa danych osobowych w urzędzie…*, które nie obejmowało całościowo zagadnień określonych w *rozporządzeniu KRI*, a dotyczyło wyłącznie danych osobowych. Burmistrz wyjaśnił, iż w Urzędzie wprowadzano projekt e-urząd, m.in. modernizujący infrastrukturę informatyczną, jak i poszukiwano optymalnych rozwiązań organizacyjnych (wybór IOD). Po wyborze IOD, zostanie opracowania i wprowadzona nowa PBI, spełniająca wymogi prawne.

(dowód: akta kontroli str. 4-73, 253-257)

2. Do dnia 6 sierpnia 2018 r. nie powołano IOD wymaganego postanowieniami art. 37 *RODO*, jak i określonego uregulowaniami wewnętrznymi ASI. Burmistrz wyjaśnił, iż nie wybrał w tym terminie IOD z uwagi na poszukiwanie optymalnych rozwiązań organizacyjnych i ze względu na ograniczoną liczbę fachowców dostępnych na rynku pracy. Z dniem 6 sierpnia 2018 r. obowiązki IOD powierzono firmie zewnętrznej. Burmistrz podał również, że nie powołano ASI, gdyż zakres zadań informatyków zawierał jego zadania. NIK wskazuje, że wobec niepowołania przed dniem 25 maja 2018 r. ABI, Urząd miał – zgodnie z art. 158 ust. 4 ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych*[14] – obowiązek powołania IOD do dnia 31 lipca 2018 r.

---

o udostępnianiu danych osobowych; połączenia do sieci Internet; środki ochrony systemu przed złośliwym oprogramowaniem.

[13] W pkt 5.1 normy ISO 27002 wskazano zasady opracowania i stosowania dokumentu PBI.

[14] Dz. U. poz. 1000.

(dowód: akta kontroli str. 74-93, 253-257

3. W Urzędzie nie prowadzono inwentaryzacji zasobów informatycznych, która zawierałaby pełne i aktualne informacje w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, co było niezgodne z § 20 ust. 2 pkt 2 *rozporządzenia KRI*. Inwentaryzacja zasobów informatycznych jednostki rozumiana powinna być jako stałe posiadanie aktualnych informacji w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji. Oznacza to potrzebę prowadzenia elektronicznego rejestru zasobów teleinformatycznych nazywanego bazą konfiguracji CMDB[15]. Zgodnie z pkt 8.1.1 ISO 27002 wszystkie aktywa powinny być zidentyfikowane oraz sporządzany i aktualizowany winien być spis wszelkich aktywów informatycznych. System taki nie funkcjonował w Urzędzie. Burmistrz wyjaśnił, iż z uwagi na natłok zadań (w Urzędzie wprowadzano projekt e-urząd modernizujący infrastrukturę informatyczną), nie prowadzono szczegółowej ewidencji zasobów informatycznych, co zostanie niezwłocznie uzupełnione i uaktualnione.

(dowód: akta kontroli str. 108-111, 207-224)

Uwaga dotycząca badanej działalności

NIK zwraca uwagę, że pełna treść *„Instrukcji zarządzania systemem informatycznym"* nie powinna być udostępniona szerokiemu gronu pracowników, ponieważ zawiera szczegółowe zasady zarządzania środowiskiem informatycznym. Zdaniem NIK, treść dokumentu powinna być udostępniona wyłącznie pracownikom odpowiedzialnym za zarządzanie środowiskiem informatycznym, aby uniknąć ryzyka, że informacje zawarte w *Instrukcji* będą wykorzystane do przełamania ustanowionych zabezpieczeń.

Ocena cząstkowa

Najwyższa Izba Kontroli negatywnie ocenia organizację bezpieczeństwa informacji w Urzędzie.

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

Opis stanu faktycznego

Na użytkowanym sprzęcie komputerowym przez pracowników Urzędu, umożliwiono im, poprzez posiadanie uprawnienia administratora, możliwość instalowania oprogramowania (w tym nieautoryzowanego)[16], czym naruszono postanowienia § 20 ust. 2 pkt 2 *rozporządzenia KRI*, gdyż nie zapewniono aktualności informacji o posiadanym oprogramowaniu do przetwarzania danych.

