**WOJEWODA**
**ZACHODNIOPOMORSKI**

Szczecin, dnia 8 grudnia 2016 r.

K–2.431.1.1.2016.5.EM

# WYSTĄPIENIE POKONTROLNE

| | |
|---|---|
| **Obszary kontroli** | 1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.<br>2. Zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych.<br>3. Zapewnienie dostępności informacji zawartych na stronie internetowej urzędu dla osób niepełnosprawnych. |
| **Nazwa i adres organu kontrolującego** | Wojewoda Zachodniopomorski,<br>ul. Wały Chrobrego 4, 70-502 Szczecin |
| **Nazwa i adres organu kontrolowanego** | Burmistrz Miasta i Gminy Stepnica[1],<br>ul. T. Kościuszki 4, 72 – 112 Stepnica. |
| **Osoba pełniąca funkcję Burmistrza Miasta i Gminy Stepnica w okresie objętym kontrolą / w okresie prowadzenia kontroli** | Pan Andrzej Wyganowski |
| **Okres objęty kontrolą** | od dnia 1 stycznia 2015 r. do dnia 21 września 2016 r. |
| **Kontrolujący** | 1. Pani Edyta Mastalerz – inspektor wojewódzki w Oddziale Koordynacji i Realizacji Kontroli w Wydziale Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie, *kierownik zespołu kontrolującego*.<br>2. Pani Anna Dąbska – kierownik Oddziału Koordynacji i Realizacji Kontroli w Wydziale Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego. |
| **Nr upoważnienia** | Nr 30/2016 z dnia 16 września 2016 r. |
| **Podstawy prawne do przeprowadzenia kontroli** | – art. 6 ust. 4 pkt 3 w związku z art. 2 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[2];<br>– art. 25 ust. 1 pkt 3 lit. a, w związku z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[3]. |
| **Kryteria prowadzenia kontroli** | legalność, rzetelność. |
| **Termin kontroli** | 19 – 21 września 2016 r. |

[1] Zwany dalej „Burmistrzem".
[2] Dz. U. Nr 185, poz. 1092.
[3] Dz. U. z 2014 r., poz. 1114.

| USTALENIA KONTROLI | |
|---|---|
| **Akty prawne, na podstawie, których dokonano ustaleń w toku kontroli** | - ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4];<br>- rozporządzenie 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[5];<br>- rozporządzenie Ministra Administracji i Cyfryzacji w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[6]. |
| **Osoby udzielające wyjaśnień w trakcie kontroli** | Pani Mariola Kwiryng, Sekretarz Gminy,<br>Pan Marcin Sokoliński, wykonujący obsługę informatyczną Urzędu[7]. |
| **Obszar kontroli Nr 1** | Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną. |
| *1.1 Usługi elektroniczne* | |
| **Podstawa prawna** | **Art. 16 ust. 1a ustawy:** *Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.*<br>**§ 5 ust. 2 pkt 1 i 4 rozporządzenia KRI**: *Interoperacyjność na poziomie organizacyjnym osiągana jest przez:*<br>- *informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty;*<br>- *publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.* |
| **Ustalenia kontroli**<br>Urząd Miasta i Gminy Stepnica[8] posiada aktywną Elektroniczną Skrzynkę Podawczą znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej[9]. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę ePUAP, zawarto na stronie internetowej Urzędu w BIP oraz w menu pionowym „BOI"[10] w podgrupie „ESP ePUAP". Urząd udostępniał oraz świadczył usługę elektroniczną, z wykorzystaniem ePUAP tj. „Pismo ogólne do podmiotu publicznego". (Dowód: akta kontroli str. 8, 242, 243 - 244) | |

[4] Zwana dalej „Ustawą".

[5] Dz. U. z 2016 r., poz. 113, zwane dalej „rozporządzeniem KRI".

[6] Dz. U. z 2014 r., poz. 584, zwane dalej „rozporządzeniem ePUAP".

[7] Zwany dalej „informatykiem Urzędu", na podstawie Umowy Nr 119/2015 z dnia 30.04.2015 r. na świadczenie usług informatycznych.

[8] Zwany dalej „Urzędem".

[9] Zwanej dalej „ePUAP".

[10] Biuro Obsługi Interesanta, zwane dalej „e-BOI".

Na dzień przeprowadzenia czynności kontrolnych strona internetowa Urzędu posiadała bezpośrednie połączenie z BIP oraz e-BOI jednakże nie posiadała informacji nt. świadczonych usług drogą elektroniczną.
Za pośrednictwem strony internetowej Urzędu (www.stepnica.pl), ikony „e-boi obsługa interesanta" odsyłającej do „Elektronicznego Biura Obsługi Interesanta Urzędu", Urząd udostępnił dla obywateli portal, gdzie zawarto niezbędne informacje dotyczące form załatwienia spraw metodą tradycyjną i elektroniczną oraz wykazane zostały usługi prowadzone przez Urząd. W tzw. „Poradniku Interesanta" wyjaśniono, czym jest ePUAP dla obywatela, opisano „krok po kroku" sposób założenia i odbioru dokumentów oraz możliwość sprawdzenia stanu sprawy.
(Dowód: akta kontroli str. 12 - 13)

Na platformie e-BOI Urząd dokonał wydzielenia, w nawigacji poziomej, świadczone usługi od elektronicznych formularzy, przy czym część usług posiadała możliwość realizacji sprawy za pośrednictwem elektronicznych formularzy z ePUAP.
W menu poziomym na e-BOI umieszczono w postaci ikon „Wnioski elektroniczne i karty usług", „Elektroniczną skrzynkę podawczą" oraz „Elektroniczne formularze z ePUAP".
W części „Wnioski elektroniczne i karty usług", na dzień przeprowadzenia czynności kontrolnych udostępnionych zostało 61 usług zawartych w 9 grupach. Szczegółowym badaniem objęto 7 usług świadczonych poprzez eBOI:

- Deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi – „Elektroniczny formularz wniosku" odsyłał na stronę ePUAP, z informacją „Wskazany Urząd nie obsługuje jeszcze poniższej sprawy";
- Skargi, wnioski, zapytania do urzędu – „Elektroniczny formularz wniosku" odsyłał na stronę ePUAP na „Pismo ogólne do podmiotu publicznego";
- Wycinka drzew i krzewów – zezwolenia – załączono wniosek w pliku pdf;
- Wpis do ewidencji obiektów świadczących usługi hotelarskie, nie będących obiektami hotelarskimi - załączono wniosek w pliku pdf;
- Wniosek o dofinansowanie kosztów kształcenia młodocianego – załączono wniosek w pliku pdf;
- Wniosek o sprzedaż nieruchomości w trybie przetargu – załączono wniosek w pliku pdf „Wniosek o nabycie nieruchomości gruntowej w drodze przetargu";
- Wniosek o wydanie zaświadczenia o niezaleganiu w podatkach – załączono wniosek w pliku word (.doc), dodatkowo udostępniono funkcjonalność, która umożliwiała generowanie druku przelewu.

Wszystkie skontrolowane usługi posiadały sporządzoną kartę opisu usługi, w której określono właściciela usługi (komórkę organizacyjną urzędu, stanowisko), opłaty, termin i sposób realizacji, aktualną podstawę prawną, wymagane dokumenty, tryb odwoławczy oraz dodatkowe informacje, uwagi. (Dowód: akta kontroli str. 27 – 29, 246 – 263)

Świadczenie części usług elektronicznych przez Urząd za pośrednictwem ePUAP możliwe do wykonania było jedynie przy tych usługach, gdzie na e-BOI (przy usłudze) znajdował się link do elektronicznych formularzy. (Dowód: akta kontroli str. 243, 261)

W ikonie „Elektroniczna skrzynka podawcza" zawarto przekierowanie na ePUAP oraz informację nt. załatwiania spraw urzędowych przez internet (plik graficzny z epuap.gov.pl).
(Dowód: akta kontroli str. 14)

W części „Elektroniczne formularze z ePUAP" zawarto informację nt. obowiązujących formularzy elektronicznych, które powinny być udostępnione w skrzynce podawczej na ePUAP Urzędu.