(dowód: akta kontroli str. 232-233, 250)

Procedury - zapewniające, by osoby zaangażowane w proces przetwarzania informacji posiadały uprawnienia w zakresie adekwatnym do realizowanych przez nie zadań i obowiązków mających na celu zapewnienie bezpieczeństwa informacji (§ 20 ust. 2 pkt 4 *rozporządzenia KRI*) - zawarto w *Polityce danych osobowych*. Wewnętrznymi regulacjami przewidziano wydawanie upoważnień do przetwarzania danych osobowych oraz do systemów informatycznych[17]. Na podstawie badania

---

[15] Ang. Configuration Management Database. Jest to baza zawierająca listę wszystkich elementów, które są zarządzane w celu świadczenia usług IT. Zawiera również informację, w jaki sposób te elementy są ze sobą powiązane (tzw. relacje).

[16] Powyższe stwierdzono podczas przeprowadzonych oględzin w dniu 24 lipca 2018 r. na próbie 10 zestawów komputerowych.

[17] W zakresie przetwarzania danych: § 11 ust. 1 zarządzenia Burmistrza nr 958.2018 oraz VI. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzania danych. Środki organizacyjne pkt 1-15 Zarządzenia Burmistrza nr 559.2017, a w zakresie dostępu do systemów informatycznych w: pkt II. ust. 1 i 2 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych w Urzędzie Zarządzenia Burmistrza nr 559.2017 i pkt III ust. 1-13 tożsamej instrukcji do zarządzenia nr 958.2018 (w załączniku nr 2).

próby uprawnień do systemów informatycznych 15 pracowników[18] Urzędu ustalono, że nie przestrzegano wewnętrznych uregulowań dotyczących nadawania uprawnień pracowników, ponieważ:

- dla czterech z sześciu pracowników, którzy zmienili stanowisko nie udokumentowano zmiany upoważnień do przetwarzania danych oraz systemów informatycznych systemów;
- w 18 przypadkach (na próbę 21) nadano uprawnienia do systemów informatycznych bez udokumentowania wnioskowania przez właściwego kierownika o nadanie uprawnień;
- w jednym przypadku[19] (na 21) nie sporządzono stosownego wniosku o nadanie uprawnień do przetwarzania danych osobowych;
- w trzech przypadkach (na 21) nie sporządzono wniosku o nadanie uprawnień do przetwarzania danych osobowych.

Ponadto stwierdzono, że każdy z 15 badanych pracowników, zgodnie z § 20 ust. 2 pkt 4 *rozporządzenia KRI*, uczestniczył w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań.

Nie przestrzegano również wewnętrznych uregulowań dotyczących pozbawiania uprawnień pracowników, z którymi zakończono stosunek pracy po 1 czerwca 2017 r., tj. kierownicy jednostek organizacyjnych nie sporządzali wniosków o odebranie uprawnień dla żadnego z 15 badanych pracowników – odrębnie do - przetwarzania danych oraz systemów informatycznych, które to uprawnienia miał odbierać Burmistrz. Osobom, które zakończyły zatrudnienie w badanym okresie zostały odebrane uprawnienia do systemów informatycznych.

(dowód: akta kontroli str. 8-73, 108-111, 243-246, 247-249)

W toku przeprowadzonych w dniu 25 lipca 2018 r. oględzin trzech systemów informatycznych[20] stwierdzono, że nie pozwalały one z poziomu aplikacji, na zarządzanie ochroną przetwarzanych informacji przed nieautoryzowanym dostępem poprzez ustanawianie zasad złożoności hasła dostępowego oraz okresów, po jakim hasło użytkownika powinno być zmienione. Dodatkowo, w toku oględzin przeprowadzonych w dniu 24 lipca 2018 r. haseł do logowania do systemów operacyjnych, stwierdzono, iż w sześć na 10 haseł, ich długość nie przekraczała 7 znaków, czym naruszono wewnętrzne regulacje (*Politykę danych osobowych)* oraz postanowienia § 20 ust. 2 pkt 7 *rozporządzenia KRI*, nakazującymi wprowadzić zabezpieczenia techniczne w celu zapewnienia ochrony przetwarzania danych przed nieuprawnionym dostępem.

(dowód: akta kontroli str. 112-113, 234-236, 237-242)

W trakcie przeprowadzonych oględzin stwierdzono, że ustawienie monitorów komputerowych w miejscach obsługi obywateli w Urzędzie, uniemożliwiało wgląd do danych wyświetlanych na tych monitorach, wypełniając uregulowania zawarte w § 20 ust. 2 pkt 7 *rozporządzenia KRI*[21].

(dowód: akta kontroli str. 225)

W regulacjach wewnętrznych ustanowiono procedury dotyczące bezpiecznego przetwarzania informacji w przypadku wykonywania czynności poza Urzędem.

---

[18] W związku z faktem, że wśród 15 pracowników, odnotowano 6 zmian stanowisk skutkujące zmianą uprawnień do przetwarzania danych i systemów informatycznych, próba badawcza wykazywana poniżej wyniosła 21.

[19] Kierownik referatu ds. ochrony środowiska dla pracownika JC.

[20] FOKA Gmina, FOKA Urząd, Proton.

[21] Na podstawie oględzin przeprowadzonych w dniu 20 lipca 2018 r. w BOK, gdzie obywatele załatwiają sprawy z zakresu: dowodów osobistych (6 stanowisk w sali głównej BOK); rejestracji pism i wniosków składanych do Urzędu, (1 stanowisko w sali głównej BOK); Profilu zaufanego (1 stanowisko w sali głównej BOK); Nr Pesel, (1 stanowisko w wydzielonym pomieszczeniu w BOK); USC (po jednym stanowisku w pokoju nr 3 i 4).

Przewidziano w nich stosowanie urządzeń mobilnych w uzasadnionych przypadkach, po uzyskaniu stosownej zgody od ASI. Wskazano również, że przetwarzanie danych osobowych za pomocą urządzeń mobilnych (poza obszarem przetwarzania danych) mogło się odbywać jedynie w przypadku szyfrowania danych.

W okresie objętym kontrolą przetwarzanie danych osobowych w systemach informatycznych Urzędu odbywało się za pomocą komputerów stacjonarnych, a trzy laptopy użytkowane przez pracowników Urzędu według wyjaśnień Burmistrza nie były wynoszone. W związku z powyższym nie wydano zgody ASI na przetwarzanie danych poza obszarem Urzędu oraz nie zapewniono na nich szyfrowania danych.

(dowód: akta kontroli str. 8-73, 99-107, 237-242)

Serwerownia Urzędu była zlokalizowana w odrębnym zamykanym pomieszczeniu, wyposażonym w klimatyzację, dedykowane zasilanie elektryczne oraz system zasilania zapasowego. Część zastosowanych zabezpieczeń fizycznych serwerowni w zakresie zapewnienia bezpieczeństwa przeciwpożarowego w niewystarczającym stopniu chroniła to pomieszczenie.

(dowód: akta kontroli str. 149-150)

W trzech[22] z czterech badanych umów na dostarczenie sprzętu komputerowego obowiązujących w badanym okresie, stwierdzono występowanie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji (w myśl § 20 ust. 2 pkt 10 *rozporządzenia KRI*), tj. zawarto zapisy mówiące o zobowiązaniu wykonawcy do zachowania tajemnicy informacji, do jakich może mieć dostęp w związku z realizowaniem umowy serwisowej.

(dowód: akta kontroli str. 4-7, 114, 127-134, 151-190, 28-269)

W badanym okresie Urząd nie przekazywał sprzętu komputerowego poza jednostkę. W uregulowaniach wewnętrznych[23] zawarto postanowienia zgodne z załącznikiem A ISO 27001, punkt A.11.2.7, tj. zapewniające by przed zbyciem lub przekazaniem sprzętu komputerowego, dane zapisane na nośnikach informacji (pamięci masowe, dyski twarde) oraz licencjonowane programy, zostały usunięte.