Zawarto w tej części 11 formularzy podzielonych na 5 grup. Formularze posiadały nawigację poprzez treść na ePUAP (aktywny link). W grupie:

1. „Działalność gospodarcza" formularze które posiadały:
   - aktywny link: „CEIDG – „Wniosek o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej" - brak możliwości skorzystania z formularza, na ePUAP podana była informacja „Wskazany urząd nie obsługuje jeszcze poniższej sprawy";
   - nieaktywne linki: „Wpis do rejestru posiadaczy odpadów prowadzących działalność w zakresie zbierania odpadów lub prowadzących działalność w zakresie transportu odpadów, którzy są zwolnieni z obowiązku uzyskania zezwolenia na prowadzenie ww. działalności", „Wpis do ewidencji obiektów świadczących usługi hotelarskie, nie będących obiektami hotelarskimi".
2. „Ochrona środowiska" formularze, które posiadały:
   - aktywny link: „Deklaracja o wysokości opłat za gospodarowanie odpadami komunalnymi" – brak możliwości skorzystania z formularza na ePUAP podana była informacja „Wskazany urząd nie obsługuje jeszcze poniższej sprawy";
   - nieaktywny linki: „Wycinka drzew i krzewów – zezwolenia".
3. „Ogólne sprawy Urzędu" formularz, który posiadał aktywny link: „Skargi, wnioski, zapytania do urzędu" – brak możliwości skorzystania z formularza.
4. „Planowanie, zagospodarowanie przestrzenne i budownictwo", wskazane trzy formularze posiadały nie aktywne linki.
5. „Urząd Stanu Cywilnego" wskazane dwa formularze posiadały nie aktywne linki.

(Dowód: akta kontroli str. 15 – 19)

| | |
|---|---|
| **Zakres i skutki stwierdzonych uchybień** | Na dzień przeprowadzenia czynności kontrolnych, na platformie e-BOI w wydzielonych funkcjonalnościach:<br>- „Wnioski elektroniczne i karty usług" w usłudze „Deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi" posiadającej elektroniczny formularz wniosku;<br>- „Elektroniczne formularze z ePUAP" wszystkie wykazane formularze,<br>nie posiadały możliwości realizacji sprawy przez ePUAP, co skutkuje brakiem spełnienia wymogu dotyczącego zakresu użytkowego posiadanego serwisu. (Dowód: akta kontroli str. 28, 15 – 19) |

*1.2 Centralne repozytorium wzorów dokumentów elektronicznych*

| | |
|---|---|
| **Podstawa prawna** | **Art. 19 b ust. 3 ustawy:** *Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich bezpiecznym podpisem elektronicznym.* |

**Ustalenia kontroli**

Urząd w badanym okresie do centralnego repozytorium wzorów dokumentów ePUAP nie przekazywał wzorów dokumentów elektronicznych. Urząd jedynie korzystał ze wzoru dokumentu „Pismo ogólne do podmiotu publicznego". (Dowód: akta kontroli str. 45, 243 – 245)

**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.**

| 1.3 Model usługowy | |
|---|---|
| **Podstawa prawna** | **§ 15 ust. 2 rozporządzenia KRI:** *Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.*<br>**§ 8 rozporządzenia ePUAP:** *Platforma ePUAP udostępnia katalog usług zawierający informacje o usługach, a w szczególności: 1) podstawę prawną usługi; 2) nazwę usługi; 3) nazwę usługodawcy; 4) cel usługi; 5) odbiorców usługi; 6) kategorię usługi; 7) umiejscowienie usługodawcy według podziału administracyjnego kraju.* |

**Ustalenia kontroli**

Strona internetowa Urzędu działa pod adresem www.stepnica.pl, a strona internetowa BIP Urzędu – pod adresem http://bip.stepnica.pl. Na stronie internetowej Urzędu zamieszono link do strony BIP oraz e-BOI. Na stronie internetowej BIP Urzędu zamieszczono link na ePUAP oraz na e-BOI. Urząd wykorzystywał platformę e-BOI, jako główne narzędzie do świadczenia usług elektronicznych poprzez automatyczną integrację ePUAP z e-BOI.

(Dowód: akta kontroli str. 242, 244, 264)

W takcie kontroli ustalono, że dla świadczenia usług elektronicznych, w dniu 18 grudnia 2014 r. Burmistrz zawarł umowę w zakresie udostępnienia systemu e-URZĄD w skład, którego wchodzi: Elektroniczny Obieg Dokumentów e-OBIEG, Biuletyn Informacji Publicznej BIP, Elektroniczne Biuro Obsługi Interesanta e-BOI, strona www oraz poczta e-mail. W umowie określono sposób zgłaszania awarii[11] oraz wyznaczony został administrator systemu e-URZĄD - informatyk Urzędu[12], z którym Burmistrz podpisał umowę na świadczenie usług informatycznych.
W umowie o udostępnienie systemu e-URZĄD nie określono czasu reakcji wykonania zgłoszenia o wystąpieniu awarii, jednakże na uwagę zasługuje fakt, iż w dniu wykonywania czynności kontrolnych miała miejsce awaria połączenia systemu e-OBIEG z platformą e-PUAP. Zgłoszenie jej nastąpiło zgodnie z zawartą umową, a przywrócenie funkcjonalności między systemami wykonano w ciągu 24 godzin.
W umowie zawartej z informatykiem Urzędu na świadczenie usług informatycznych, określono zasady zgłaszania uwag, awarii oraz podano czas reakcji wraz z terminem usunięcia awarii[13]. Profil Urzędu na platformie ePUAP obsługiwany jest przez informatyka Urzędu oraz Sekretarza.

(Dowód: akta kontroli str. 269, 271 – 272, 275 -276, 243, 284, 285, 288 – 290)

Badanie zapisów procedur dotyczących usługi ePUAP „Pismo ogólne do podmiotu publicznego" oraz 7 usług na e-BOI, dla których wykonanie części czynności Urząd umożliwił drogą elektroniczną[14] wykazało, że ich opisy zamieszczone na platformie e-BOI zawierały zgodnie z wymogami rozporządzenia ePUAP – dane dotyczące: właściciela usługi (komórka organizacyjna urzędu, stanowisko), opłaty, termin i sposób realizacji, aktualną podstawę prawną, wymagane dokumenty, tryb odwoławczy oraz dodatkowe informacje i uwagi.

(Dowód: akta kontroli str. 27 – 29, 246 – 263)

Urząd w procesie zarządzania usługami elektronicznymi wspiera model usługowy.
W celu popularyzacji modelu usług świadczonych drogą elektroniczną w Urzędzie otwarto punkt potwierdzania „Profilu zaufanego". Sposób organizacji i zasady działania Punktu Potwierdzającego Profile Zaufane ustanowione zostały Zarządzeniem Nr 119/2015 Burmistrza Miasta i Gminy

[11] § 9 pkt 2, 3, 4 Umowy Nr 414/2014 z dnia 18.12.2014 r. na udostępnienie systemu e-URZĄD.
[12] § 4 Umowy Nr 414/2014 z dnia 18.12.2014 r. na udostępnienie systemu e-URZĄD.
[13] § 5 Umowy Nr 11/2015 z dnia 30.04.2015 r. na świadczenie usług informatycznych.
[14] Opisanych w punkcie 1.1 wystąpienia pokontrolnego.

| | |
|---|---|
| Stepnica z dnia 18 grudnia 2015 r. w sprawie utworzenia i zasad działania Punktu Potwierdzającego Profile Zaufane elektronicznej Platformy Usług Administracji Publicznej (ePUAP).<br>(Dowód: akta kontroli str. 291 - 303) | |
| **Zakres, przyczyny i skutki stwierdzonych uchybień** | W umowie zawartej na świadczenie usług informatycznych oraz w zakresie czynności Sekretarza, brak jest zapisu stanowiącego o obsłudze profilu Urzędu na platformie ePUAP.<br>W umowie zawartej na udostępnienia sytemu e-URZĄD nie podano czasu reakcji wykonania zgłoszenia o wystąpieniu awarii oraz nie określono maksymalnego czasu niedostępności systemu.<br>Brak ustalenia odpowiedzialności za utrzymanie usługi oraz określenia poziomu niedostępności usług skutkować może nie wykonaniem ich na zdeklarowanym poziomie. |
| *1.4 Współpraca systemów teleinformatycznych z innymi systemami* | |
| **Podstawa prawna** | **§ 5 ust. 3 pkt 3 rozporządzenia KRI:** *Interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.*<br>**§ 16 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.* |