(dowód: akta kontroli str. 4-7, 8-73)

Według stanu na dzień 27 lipca 2018 r. w 38 użytkowanych (33,0% ogółu[24]) zestawach komputerowych zainstalowany był system operacyjny Windows XP, który nie posiadał już wsparcia producenta, czym nie zapewniono odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na dbałości o aktualizację oprogramowania oraz redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych (§20 ust. 2 pkt 12 lit. a i f *rozporządzenia KRI*).

(dowód: akta kontroli str. 99-107)

Obowiązek tworzenia kopii zapasowych został uregulowany w *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie* stanowiącej część *Polityki danych osobowych*[25]. Zgodnie z powyższą procedurą kopie zapasowe wykonywano codziennie w dni robocze (nadpisywane w cyklu tygodniowym), a archiwalną kopię danych tworzono raz na tydzień.

---

[22] Umowy z dnia: 5 czerwca 2017 r.; 12 października 2017 r., 12 stycznia 2018 r.

[23] W pkt VI.4-6 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych w Urzędzie zarządzenia Burmistrza nr 559.2017 i pkt VII.4-6 tożsamej instrukcji do zarządzenia nr 958.2018 (w załączniku nr 2).

[24] Wg prowadzonej ewidencji na ten dzień użytkowano 115 zestawów komputerowych.

[25] Zarządzeniem nr 559.2017 Burmistrza z dnia 9 stycznia 2017 r. oraz 958.2018 z dnia 25 maja 2018 r. *w sprawie wprowadzenia Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie.*

W toku przeprowadzonych w dniu 25 lipca 2018 r. oględzin stwierdzono, że kopie zapasowe były wykonywane na dostępnych zasobach dyskowych (serwerze *archiwum* oraz dwóch Qnap'ach) znajdujących się w serwerowni Urzędu, i tam też były przechowywane. Kopie zapasowe zapisywano od dnia 12 czerwca 2018 r. na Qnap'ach. Na serwerze archiwalnym, stwierdzono brak wymaganych tygodniowych kopii archiwalnych w miesiącu lutym 2018 r. oraz przed grudniem 2017 r. Ze względu na to, że system ten nie zapisuje danych nieprzetestowanych (nie do odtworzenia) nie testowano dodatkowo kopii zapasowych.

(dowód: akta kontroli str. 8-73, 237-238)

W trakcie oględzin 10 komputerów ustalono, że we wszystkich zainstalowane było oprogramowanie antywirusowe, które wykorzystywało aktualne definicje wirusów, co było zgodne z § 20 ust. 2 pkt 12 lit. f *rozporządzenia KRI*.

(dowód: akta kontroli str. 232-233)

W Urzędzie nie obowiązywały procedury dotyczące monitorowania pojemności nośników pamięci systemów urzędu, a także nie stosowano oprogramowania automatyzującego monitorowanie pojemności pamięci masowych (dysków twardych) wykorzystywanych w serwerach. Monitoring taki był prowadzony ręcznie przez Informatyka.

W toku przeprowadzonych w dniu 25 lipca 2018 r. oględzin dwóch serwerów wykorzystywanych przez Urząd stwierdzono, że ich dyski twarde były zajęte w części odpowiadającej od 19,7% do 77,7% ich pojemności.

(dowód: akta kontroli str. 234-236)

Wdrażanie nowych wersji oprogramowania przeprowadzali informatycy zatrudnieni w Urzędzie. Zadania te realizowali poza godzinami pracy urzędników. Po dokonaniu wdrożenia nowej wersji oprogramowania monitorowali funkcjonowanie wdrożonych zmian. Proces ten nie był sformalizowany.

(dowód: akta kontroli str. 237-242)

Stosownie do art. 30 ust. 1 *RODO* w Urzędzie prowadzono rejestr czynności przetwarzania danych. Rejestr zawierał informacje, o których mowa w ww. przepisie.

(dowód: akta kontroli str. 4-7, 115-126)

Ustalone nieprawidłowości

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

1. Każdy z 10 badanych użytkowników komputerów niebędący pracownikiem służb informatycznych Urzędu, posiadał przyznane uprawnienia administracyjne na wykorzystywanych przez nich komputerach, czym naruszono § 20 ust. 2 pkt 4 *rozporządzenia KRI*, tj. nie zapewniono by osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia i uczestniczyły w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Burmistrz wyjaśnił, iż *Zablokowanie możliwości instalowania oprogramowania na użytkowanym sprzęcie (...) uniemożliwiałoby automatyczną aktualizację oprogramowania.* NIK nie zgadza się z tą argumentacją, ponieważ do automatycznej instalacji aktualizacji oprogramowania (w tym oprogramowania systemowego) nie jest wymagane posiadanie przez użytkowników uprawnień administratora systemu.

(dowód: akta kontroli str. 232-233, 237-242)

2. Nie przestrzegano uregulowań wewnętrznych[26] w zakresie przyznawania/ zmiany/pozbawiania uprawnień do przetwarzania danych osobowych oraz systemów informatycznych, poprzez niedokumentowanie tych czynności[27]. Burmistrz wyjaśnił, iż przyznanie lub zmianę uprawnień do przetwarzania danych osobowych oraz systemów informatycznych, dokonywano na podstawie ustnych wniosków, a wraz z zakończeniem stosunku pracy w Urzędzie nie dokumentowano odbierania uprawnień tych pracowników.

(dowód: akta kontroli str. 243-249)

3. W Urzędzie możliwe było ustanowienie przez użytkowników hasła niespełniającego standardów bezpieczeństwa, tj. zawierającego mniej niż 8 znaków, bez okresu ważności. Było to niezgodne z § 20 ust. 2 pkt 7 *rozporządzenia KRI*, stanowiącym, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na zapewnieniu ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. (co stwierdzono w przypadku sześciu użytkowników systemów operacyjnych z 10 kontrolowanych). Powyższe stanowiło także niewypełnienie uregulowań wewnętrznych obowiązujących w Urzędzie[28]. Burmistrz wyjaśnił, iż uregulowania wewnętrzne stanowią jedynie zalecenia do stosowania przez pracowników, które planowano przy najbliższej nowelizacji złagodzić, gdyż utrudniają pracę użytkownikom.

(dowód: akta kontroli str. 232-233, 237-242)

4. Serwerownia Urzędu nie posiadała dostatecznego zabezpieczenia w zakresie bezpieczeństwa przeciwpożarowego, wypełniającego zalecenia pkt 11.2.1 ISO 27002 oraz dla tego obiektu nie była prowadzona ewidencja wejść/wyjść gości, o której mowa w pkt 11.1.2 normy ISO 27002. Powyższe stanowiło naruszenie § 20 ust. 2 pkt 9 *rozporządzenia KRI*. Burmistrz wyjaśnił, iż do pomieszczeń serwerowni mają tylko dostęp informatycy, a *w budynku Urzędu nie ma obowiązku posiadania czujników ppoż. czy alarmu ppoż.* NIK nie zgadza się z powyższymi argumentami wskazując, że zgodnie z § 20 ust. 3 *rozporządzenia KRI* wymagania określone m.in. w § 20 ust. 2 pkt 9 uznaje się za spełnione, jeżeli ustanawianie zabezpieczeń odbywa się na podstawie normy ISO 27002.

(dowód: akta kontroli str. 149-150, 209-210)

5. W jednej[29] z czterech badanych umów na dostarczenie sprzętu komputerowego (obowiązujących w okresie objętym kontrolą) nie zawarto zapisów zobowiązujących wykonawcę do zachowania tajemnicy informacji, do jakich może mieć dostęp w związku z realizowaniem umowy serwisowej, co – w myśl § 20 ust. 2 pkt 10 *rozporządzenia KRI* – nie gwarantowało odpowiedniego poziomu bezpieczeństwa informacji. Burmistrz wyjaśnił, iż przedmiotowa umowa dotyczyła jedynie

---

[26] W zakresie przetwarzania danych: § 11 ust. 1 Zarządzenia Burmistrza nr 958.2018 oraz VI. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzania danych. Środki organizacyjne pkt 1-15 Zarządzenia Burmistrza nr 559.2017, a w zakresie dostępu do systemów informatycznych w: pkt II. ust. 1 i 2 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych w Urzędzie Zarządzenia Burmistrza nr 559.2017 i pkt III ust. 1-13 tożsamej instrukcji do zarządzenia nr 958.2018 (w załączniku nr 2).