**Ustalenia kontroli**

Zakres i sposób współpracy systemów informatycznych wewnątrz Urzędu oraz ich współpraca z systemami zewnętrznymi (m.in. innych jednostek administracji publicznej) zbadano na próbie wybranych trzech systemów, tj.:

1. Programu do obsługi Lokalnego Rejestru Mieszkańców[15] – wspierającego prowadzenie rejestru mieszkańców, rejestru zamieszkania cudzoziemców oraz rejestru wyborców, który umożliwia tworzenie spisów i zestawień z ww. rejestrów;
2. Oprogramowania PB_USC w skład, którego wchodzi EKSPORT_USC – gromadzącego dane zgodnie z ustawą o aktach stanu cywilnego m.in. o urodzeniach, małżeństwach i zgonach oraz umożliwiającego przeniesienie danych za pośrednictwem aplikacji ŹRÓDŁO – do centralnego rejestru stanu cywilnego prowadzonego przez Ministra Spraw Wewnętrznych oraz wspierającego zarządzanie archiwum USC i wykonywanie czynności kancelaryjnych;
3. Systemu e-URZĄD w skład, którego wchodzi Elektroniczny Obieg Dokumentów e-OBIEG, Biuletyn Informacji Publicznej BIP, Elektroniczne Biuro Obsługi Interesanta e-BOI, strona www oraz poczta e-mail – wspomagającego elektroniczny obieg dokumentów oraz elektroniczną komunikację z obywatelem poprzez komunikację z platformą ePUAP. (Dowód: akta kontroli str. 35, 306 – 307, 318, 326, 264, 227)

**Program Ewidencja Ludności** – działa na poziomie jednostronnej komunikacji z systemem ŹRÓDŁO. Komunikacja następuje poprzez automatyczne przesyłanie danych z systemu ŹRÓDŁO

[15] Zwanego dalej „ Programem Ewidencja Ludności".

do Programu Ewidencja Ludności. Do Programu Ewidencja Ludności pobierane są subskrypcje z systemu ŹRÓDŁO z wykorzystaniem protokołu komunikacyjnego SOAP, dane kodowane są do postaci wyrażalnej w xml. (Dowód: akta kontroli str. 35, 304)

**Oprogramowanie PB_USC** – działa na poziomie jednostronnej komunikacji z systemem ŹRÓDŁO. Umożliwia pracownikowi wprowadzanie ręczne danych do programu (m.in. dane o urodzeniach, zawartych małżeństwach i zgonach) następnie zapisuje informację. Migracja danych do systemu ŹRÓDŁO odbywa się poprzez protokół komunikacyjny https (protokół szyfrujący TLS) oraz protokół SOAP. Program umożliwia tworzenie plików xml.
(Dowód: akta kontroli str. 35, 304, 307, 311, 326)

**System e-URZĄD** – działa na poziomie jednostronnej komunikacji. System powiązany jest z platformą ePUAP. Pracownik tworzy paczkę danych i dokonuje jej wysyłki lub odbioru danych przekazanych poprzez ePUAP. System e-URZĄD służy do elektronicznego obiegu dokumentów w całym urzędzie. Dane pomiędzy systemami są natychmiast synchronizowane. System umożliwia eksport i import danych w formatach jpg, pdf, xls, doc, xml, docx. Komunikacja systemu e-URZĄD z ePUAP jest automatyczna. (Dowód: akta kontroli str. 44, 242, 264, 367, 370)

Prowadzone rejestry publiczne odwoływały się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.
Współpraca pomiędzy systemami Urzędu była możliwa jedynie dzięki wyposażeniu w odpowiednie składniki sprzętowe oraz oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących. Systemy informatyczne spełniały minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu, jak również systemami innych jednostek administracji publicznej.

**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.**

*1.5 Obieg dokumentów w Urzędzie*

| | |
|---|---|
| **Podstawa prawna** | **§ 20 ust. 2 pkt 9 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególność przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.* |

**Ustalenia kontroli**
W Urzędzie w celu zarządzania obiegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do Urzędu zawarte w Instrukcji Kancelaryjnej, stanowiącej załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych[16]. W Urzędzie obowiązuje tradycyjny (papierowy) system wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci nie elektronicznej z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentacji, zgodnie z § 33 Regulaminu Organizacyjnego Urzędu Miasta i Gminy w Stepnicy, wprowadzonego Zarządzeniem Nr 8/2014 Burmistrza Miasta i Gminy Stepnica z dnia 28 lutego 2014 r. (Dowód: akta kontroli str. 376, 380, 381 – 388)

[16] Zwana dalej „Instrukcją Kancelaryjną".

| | |
|---|---|
| Czynności kancelaryjne w systemie e-OBIEG wykonywano zgodnie z przepisami rozporządzenia w sprawie Instrukcji Kancelaryjnej, w następujący sposób:<br>- pisma składane przez klientów za pomocą ePUAP były automatycznie przekierowane do systemu e-OBIEG, następnie przez kancelarię główną rejestrowane i przesyłane do dekretacji w systemie do adresatów wskazanych w pismach (tj. Burmistrza, Sekretarza, kierowników referatów);<br>- dekretację danego pisma w systemie dokonywał Burmistrz, Sekretarz, kierownik referatu i przekazywał do właściwego referatu lub pracownika (wg kompetencji określonych w regulaminie organizacyjnym lub w zakresie czynności pracownika);<br>- po przygotowaniu odpowiedzi (poza systemem e-OBIEG) kierownik referatu lub właściwy pracownik przesyłał za pośrednictwem systemu pismo (poprzez pobranie pliku) do Burmistrza (jego zastępców, Sekretarza, Skarbnika) do akceptacji oraz w celu złożenia podpisu elektronicznego. Po podpisaniu elektronicznie, dokument wysyłano odbiorcy z użyciem systemu e-OBIEG za pośrednictwem ePUAP.<br>Zastosowany system e-OBIEG w Urzędzie współpracuję na zasadzie automatycznej integracji z platformą ePUAP, co wpływa na przyśpieszenie załatwiania spraw.<br>(Dowód: akta kontroli str. 242, 264, 266, 367, 387, 388 - 390, 381, 688 - 690) | |
| **Zakres, przyczyna i skutek stwierdzonej nieprawidłowości** | W wewnętrznych procedurach Urzędu dotyczących wykonywania czynności kancelaryjnych nie określono zasad obiegu dokumentów wpływających do Urzędu drogą elektroniczną oraz zasad wykorzystywania systemu informatycznego e-OBIEG do wspomagania procesu obiegu dokumentów, co powoduje naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI. Niewskazanie sposobu postępowania z dokumentami w postaci elektronicznej stanowi narażenie autentyczności, integralności oraz poufności informacji zawartych w sprawie, której dokument dotyczy. |
| *1.6 Formaty danych udostępniane przez systemy teleinformatyczne* | |
| **Podstawa prawna** | **§ 17 ust. 1 rozporządzenia KRI:** *Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą.*<br>**§ 18 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia.*<br>**§ 18 ust. 2 rozporządzenia KRI:** *Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia* |