[27] Tj.: dla czterech z sześciu pracowników, którzy zmienili stanowisko nie udokumentowano zmiany upoważnień do przetwarzania danych oraz systemów informatycznych systemów; w przypadku dla trzech zmian uprawnień pracowników (na próbę 20) udokumentowano wnioskowanie o nadanie uprawnień do systemów informatycznych; w jednym przypadku kierownik nie sporządził stosownego wniosku o nadanie uprawnień do przetwarzania danych osobowych; dla próby 15 pracowników, z którymi zakończono stosunek pracy, kierownicy jednostek organizacyjnych nie sporządzali wniosków o odebranie uprawnień – odrębnie do - przetwarzania danych oraz systemów informatycznych.

[28] § 9 ust. 10 *Polityki danych osobowych ....* z dnia 25 maja 2018 r.

[29] Umowa z dnia 11 stycznia 2018 r.

dostarczenia sprzętu komputerowego i nowego oprogramowania, bez dostępu do informacji wewnętrznych Urzędu. NIK wskazuje, iż zgodnie z treścią § 1 ust. 1 przedmiotowej umowy, do obowiązków wykonawcy umowy należało również świadczenie usług serwisu gwarancyjnego sprzętu komputerowego.

(dowód: akta kontroli str. 151-190, 209-210)

6. W 38 użytkowanych zestawach komputerowych zainstalowany był system operacyjny Windows XP, który nie posiadał już wsparcia producenta. Było to niezgodne z § 20 ust.2 pkt 12 lit. a i f *rozporządzenia KRI*, który stanowi, że należy zapewnić odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, polegający w szczególności na dbałości o aktualizację oprogramowania oraz redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych. Burmistrz wskazał, iż *sprzęt komputerowy (...) posiada oprócz zabezpieczeń systemowych producenta oprogramowania systemu operacyjnego jest dodatkowo zabezpieczony oprogramowaniem antywirusowym oraz innymi zabezpieczeniami.* Burmistrz wskazał, iż Urząd sukcesywnie wycofywał sprzęt komputerowy z Windows XP, w miarę możliwości czasowych informatyków Urzędu.

(dowód: akta kontroli str. 99-107, 237-242)

7. Kopie zapasowe serwerów i baz danych były wykonywane na dostępnych zasobach dyskowych znajdujących się w serwerowni Urzędu i tam też były przechowywane (tj. w miejscu przetwarzania danych). Ponadto, nie wykonywano cotygodniowych kopii archiwalnych do grudnia 2017 r. i w lutym 2018 r. Było to niezgodne z regulacjami wewnętrznymi Urzędu, wymagającymi sporządzania kopii archiwalnych raz w tygodniu oraz przechowywania ich w zamykanych szafach. Stanowi to również naruszenie § 20 ust. 2 pkt 12 lit. b i e *rozporządzenia KRI*. Burmistrz wyjaśnił, iż prowadzono prace dostosowujące pomieszczenie w piwnicach Urzędu, gdzie umieszczone zostaną kopie zapasowe serwerów oraz uaktualnione zapisy Polityki bezpieczeństwa.

(dowód: akta kontroli str. 8-73, 234-242)

Ocena cząstkowa

Najwyższa Izba Kontroli negatywnie ocenia wdrożone i wykorzystywane w Urzędzie rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

W okresie objętym kontrolą w Urzędzie nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, o których mowa w § 20 ust. 2 pkt 3 *rozporządzenia KRI*.

(dowód: akta kontroli str. 4-7, 191-206, 237-242)

W obowiązującej w Urzędzie *Polityce danych osobowych* uregulowano wymóg wynikający z postanowień § 20 ust. 2 pkt 13 *rozporządzenia KRI* dotyczące bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji oraz obowiązki określone w art. 36 *RODO* w zakresie zgłaszania incydentów dotyczących danych osobowych[30]. Pracownicy zostali zapoznani z powyższymi regulacjami. Według informacji udzielonej przez Burmistrza, badanym okresie nie stwierdzono incydentów z zakresu naruszenia bezpieczeństwa informacji.