| | |
|---|---|
| **Ustalenia kontroli**<br>W toku kontroli dokonano weryfikacji kodowania znaków, w odniesieniu do informacji wymienianych przez trzy systemy Urzędu [17] z innymi systemami zewnętrznymi[18], na drodze teletransmisji, która wykazała stosowanie standardu Unicode UTF-8.<br>(Dowód: akta kontroli str. 268, 305, 307, 325 – 326, 368)<br>Badane systemy informatyczne posiadały możliwość generowania zasobów informacyjnych oraz przyjmowanie elektronicznych dokumentów w formatach danych zawartych w załączniku nr 2 do rozporządzenia KRI tj. jpg, pdf, xls, doc, xml, docx.<br>(Dowód: akta kontroli str. 242, 268, 304, 326, 368, 383, 387)<br><br>**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.** | |
| **Ocena obszaru kontroli nr 1** | W toku badania obszaru za **uchybienia** uznano, w części:<br>**1.1 Usługi elektroniczne**<br>Na dzień przeprowadzenia czynności kontrolnych, na platformie e-BOI w wydzielonych funkcjonalnościach:<br>- „Wnioski elektroniczne i karty usług" w usłudze „Deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi" posiadającej elektroniczny formularz wniosku;<br>- „Elektroniczne formularze z ePUAP" wszystkie wykazane formularze,<br>nie posiadały możliwości realizacji sprawy przez ePUAP, co skutkuje brakiem spełnienia wymogu dotyczącego zakresu użytkowego posiadanego serwisu.<br>**1.3 Model usługowy**<br>W umowie zawartej na świadczenie usług informatycznych oraz w zakresie czynności Sekretarza, brak jest zapisu stanowiącego o obsłudze profilu Urzędu na platformie ePUAP.<br>W umowie zawartej na udostępnienia sytemu e-URZĄD nie podano czasu reakcji wykonania zgłoszenia o wystąpieniu awarii oraz nie określono maksymalnego czasu niedostępności systemu.<br>Brak ustalenia odpowiedzialności za utrzymanie usługi oraz określenia poziomu niedostępności usług skutkować może nie wykonaniem ich na zdeklarowanym poziomie.<br>Za **nieprawidłowość** w części **1.5 Obieg dokumentów** uznano:<br>W wewnętrznych procedurach Urzędu dotyczących wykonywania czynności kancelaryjnych nie określono zasad obiegu dokumentów wpływających do Urzędu drogą elektroniczną oraz zasad wykorzystywania systemu informatycznego e-OBIEG do wspomagania procesu obiegu dokumentów, co powoduje naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI. Niewskazanie sposobu postępowania z dokumentami w postaci elektronicznej stanowi narażenie autentyczności, integralności oraz poufności informacji zawartych w sprawie, której dokument dotyczy.<br><br>W związku z powyższym uzyskana ocena z badanego obszaru jest **Pozytywna z nieprawidłowościami.** |

[17] Ewidencja Ludności, PB_USC, e-OBIEG.

[18] ŹRÓDŁO oraz ePUAP.

| **Obszar kontroli Nr 2** | System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych. |
|---|---|
| | *2.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu* |
| **Podstawa prawna** | **§ 20 ust. 1 rozporządzenia KRI:** *Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.*<br>**§ 20 ust. 2 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji.*<br>**§ 20 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.* |
| **Ustalenia kontroli**<br>Zarządzeniem Nr 69/2015 z dnia 15 maja 2015 r. Burmistrz Miasta i Gminy Stepnicy wprowadził do stosowania w Urzędzie:<br>- Politykę Bezpieczeństwa Informacji[19];<br>- Politykę Przetwarzania Danych Osobowych, stanowiącą załącznik nr 1 do PBI[20];<br>- Instrukcję Zarządzania Systemami Informatycznymi[21], stanowiącą załącznik nr 2 do PBI.<br>Do zapoznania się oraz stosowania i przestrzegania powyższych dokumentów[22] zobowiązano wszystkich pracowników. Nadzór nad wykonaniem zarządzenia powierzono Sekretarzowi Gminy[23].<br>(Dowód: akta kontroli str. 47 – 90, 391 – 429)<br><br>Dodatkowo Urząd w dniu przeprowadzenia czynności kontrolnych, posiadał:<br>- przeprowadzoną Analizę Ryzyka wraz z szacowaniem ryzyka;<br>- dokumentację z przeprowadzonych przeglądów;<br>- dokumentację z incydentu naruszenia Bezpieczeństwa Informacji[24];<br>- dokumentację z przeprowadzonego audytu wewnętrznego;<br>- dokumentację z realizacji zaleceń poaudytowych.<br>Ww. dokumenty w dniu przeprowadzenia czynności kontrolnych tworzyły całościowy System Zarządzania Bezpieczeństwem Informacji[25].<br>(Dowód: akta kontroli str. 91-120, 228 – 229, 431 – 432; 121 – 227, 433 – 442) | |

[19] Zwaną dalej „PBI".
[20] Zwaną dalej „PPDO".
[21] Zwaną dalej „Instrukcją".
[22] § 2 Zarządzenia Nr 69/2015.
[23] § 3 Zarządzenia Nr 69/2015.
[24] Zwaną dalej „BI".
[25] Zwane dalej „SZBI".

Dokumentacja SZBI dotyczyła wszystkich danych przetwarzanych w Urzędzie, określała m.in. zasady bezpieczeństwa, zasady bezpiecznego korzystania z systemu informatycznego, zastosowane zabezpieczenia organizacyjne, fizyczne i logiczne w systemie informatycznym, procedury nadawania uprawnień do przetwarzania danych, stosowane metody i środki uwierzytelniania, opis procedur dotyczących tworzenia kopii zapasowych, zbiorów danych oraz programów, opis środków technicznych i organizacyjnych służących zapewnieniu poufności, integralności przetwarzania danych, opis zdarzeń naruszających ochronę danych (w tym osobowych) oraz opis postępowania w przypadku naruszenia zasad bezpieczeństwa informacji.
W badanym okresie przeprowadzono dwukrotnie przeglądu SZBI zgodnie z zapisami zawartymi w rozdziale VIII PBI, w efekcie których nie stwierdzono konieczności zmiany dokumentacji SZBI.
(Dowód: akta kontroli str. 228-229)

**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.**

*2.2 Analiza zagrożeń związanych z przetwarzaniem informacji*

| | |
|---|---|
| **Podstawa prawna** | **§ 20 ust. 2 pkt 3 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.* |

**Ustalenia kontroli**
W okresie objętym kontrolą została przeprowadzona jedna analiza ryzyka utraty integralności, poufności lub dostępności informacji, w której wyniku nie stwierdzono istotnego naruszenia atrybutów bezpieczeństwa informacji. Analiza ryzyka przeprowadzona została zgodnie z zapisami rozdziału X PBI, dla której przedstawiono plan naprawczy. W trakcie przeprowadzania czynności kontrolnych dokonano weryfikacji realizacji planu naprawczego, który jest systematycznie wdrażany.
(Dowód: akta kontroli str. 105, 614 - 615, 107, 444, 446, 448, 450, 452, 454, 456, 458, 461, 462, 464, 108, 79, 96,92, 640 – 641, 93, 600, 633, 91 – 114, 433 – 441)

Urząd zaplanował przeprowadzenie następnej analizy ryzyka po wykonaniu „Audytu Bezpieczeństwa Informacji", który odbędzie się pod koniec września 2016 r.
(Dowód: akta kontroli str. 442)

**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.**

*2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego*

| | |
|---|---|
| **Podstawa prawna** | **§ 20 ust. 2 pkt 2 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.* |

**Ustalenia kontroli**
W trakcie kontroli ustalono, że w okresie od dnia 20 stycznia do dnia 19 lutego 2015 r. w Urzędzie przeprowadzono „Analizę wykorzystania sprzętu, audytu zainstalowanego oprogramowania"[26].
Podczas przedmiotowej analizy weryfikacji poddano 30 urządzeń. W raporcie zamieszczono informację o zasobach sprzętowych poszczególnych jednostek komputerowych, które obejmowały m.in. model komputera, zainstalowany system operacyjny płytę główną, procesor, całkowitą

[26] Umowa Nr UM/A/MG/2014/11/03 z dnia 13.01.2015 r. na wykonanie audytu bezpieczeństwa informatycznego.

i dostępną pamięć, dyski twarde, napędy CD-ROM, monitory, karty graficzne i dźwiękowe, urządzenia sieciowe oraz zainstalowane drukarki. Kolejna inwentaryzacja w postaci audytu sprzętu i oprogramowania, zaplanowana została na koniec września 2016 r.

(Dowód: akta kontroli str. 495 – 497, 628 – 633)

Badaniem szczegółowym[27], w dniu przeprowadzenia kontroli objęto 20 stacji roboczych (urządzeń) oraz jeden serwer. Dane dotyczące badanych stacji roboczych zawierały m.in. informacje o jednostce Urzędu, w której znajduje się urządzenie, osobie, która obsługuje komputer (imię i nazwisko), adresie IP oraz zainstalowanych aplikacjach (firma, wersja i rodzaj aplikacji, data instalacji), systemie operacyjnym i oprogramowaniu. Dane dotyczące badanego serwera zawierały m.in. informacje o jednostce organizacyjnej Urzędu, której podlega serwer, nazwie, typie oraz zainstalowanych aplikacjach (data instalacji, firma, wersja i rodzaj), systemie operacyjnym.

(Dowód: akta kontroli str. 443 – 449)

**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.**

| | |
|---|---|
| | *2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych* |
| **Podstawa prawna** | **§ 20 ust. 2 pkt 4 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.*<br>**§ 20 ust. 2 pkt 5 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.* |
| **Ustalenia kontroli**<br>W trakcie kontroli dokonano przeglądu uprawnień do systemów i zasobów informatycznych dla 6 losowo wybranych pracowników Urzędu na podstawie, którego potwierdzono posiadanie adekwatnych uprawnień do realizacji zadań określonych w zakresie obowiązków.<br>(Dowód: akta kontroli str. 574,580 – 581, 562 – 563, 559 – 561, 556 – 558, 542, 539 – 541, 532, 526 – 528, 553 – 555)<br><br>Ponadto ustalono, że zasady nadawania, odbierania uprawnień oraz metody i środki uwierzytelniania i procedury związane z zarządzaniem i użytkowaniem systemów teleinformatycznych, były realizowane w Urzędzie w oparciu o regulacje wewnętrzne określone w rozdziale XI i XII PBI oraz rozdziale VII i VIII Instrukcji.<br>(Dowód: akta kontroli str. 82 – 83, 56 – 57)<br><br>Jednocześnie dokonano sprawdzenia ważności kont użytkowników do systemów informatycznych, których stosunek pracy wygasł w trakcie okresu objętego kontrolą i ustalono, że przydzielone konta zostały usunięte. (Dowód: akta kontroli str. 593, 571 – 574) | |
| **Zakres, przyczyny i skutki stwierdzonych uchybień** | W upoważnieniach imiennych do przetwarzania danych osobowych w części dot. zakresu nie wskazano systemu e-OBIEG, ponadto zwrócono uwagę na brak jednoznacznego doprecyzowania okresu obowiązywania upoważnienia – „data nadania/ustania upoważnienia". |

[27] Na podstawie wygenerowanego Raportu z Axence nVision.

| | |
|---|---|
| | Osoby zaangażowane w proces przetwarzania informacji posiadające stosowne uprawnienia i uczestniczące w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków muszą posiadać stosowne upoważnienia ze wskazaniem okresu ich obowiązywania oraz zawierać wskazanie każdego posiadanego systemu informatycznego, w którym przetwarzane są informacje, brak wskazania systemu oraz jednoznacznego wskazania okresu obowiązywania upoważnienia może skutkować brakiem zapewnienia odpowiedniego bezpieczeństwa informacji.<br>(Dowód: akta kontroli str. 588, 583, 525) |
| | *2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji* |
| **Podstawa prawna** | **§ 20 ust. 2 pkt 6 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.* |
| **Ustalenia kontroli**<br>W badanym okresie pracownicy Urzędu, zaangażowani w proces przetwarzania informacji, zostali przeszkoleni w przedmiotowej tematyce. Zakres szkolenia obejmował obszary dotyczące zagrożenia bezpieczeństwa informacji, odpowiedzialność prawną za naruszenie bezpieczeństwa informacji oraz stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.<br>(Dowód: akta kontroli str. 594 – 601)<br><br>**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.** | |
| | *2.6 Praca na odległość i mobilne przetwarzanie danych* |
| **Podstawa prawna** | **§ 20 ust. 2 pkt 8 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.* |
| **Ustalenia kontroli**<br>Na dzień kontroli zarządzanie bezpieczeństwem informacji w Urzędzie odbywało się zgodnie z zapisami rozdziału XV, XVIII PBI, za pomocą urządzenia FortiGate, poprzez funkcje tj. firewall'a, szyfrowania, zapobiegania włamaniom, ochrony antywirusowej i anstyspamowej, filtrowanie stron www oraz serwera VPN. Dokonano weryfikacji ustawień VPN na urządzeniu FortiGate i porównano z ustawieniami użytkownika końcowego wykonującego pracę na odległość, która wykazała poprawność wprowadzonych ustawień na obydwu urządzeniach. Dodatkowo w Urzędzie prowadzony jest rejestr urządzeń przenośnych typu USB uniemożliwiający użycia nie zarejestrowanego urządzenia w stacji roboczej Urzędu.<br>(Dowód: akta kontroli str. 53-54, 602 – 603, 606 – 612, 613 – 615)<br><br>**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.** | |

| 2.7 *Serwis sprzętu informatycznego i oprogramowania* | |
|---|---|
| **Podstawa prawna** | **§ 20 ust. 2 pkt 10 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.* |

**Ustalenia kontroli**

Badaniem w zakresie zawarcia zapisów, gwarantujących odpowiedni poziom bezpieczeństwa informacji objęto umowę dotyczącą udostępnienia systemu e-URZĄD, umowę na asystę techniczną, umowę serwisową oraz umowę na świadczenie usług informatycznych:

- nr 414/2014 z dnia 18.12.2014 r. zawartą z Wytwórnią Telewizyjno – Filmową „ALFA" Sp. z o.o. z siedzibą w Szczecinie, dotyczącą systemu e-URZĄD;
- nr 119/2015 z dnia 30.04.2015 r. zawartą z PHU ORDITEL Marcin Sokoliński z siedzibą w Stepnicy na świadczenie usług informatycznych;
- nr E160/2016 z dnia 05.01.2016 r. zawartą z Clanet z siedzibą w Nakle Śląskim dotyczącą serwisu technicznego, pogwarancyjnego systemów oprogramowań zainstalowanych w Referacie Ewidencji Ludności na Program Ewidencja Ludności;
- nr 2016-3204072-0462 z dnia 05.01.2016 r. zawartą z TECHNIKA IT S.A. z siedzibą w Gliwicach dotyczącą asysty technicznej oprogramowania PB_USC i EKSPORT_USC lub oprogramowania je zastępującego.

(Dowód: akta kontroli str. 274 – 276; 266 – 272; 316 – 318; 322 – 326)

1. W umowie dot. systemu e-URZĄD (nr 414/2014 z dnia 18.12.2014) w:
   - §7 ust. 3 zawarto zapis zobowiązujący wykonawcę do realizacji usługi zgodnie z wewnętrznymi zasadami bezpieczeństwa;
   - § 10 ust. 22 zobowiązano wykonawcę do stosowania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[28].
2. W umowie na świadczenie usług informatycznych (nr 119/2015 z dnia 30 kwietnia 2015 r.) w § 4 zawarto zapis zapewniający poufność wszystkich danych Urzędu, do których zleceniobiorca ma dostęp w wyniku realizacji przedmiotowej umowy oraz zapis gwarantujący poufność i zachowanie bezpieczeństwa w zakresie przetwarzania danych osobowych.
3. W umowie dot. asysty technicznej oprogramowania PB_USC oraz EKSPORT_USC (nr 2016-3204072-0462) w § 7 zawarto zapisy zobowiązujące wykonawcę do ochrony wszelkich zbiorów danych osobowych, a ich przetwarzanie zostało zastrzeżone w zakresie i celu związanym z realizacją umowy, które pozyskał w wyniku jej realizacji.