[30] Odpowiednio w Zarządzeniu nr 559.2017 – załącznik nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie – do 25 maja 2018 r., a po tym dniu w Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych (załączniku nr 9 do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie).

(dowód: akta kontroli str. 8-73, 251)

W obowiązującej *Polityce danych osobowych* uregulowano kwestię szkoleń pracowników zaangażowanych w proces przetwarzania informacji, tj. wynikający z postanowień § 20 ust. 2 pkt 6 *rozporządzenia KRI*[31]. Według zapisów zawartych w ww. *Polityce,* odpowiedzialnym za zorganizowanie szkoleń był IOD. W badanym okresie przeszkolono pięciu pracowników zatrudnionych w Urzędzie na staż lub praktyki. Mimo zatrudnienia w okresie od czerwca 2017 r. do lipca 2018 r. 13 pracowników, nie zostali oni przeszkoleni w zakresie bezpieczeństwa informacji.

(dowód: akta kontroli str. 127-134, 209-224, 237-242)

Wypełniając postanowienia § 20 ust. 2 pkt 14 *rozporządzenia KRI*, w Urzędzie przeprowadzono w 2017 r. audyt zewnętrzny z zakresu bezpieczeństwa informacji. W sprawozdaniu z audytu[32], stwierdzono, iż *proces udokumentowania przyjętych w Urzędzie rozwiązań w zakresie KRI oraz ich wdrożenie w Urzędzie nie jest w pełni adekwatny, skuteczny i efektywny*. Sformułowano w nim szereg zaleceń, dot. m.in. powołania IOD; wprowadzenia zasady zarządzania ryzykiem w zakresie SZBI; zapewnienia aktualności inwentaryzacji sprzętu i oprogramowania; wyeliminowania możliwości instalowania oprogramowania na kontach użytkownika; zapewnienia szkoleń pracowników. Do dnia 2 sierpnia 2018 r., nie wykonano zaleceń z ww. audytu. Burmistrz wskazał, iż rekomendacje wciąż wprowadzano, lecz wprowadzany projekt e-usług w Urzędzie generował zwiększoną ilość obowiązków i nakładów pracy związanych z wymianą sprzętu i instalacją nowoczesnego oprogramowania, co skutkowało niepełnym wykonaniem zaleceń.

(dowód: akta kontroli str. 135-148, 226-231, 237-242)

Wypełniając regulacje wynikające z postanowień art. 32 ust. 1 *RODO*, w Urzędzie przeprowadzono analizę zachodzących procesów przetwarzania danych, kwalifikując do nich stosowne zabezpieczenia dla bezpiecznego przetwarzania danych.

(dowód: akta kontroli str. 4-7, 125-136)

W uregulowaniach wewnętrznych przewidziano obowiązek szkolenia dla osób upoważnionych do przetwarzania danych raz na dwa lata, bądź częściej np. w przypadku zmiany przepisów. Nie stwierdzono zorganizowania szkoleń dla osób upoważnionych do przetwarzania danych w okresie od dnia 22 czerwca 2016 r. do dnia 2 sierpnia 2018 r., pomimo iż od 25 maja 2018 r. weszły w życie przepisy *RODO*.

W badanym okresie czterech pracowników Urzędu uczestniczyło w szkoleniach zewnętrznych w zakresie *RODO*, a w dniu 12 września 2018 r. (wg Burmistrza w pierwszym wolnym terminie) planowano przeprowadzić szkolenie pozostałych pracowników Urzędu w tym zakresie.

(dowód: akta kontroli str. 237-242)

Ustalone nieprawidłowości

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

1. W Urzędzie nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji. Było to niezgodne z § 20 ust. 2 pkt 3 *rozporządzenia KRI*, które zobowiązywało do wykonywania takich analiz oraz do podejmowania działań minimalizujących te ryzyka. Burmistrz wyjaśnił, iż takie analizy odbywały się w sposób ciągły poprzez monitorowanie zagrożeń mogących wystąpić podczas pracy Urzędu. Zdaniem NIK powyższe analizy powinny zostać

[31] W *Polityce szkoleń osób upoważnionych do przetwarzania danych osobowych w Urzędzie* (załącznik nr 8 do Polityki bezpieczeństwa danych osobowych w Urzędzie).
[32] Sporządzonego w dniu 17 listopada 2017 r.

określone w formie pisemnej, w regulacjach wewnętrznych opisujących sposób zarządzania ryzykiem bezpieczeństwa informacji. Taka analiza powinna zawierać m.in. opis procesu szacowania ryzyka, tj. od jego identyfikacji, poprzez analizę i ocenę ryzyka, do sporządzenia planu postępowania z ryzykiem oraz z jego wystąpieniem.