(Dowód: akta kontroli str. 267, 270; 275; 323 – 324)

| | |
|---|---|
| **Zakres, przyczyny i skutki stwierdzonych uchybień, nieprawidłowości** | W toku wykonywanych czynności kontrolnych zwrócono uwagę, że w umowie na asystę techniczną oprogramowania PB_USC oraz EKSPORT_USC (nr 2016-3204072-0462) uwzględniono jedynie zapewnienie bezpieczeństwa zbiorów danych osobowych, nie zawarto zaś dodatkowego zapisu zobowiązującego wykonawcę do ochrony wszelkich dodatkowych informacji, które pozyska w wyniku realizacji umowy, co nie zapewnia odpowiedniego poziomu bezpieczeństwa posiadanych informacji.<br>W umowie dot. serwisu technicznego programu Ewidencja Ludności (nr E160/2016 z dnia 05.01.2016 r.) nie zawarto zapisów mówiących |

[28] Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.

| | |
|---|---|
| | o zobowiązaniu zleceniobiorcy do zachowania tajemnicy informacji, do jakich może mieć dostęp w związku z realizowaniem umowy, co nie gwarantuje odpowiedniego poziomu bezpieczeństwa informacji i narusza § 20 ust. 2 pkt 10 rozporządzenia KRI.<br>(Dowód: akta kontroli str. 312 – 318, 323 – 324) |
| | *2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji* |
| **Podstawa prawna** | **§ 20 ust. 2 pkt 13 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określonym i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.* |
| **Ustalenia kontroli**<br>Sposób bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji został uregulowany w rozdziale XX PBI. Zgodnie z jego zapisami pracownik ma obowiązek niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji[29] lub Administratora Systemu Informatycznego[30], a w przypadku braku możliwości kontaktu z nimi bezpośredniego przełożonego. Z faktu naruszenia bezpieczeństwa informacji ABI dokonuje kwalifikacji zdarzenia, analizy incydentu, po czym sporządza raport z zaistniałej sytuacji oraz rejestruje w rejestrze incydentów. (Dowód: akta kontroli str. 49 – 51)<br><br>W badanym okresie w Urzędzie stwierdzono jeden przypadek naruszenia bezpieczeństwa informacji, który zakwalifikowany został, jako incydent. Sposób postępowania z incydentem był zgodny z zawartymi zapisami w PBI Urzędu. Nie stwierdzono konieczności zmiany dokumentacji stanowiącej SZBI. (Dowód: akta kontroli str. 229, 430 – 432)<br><br>**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.** | |
| | *2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji* |
| **Podstawa prawna** | **§ 20 ust. 2 pkt 14 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.* |
| **Ustalenia kontroli**<br>W 2015 r. w Urzędzie przeprowadzono audyt wewnętrzny z zakresu bezpieczeństwa informacji. W wyniku wykonanego Audytu przedstawione zostały rekomendacje, które są sukcesywnie wdrażane, zaś z działań naprawczych prowadzona jest ewidencja działań poaudytowych. Przeprowadzenie kolejnego audytu zaplanowane zostało na koniec września 2016 r.[31]<br>(Dowód: akta kontroli str.121 – 227, 433 – 442, 628 – 633)<br><br>**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.** | |

[29] Zwanego dalej „ABI".

[30] Zwanego dalej „ASI".

[31] Umowa Nr 221/2016 z dnia 6.09.2016 r. na wykonanie „Audytu Bezpieczeństwa Informacji".

| *2.10 Kopie zapasowe* | |
|---|---|
| **Podstawa prawna** | **§ 20 ust. 2 pkt 12 lit. b rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii.* |

**Ustalenia kontroli**

Procedurę tworzenia i przechowywania kopii zapasowych zawarto w rozdziale XI PBI, w którym określono zasady sporządzania i testowania kopii zapasowych. Urząd sporządzał zgodnie z przyjętą procedurą kopie danych w okresach dziennych, miesięcznych i rocznych. Wykonane kopie danych były testowane a nośnik, na którym zostały sporządzone znajdował się w serwerowni oraz środowisku wirtualnym. Pomieszczenie serwerowni zostało zabezpieczone systemem alarmowym oraz dodatkowo wprowadzono odpowiednie przepisy porządkowe[32].

Dodatkowo w umowie na system e-URZĄD w § 7 ust. 4 zawarto zapis zobowiązujący wykonawcę do wykonywania dodatkowych kopii zapasowych.

(Dowód: akta kontroli str. 80, 270, 673 – 679)

**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.**

| *2.11 Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych* | |
|---|---|
| **Podstawa prawna** | **§ 15 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.* |

**Ustalenia kontroli**

Kontroli poddano dwa systemy[33], które są eksploatowane w Urzędzie. Wskazane systemy spełniały poniższe wymagania:

- funkcjonalności – dostosowanie do zadań pełnionych przez pracowników Urzędu;
- używalności – posiadanie intuicyjnego interfejsu użytkownika;
- niezawodności – zdolność do wykonywania wymaganych funkcji;
- wydajności – wykonanie dedykowanych funkcji dla systemu w określonym czasie ich przetwarzania.

W rozdziale XIII Instrukcji uregulowano sposób wykonywania przeglądu i konserwacji systemów Urzędu przez ASI.

Na etapie eksploatacji systemów nie stwierdzono zapisów mówiących o monitorowaniu środowiska ich pracy pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom.

(Dowód: akta kontroli str. 79, 531 – 532, 581, 308, 304 – 306, 430)

W okresie objętym kontrolą nie zidentyfikowano systemów będących na etapie projektowania oraz wdrażania w związku, z czym nie wskazano, na potrzebę posiadania przez jednostkę procedury zamawiania oprogramowania, dokumentacji monitorowania systemów IT, dokumentacji działań zapobiegawczych będących wynikiem dostrzeżonych problemów podczas monitorowania.

**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.**

---

[32] § 41 ust. 5 i 6 Zarządzenia Nr 117/2015 Burmistrza Miasta i Gminy Stepnica z dnia 8 grudnia 2015 r. w sprawie wprowadzenia Regulaminu Pracy Urzędu Miasta i Gminy w Stepnicy, zwanego dalej „Regulaminem pracy Urzędu".

[33] e-URZĄD oraz Ewidencja Ludności.

| | |
|---|---|
| | *2.12 Zabezpieczenia techniczno – organizacyjne systemów informatycznych* |
| **Podstawa prawna** | **§ 20 ust. 2 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:*<br>**pkt 7:** *zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a)monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;*<br>**pkt 9:** *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;*<br>**pkt 11:** *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.* |
| **Ustalenia kontroli**<br>Zasady postępowania zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji oraz urządzeń mobilnych zawarto w rozdziale XVIII PBI.<br>Zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniem realizowane było poprzez wprowadzenie zabezpieczeń organizacyjnych zawartych w § 40 oraz § 41 Regulaminu Pracy Urzędu oraz funkcjonującego systemu alarmowego, pozwalającego na monitorowanie ruchu w Urzędzie.<br>(Dowód: akta kontroli str. 652 – 673, 52, 39)<br><br>Monitoring sieci oraz stacji roboczych Urzędu zapewniono poprzez oprogramowanie Axence nVision. Środkami uniemożliwiającymi nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji było zastosowanie następujących zabezpieczeń:<br>- filtracji URL;<br>- blokowanie prób nieupoważnionego dostępu;<br>- inspekcji ruchu sieciowego;<br>- inspekcji aplikacji indywidualnych użytkowników;<br>- gromadzenie logów o zaistniałych zdarzeniach;<br>- posiadanie oprogramowania antywirusowego;<br>- wdrożenie zaleceń z planu naprawczego po przeprowadzonej Analizie ryzyka.<br>(Dowód: akta kontroli str. 100, 105, 107, 106, 108, 109, 112, 113, 114, 641, 603 – 605, 644 – 651, 641, 631)<br><br>**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.** | |
| | *2.13 Zabezpieczenia techniczno – organizacyjne systemów informatycznych* |
| **Podstawa prawna** | **§ 20 ust. 2 pkt 12 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii; c) ochronie przed błędami, nieuprawnioną* |

| | |
|---|---|
| | *modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.*<br>**§ 20 ust. 4 rozporządzenia KRI:** *Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia* |
| **Ustalenia kontroli**<br>W celu zapewnienia odpowiedniego bezpieczeństwa informacji w Urzędzie wprowadzono zapisy w zakresie minimalizacji ryzyka utraty informacji w wyniku awarii, ochrony przed błędami, nieuprawnioną modyfikacją oraz niezwłocznego podejmowania działań po dostrzeżeniu podatności systemów, w rozdziałach X, XII, XIII, XIV Instrukcji, w rozdziałach IX, X, XVI, XVIII, XIX, XXII PBI, oraz w rozdziale V PPDO.<br>(Dowód: akta kontroli str. 78 – 80, 58, 51 – 53, 48 – 49, 395 – 398)<br><br>W takcie kontroli zwrócono uwagę, że w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych z jednoczesnym zminimalizowaniem ryzyka, w ramach dobrej praktyki stosownym jest posiadanie regulacji wewnętrznych warunkujących postępowanie z ryzykiem tj. *plan postępowania z ryzykiem.*<br>W przeprowadzonej Analizie ryzyka pod każdym z zagrożeń przedstawiony został plan naprawczy jednakże nie stanowił on *planu postępowania z ryzykiem.*<br>(Dowód: akta kontroli str. 91 – 120)<br><br>W toku kontroli dokonano przeglądu aktualizacji oprogramowań znajdujących się na 10 stacjach roboczych, nie stwierdzono nieprawidłowości w tym zakresie.<br>(Dowód: akta kontroli str. 467 – 482)<br><br>Ustalono, że bezpieczeństwo plików systemowych realizowane jest przez:<br>• tworzenie kopii zapasowych serwerów, systemów informatycznych, programów dedykowanych;<br>• ograniczenie dostępu do Internetu, wykorzystując mechanizmy ochrony tj. firewall, serwer;<br>• wydzielenie w systemach informatycznych konta administratora od konta użytkownika;<br>opisanych w punkcie 2.12 wystąpienia pokontrolnego.<br><br>**Nieprawidłowości/uchybień nie stwierdzono, związku z powyższym badaną część obszaru oceniono pozytywnie.** | |
| *2.14 Rozliczalność działań w systemach teleinformatycznych.* | |
| **Podstawa prawna** | **§ 21 ust. 2 rozporządzenia KRI:** *W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.* |

| | |
|---|---|
| | **§ 21 ust. 3 rozporządzenia KRI:** *w zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka.*<br>**§ 21 ust. 4 rozporządzenia KRI:** *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.* |
| **Ustalenia kontroli**<br>W trakcie kontroli stwierdzono, że dostęp do przetwarzania informacji w systemach teleinformatycznych w Urzędzie posiadają uprawnione osoby. W dziennikach systemów informatycznych można dokonać weryfikacji kto, kiedy i jakie czynności wykonywał.<br>(Dowód: akta kontroli str. 37, 56 – 57, 80 – 84, 305, 474 – 475, 309, 500, 510, 543, 533, 537, 551) | |
| **Zakres i skutki stwierdzonych uchybień** | W toku przeprowadzenia czynności kontrolnych nie stwierdzono przepisów wewnętrznych regulujących przechowywanie zapisów z dzienników systemów teleinformatycznych. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji wykonywanych czynności w danych systemach informatycznych, brak zapisów stanowiących powyższe może zaburzyć proces rozliczalności a w efekcie bezpieczeństwo posiadanych informacji w Urzędzie. |
| **Ocena obszaru kontroli nr 2** | W toku badania obszaru za **uchybienia** uznano, w części:<br>**2.4 Zarządzenie uprawnieniami do pracy w systemach informatycznych**<br>W upoważnieniach imiennych do przetwarzania danych osobowych w części dot. zakresu nie wskazano systemu e-OBIEG, ponadto zwrócono uwagę na brak jednoznacznego doprecyzowania okresu obowiązywania upoważnienia – „data nadania/ustania upoważnienia". Osoby zaangażowane w proces przetwarzania informacji posiadające stosowne uprawnienia i uczestniczące w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków muszą posiadać stosowne upoważnienia ze wskazaniem okresu ich obowiązywania oraz zawierać wskazanie każdego posiadanego systemu informatycznego, w którym przetwarzane są informacje, brak wskazania systemu oraz jednoznacznego wskazania okresu obowiązywania upoważnienia może skutkować brakiem zapewnienia odpowiedniego bezpieczeństwa informacji.<br>**2.7 Serwis sprzętu informatycznego i oprogramowania**<br>W toku wykonywanych czynności kontrolnych zwrócono uwagę, że w umowie na asystę techniczną oprogramowania PB_USC oraz EKSPORT_USC (nr 2016-3204072-0462) uwzględniono jedynie zapewnienie bezpieczeństwa zbiorów danych osobowych, nie zawarto zaś dodatkowego zapisu zobowiązującego wykonawcę do ochrony wszelkich dodatkowych informacji, które pozyska w wyniku realizacji umowy, co nie zapewnia odpowiedniego poziomu bezpieczeństwa posiadanych informacji. |

| | |
|---|---|
| | **2.14 Rozliczalność działań w systemach teleinformatycznych**<br>W toku przeprowadzenia czynności kontrolnych nie stwierdzono przepisów wewnętrznych regulujących przechowywanie zapisów z dzienników systemów teleinformatycznych. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji wykonywanych czynności w danych systemach informatycznych, brak zapisów stanowiących powyższe może zaburzyć proces rozliczalności a w efekcie bezpieczeństwo posiadanych informacji w Urzędzie.<br>Za **nieprawidłowość** w części **2.7 Serwis sprzętu informatycznego i oprogramowania** uznano:<br>W umowie dot. serwisu technicznego programu Ewidencja Ludności (nr E160/2016 z dnia 05.01.2016 r.) nie zawarto zapisów mówiących o zobowiązaniu zleceniobiorcy do zachowania tajemnicy informacji, do jakich może mieć dostęp w związku z realizowaniem umowy, co nie gwarantuje odpowiedniego poziomu bezpieczeństwa informacji i narusza § 20 ust. 2 pkt 10 rozporządzenia KRI.<br><br>W związku z powyższym uzyskana ocena z badanego obszaru jest **Pozytywna z nieprawidłowościami.** |
| **Obszar kontroli Nr 3** | Zapewnienie dostępności informacji zawartej na stronie internetowej urzędu dla osób niepełnosprawnych. |
| **Podstawa prawna** | **§ 19 rozporządzenia KRI:** *W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.* |
| **Ustalenia kontroli**<br>W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu oraz BIP Urzędu ze standardem WCAG 2.0 poprzez wykorzystanie narzędzia dostępnego na stronie internetowej http://achecker.ca/checker/index.php, który nie wykazał istotnych niezgodności ze standardem WCAG 2.0. w zakresie zasady 4 – Kompatybilności z uwzględnieniem poziomu AA. Walidator podał informację o wystąpieniu 55 błędów i 492 ostrzeżeniach na stronie BIP Urzędu oraz 1 błędzie i 645 ostrzeżeniach na stronie BIP Urzędu. Wskazane błędy nie miały istotnego wpływu na prezentowane treści dla osób niepełnosprawnych.<br>(Dowód: akta kontroli str. 680 – 686)<br><br>Na stronie BIP Urzędu (prawy górny róg) zamieszczono ikonę pozwalającą na przedstawienie strony z dostosowaniem dla osób niepełnosprawnych. Dostosowanie zostało wykonane z możliwością wyboru czterech różnych kontrastów oraz trzech rozmiarów trzcionki.<br>(Dowód: akta kontroli str. 5, 24, 687 ) | |
| **Zakres, przyczyny i skutki stwierdzonych uchybień** | Strona internetowa Urzędu, pomimo spełnienia wymogów w zakresie 4 – Kompatybliności i poziomu AA, nie posiadała możliwości wyświetlania treści w wersji dla osób niepełnosprawych. Dobrą praktyką jest zastosowanie funkcjonalności umożliwiającej wyświetlanie treści strony internetowej Urzędu dla osób niepełnosprawnych.<br>(Dowód: akta kontroli str. 5) |
| **Ocena obszaru kontroli** | **Ocena pozytywna z uchybieniami** |

| Wpis do książki kontroli | Pozycja Nr 21/2016 |
|---|---|

**Podsumowanie**

Ustalenia kontroli wykazały następujące uchybienia/nieprawidłowości przy realizacji zadań określonych w rozporządzeniu KRI, w obszarach:

1. **Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.**

***1.1. Usługi elektroniczne***

Na dzień przeprowadzenia czynności kontrolnych, na platformie e-BOI w wydzielonych funkcjonalnościach:

- „Wnioski elektroniczne i karty usług" w usłudze „Deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi" posiadającej elektroniczny formularz wniosku;
- „Elektroniczne formularze z ePUAP" wszystkie wykazane formularze,

nie posiadały możliwości realizacji sprawy przez ePUAP, co skutkuje brakiem spełnienia wymogu dotyczącego zakresu użytkowego posiadanego serwisu.

***1.3. Model usługowy***

W umowie zawartej na świadczenie usług informatycznych oraz w zakresie czynności Sekretarza, brak jest zapisu stanowiącego o obsłudze profilu Urzędu na platformie ePUAP.

W umowie zawartej na udostępnienia sytemu e-URZĄD nie podano czasu reakcji wykonania zgłoszenia o wystąpieniu awarii oraz nie określono maksymalnego czasu niedostępności systemu.

Brak ustalenia odpowiedzialności za utrzymanie usługi oraz określenia poziomu niedostępności usług skutkować może nie wykonaniem ich na zdeklarowanym poziomie.

***1.5. Obieg dokumentów***

W wewnętrznych procedurach Urzędu dotyczących wykonywania czynności kancelaryjnych nie określono zasad obiegu dokumentów wpływających do Urzędu drogą elektroniczną oraz zasad wykorzystywania systemu informatycznego e-OBIEG do wspomagania procesu obiegu dokumentów, co powodowało naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI. Niewskazanie sposobu postępowania z dokumentami w postaci elektronicznej stanowi narażenie autentyczności, integralności oraz poufności informacji zawartych w sprawie, której dokument dotyczy.

2. **System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.**

***2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych***

W upoważnieniach imiennych do przetwarzania danych osobowych w części dot. zakresu nie wskazano systemu e-OBIEG, ponadto zwrócono uwagę na brak jednoznacznego doprecyzowania okresu obowiązywania upoważnienia – „data nadania/ustania upoważnienia".

Osoby zaangażowane w proces przetwarzania informacji posiadające stosowne uprawnienia i uczestniczące w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków muszą posiadać stosowne upoważnienia ze wskazaniem okresu ich obowiązywania oraz zawierać wskazanie każdego posiadanego systemu informatycznego, w którym przetwarzane są informacje, brak wskazania systemu oraz jednoznacznego wskazania okresu obowiązywania upoważnienia może skutkować brakiem zapewnienia odpowiedniego bezpieczeństwa informacji.

***2.7. Serwis sprzętu informatycznego i oprogramowania***

W toku wykonywanych czynności kontrolnych zwrócono uwagę, że w umowie na asystę techniczną oprogramowania PB_USC oraz EKSPORT_USC (nr 2016-3204072-0462) uwzględniono jedynie zapewnienie bezpieczeństwa zbiorów danych osobowych, nie zawarto

zaś dodatkowego zapisu zobowiązującego wykonawcę do ochrony wszelkich dodatkowych informacji, które pozyska w wyniku realizacji umowy, co nie zapewnia odpowiedniego poziomu bezpieczeństwa posiadanych informacji.

W umowie dot. serwisu technicznego programu Ewidencja Ludności (nr E160/2016 z dnia 05.01.2016 r.) nie zawarto zapisów mówiących o zobowiązaniu zleceniobiorcy do zachowania tajemnicy informacji, do jakich może mieć dostęp w związku z realizowaniem umowy, co nie gwarantuje odpowiedniego poziomu bezpieczeństwa informacji i narusza § 20 ust. 2 pkt 10 rozporządzenia KRI.

***2.14. Roliczalność działań w systemach teleinformatycznych***

W toku przeprowadzenia czynności kontrolnych nie stwierdzono przepisów wewnętrznych regulujących przechowywanie zapisów z dzienników systemów teleinformatycznych. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji wykonywanych czynności w danych systemach informatycznych, brak zapisów stanowiących powyższe może zaburzyć proces rozliczalności a w efekcie bezpieczeństwo posiadanych informacji w Urzędzie.

**3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych.**

Strona internetowa Urzędu, pomimo spełnienia wymogów w zakresie 4 – Kompatybliności i poziomu AA, nie posiadała możliwości wyświetlania treści w wersji dla osób niepełnosprawych. Dobrą praktyką jest zastosowanie funkcjonalności umożliwiającej wyświetlanie treści strony internetowej Urzędu dla osób niepełnosprawnych.

**ZALECENIA**

Przedstawiając powyższe oceny wynikające z ustaleń kontroli zaleca się:

1. Udostępnić na Elektronicznej Platformie Usług Administracji Publicznej (ePUAP) formularze zgodnie z zawartym opisem w Elektronicznym Biurze Obsługi Interesanta (e-BOI).
2. Zawrzeć w umowie na świadczenie usług informatycznych oraz w zakresie czynności Sekretarza zapis stanowiący o obsłudze profilu Urzędu na platformie ePUAP.
3. Określić w umowie na udostępnianie systemu e-URZĄD czas reakcji wykonania zgłoszenia o wystąpieniu awarii oraz maksymalny czas niedostępności systemu.
4. Opracować i wdrożyć regulacje wewnętrzne określające zasady obiegu dokumentów wpływających do Urzędu drogą elektroniczną oraz zasady wykorzystania systemu informatycznego e-OBIEG w celu spełnienia wymogów zawartych w § 20 ust. 2 pkt 9 rozporządzenia KRI.
5. Zamieścić w upoważnieniach imiennych do przetwarzania danych osobowych zapis dotyczący obsługi systemu e-OBIEG oraz doprecyzować okres obowiązywania ww. upoważnień.
6. Uwzględnić w umowie na asystę techniczną oprogramowania PB_USC oraz EKSPORT_USC zapis gwarantujący odpowiedni poziom bezpieczeństwa informacji w postaci zobowiązania wykonawcy do ochrony wszelkich dodatkowych informacji, które pozyska w wyniku realizacji umowy.
7. Uwzględnić w umowie dot. serwisu technicznego programu Ewidencja Ludności zapisy mówiące o zobowiązaniu zleceniobiorcy o zachowaniu tajemnicy informacji, do jakich może mieć dostęp w związku z realizowaniem umowy zgodnie z wymogami wskazanymi w § 20 ust. 2 pkt 10 rozporządzenia KRI.
8. Opracować i wdrożyć regulację wewnętrzną zawierającą zasady prowadzenia i wykorzystywania dzienników systemowych (logów).
9. Dostosować stronę internetową Urzędu do możliwości wyświetlania treści w wersji dla osób niepełnosprawnych.

| POUCZENIE |
| --- |
| - od wystąpienia pokontrolnego nie przysługują środki odwoławcze;<br>- o podjętych działaniach, mających na celu wyeliminowanie stwierdzonych nieprawidłowości, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie w terminie miesiąca od daty otrzymania niniejszego wystąpienia. |
| **PODPIS KIEROWNIKA JEDNOSTKI KONTROLUJĄCEJ** |
| wz. WOJEWODY ZACHODNIOPOMORSKIEGO<br>*Marek Subocz*<br>WICEWOJEWODA |