(dowód: akta kontroli str. 4-7, 191-206, 237-242)

2. W Urzędzie nie zapewniono szkoleń dla 13 osób zatrudnionych w okresie od dnia 1 czerwca 2017 r. do dnia 30 czerwca 2018 r. i zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem zagadnień określonych w § 20 ust. 2 pkt 6 *rozporządzenia KRI*. Burmistrz wyjaśnił, że wynikało to z nieobecności osoby odpowiedzialnej za szkolenie i w najbliższym czasie zostaną te osoby przeszkolone.

(dowód: akta kontroli str. 127-134, 209-224, 237-242)

3. W Urzędzie w okresie od dnia 22 czerwca 2016 r. do dnia 2 sierpnia 2018 r. przeszkolono jedynie czterech pracowników w zakresie zmian wynikających z wprowadzenia *RODO*. Nie zapewniono szkoleń pozostałych pracowników Urzędu zaangażowanych w proces przetwarzania informacji, mimo zmiany obowiązujących przepisów od dnia 25 maja 2018 r. (tj. obowiązywania *RODO*), do czego zobowiązywały również regulacje wewnętrzne, wprowadzające obowiązek szkolenia osób upoważnionych do przetwarzania danych raz na dwa lata, bądź częściej np. w przypadku zmiany przepisów. Burmistrz wyjaśnił, iż przeszkolił jedynie cztery osoby (odpowiedzialne za realizację przepisów ochrony danych) w zakresie *RODO*, oraz zaplanowano w dniu 12 września 2018 r. przeprowadzenie szkolenia pozostałych pracowników Urzędu w tym zakresie.

(dowód: akta kontroli str. 237-242)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie realizację działań Urzędu podejmowanych w celu zapobiegania incydentom bezpieczeństwa informacji.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny 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*[33] (dalej: „*ustawa o* NIK"), wnosi o:

1. Opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji, uwzględniającego zalecenia normy PN-ISO/IEC 27001 i norm z nią związanych (PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762).
2. Prowadzenie aktualnej i kompletnej inwentaryzacji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację.
3. Wdrożenie rozwiązań umożliwiających odpowiednie zabezpieczenie pomieszczenia serwerowni.
4. Przechowywanie kopii zapasowych poza miejscem ich wytwarzania.
5. Odebranie pracownikom Urzędu uprawnień administratora systemu, nieadekwatnych do zadań przez nich realizowanych.
6. Wprowadzenie w Urzędzie obowiązku stosowania haseł dostępu do systemów informatycznych składających się z co najmniej ośmiu znaków oraz o odpowiedniej złożoności.

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

7. Uwzględnianie w umowach zawieranych z podmiotami zewnętrznymi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
8. Wykorzystywanie w Urzędzie systemów operacyjnych posiadających wsparcie producenta.
9. Prowadzenie okresowych analiz utraty integralności, dostępności lub poufności informacji i podejmowanie działań minimalizujących stwierdzone ryzyko.
10. Zapewnienie szkoleń dla osób zaangażowanych w proces przetwarzania informacji – zgodnie z § 20 ust. 2 pkt 6 *rozporządzenia KRI*, oraz w zakresie ochrony danych osobowych – w związku z wejściem w życie *RODO*.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

Obowiązek poinformowania NIK o sposobie wykonania wniosków pokontrolnych i wykorzystania uwagi

Zgodnie z art. 62 *ustawy o NIK* proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwagi 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.

Wrocław, dnia 10 września 2018 r.

Kontroler:
Paweł Potempski
Główny specjalista kontroli państwowej

Potempski
.....
podpis

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
Dyrektor

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