WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 27 lipca 2022 r

Wydział Finansów i Kontroli
FK-IV.431.8.2022

Szanowny Pan
Witold Wróblewski
Prezydent Miasta Elbląg
Urząd Miejski w Elblągu
ul. Łączności 1, 82-300 Elbląg

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Miejskim w Elblągu[1], ul. łączności 1, 82-300 Elbląg, NIP jednostki 5780007338, REGON jednostki: 000595111.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Witold Wróblewski** – Prezydent Miasta Elbląg, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 4 listopada 2018 r.

W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą w Urzędzie był Pan **Jacek Boruszka** - Dyrektor Departamentu Innowacji i Informatyki, zatrudniony na podstawie umowy o pracę od dnia 1 marca 2011 r.

Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania była Pan **Michał Missan** - Wiceprezydent Miasta Elbląg zatrudniony na podstawie umowy o pracę od dnia 28 lutego 2020 r.

[akta kontroli str. 66]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – starszy inspektor wojewódzki; przewodniczący zespołu kontrolnego, legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.358.2022 z 16 maja 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – starszy inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu

[1] Zwanym dalej: Urzędem

Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.359.2022 z 16 maja 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 17-22]

Kontrolę przeprowadzono w dniach 6 – 27 czerwca 2022 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją 33 / 2022.

[akta kontroli str. 67]

Kontrola prowadzona była w trybie hybrydowym, tj. w dniu 6 czerwca – rozpoczęcie czynności kontrolnych w Urzędzie Miejskim w Elblągu oraz oględziny serwerowni na miejscu w jednostce. Pozostałe dni (7-27 czerwca br.) kontrola prowadzona była zdalnie, bez osobistej obecności kontrolerów w Urzędzie, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. W dniu rozpoczęcia czynności kontrolnych okazano legitymacje oraz upoważnienia do kontroli, poinformowano o zasadach kontroli w trybie hybrydowym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania.

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 2070). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2021 r.

[akta kontroli str. 1-2, 49-60]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2022 r., poz. 135), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 2070)[2], rozdziału III i IV 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 (Dz.U. z 2017 r. poz. 2247 ze zm.)[3], jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 49-60]

Prezydent Elbląga upoważnił Dyrektora Departamentu Innowacji i Informatyki, do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 68]

---

[2] Zwanej dalej: ustawą

[3] Zwanego dalej: rozporządzeniem KRI

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się pozytywnie z uchybieniami.

Ocena działalności jednostki kontrolowanej wynika z ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

Z informacji przekazanych przez Urząd przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywanych jest 9 niżej wymienionych systemów teleinformatycznych.

Systemy teleinformatyczne wykorzystywane w Urzędzie:

1) **OTAGO SWR Asseco Data Systems** – moduł w zakresie świadczeń rodzinnych, zasiłków opiekuńczych, zaliczek alimentacyjnych, jednorazowych świadczeń z tytułu urodzenia dziecka,
2) **OTAGO OFA Asseco Data Systems** – moduł w zakresie świadczeń z funduszu alimentacyjnego, postępowań wobec dłużników alimentacyjnych,
3) **OTAGO RODZINA+ Asseco Data Systems** - moduł w zakresie świadczeń wychowawczych, świadczeń Dobry start,
4) **OTAGO SWR Asseco Data Systems** (Dodatek osłonowy),
5) **OTAGO SWR Asseco Data Systems** - moduł czyste powietrze – wydawanie zaświadczeń o wysokości przeciętnego miesięcznego dochodu,
6) **OTAGO ELUD Asseco Data Systems** – moduł w zakresie prowadzenia rejestru mieszkańców,
7) **Źródło** (system rejestrów państwowych PESEL) – gromadzenie danych w zakresie pobytu obywateli RP oraz cudzoziemców przebywających na terenie RP,
8) **RDO** system rejestrów państwowych, Rejestr Dowodów Osobistych – obsługa wniosków o wydanie dowodów osobistych,
9) **BUSC** system rejestrów państwowych, Baza Usług Stanu Cywilnego – gromadzenie danych w zakresie zmiany stanu cywilnego obywateli RP i cudzoziemców.

[akta kontroli str. 36-40]

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

1.1. Usługi elektroniczne

Z art. 16 ust. 1a ustawy wynika, że podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.
Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez:

a) 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;

b) publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

Urząd posiada aktywną Elektroniczną Skrzynkę Podawczą **/974x3yyiku/SkrytkaESP**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Ścieżkę bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu w zakładce Elektroniczna skrzynka podawcza. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Na stronie głównej BIP Urzędu - w nagłówku strony (Urząd on-line) oraz w zakładce „Załatwianie spraw" – podzakładka „Urząd on-line" zawarto listę formularzy niezbędnych do załatwienia wybranych spraw, tj.:
1. Zgłaszanie uszkodzeń w nawierzchni dróg i chodników.
2. Udzielanie bonifikaty od opłaty rocznej z tytułu użytkowania wieczystego nieruchomości gruntowej Gminy Miasto Elbląg przeznaczonej lub wykorzystywanej na cele mieszkaniowe.
3. Zaświadczenie o cenie sprzedaży lokalu.
4. Wydzierżawienie nieruchomości lub przedłużenie umowy dzierżawy.
5. Zamiana lokalu mieszkalnego.
6. Wniosek o wydanie zaświadczenia podatkowego.
7. Wniosek o udzielenie pomocy de minimis.
8. Wniosek o wydanie zezwolenia na utrzymywanie psa rasy uznawanej za agresywną.
9. Wniosek o zezwolenie na przeprowadzenie imprezy masowej.

Kliknięcie wybranego odnośnika przenosi bezpośrednio na stronę ePUAP.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że na stronie BIP w zakładce „Załatwianie spraw" – podzakładka „Karty usług, wnioski", opublikowane są poszczególne karty usług opisujące przyjętą procedurę obowiązującą podczas załatwiania danej sprawy oraz wzory wniosków i formularzy, będących w zakresie działania poszczególnych departamentów w Urzędzie.

Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą badanych systemów teleinformatycznych.
Ponadto Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego". Usługa te umożliwiają złożenie do wybranego organu administracji publicznej pisma w sprawie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 69-73]

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

Stosownie do art. 19b 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 kwalifikowanym podpisem elektronicznym.

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory dokumentów, jakie zostały już opracowane i są używane. W przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.

W trakcie kontroli ustalono, że w okresie objętym kontrolą (2021) Urząd nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt nie uruchomienia nowej usług dla których nie ma wzorów dokumentów w CRWDE. Z informacji uzyskanej podczas kontroli wynika ponadto, że: Urząd Miasta Elbląg nie korzystał, ani nie publikował wzorów w CRWDE, udostępnia natomiast wzory dokumentów elektronicznych.

Jednocześnie należy zaznaczyć, że na stronie BIP w zakładce „Załatwianie spraw" – podzakładka „Karty usług, wnioski", opublikowane są poszczególne karty usług opisujące przyjętą procedurę obowiązującą podczas załatwiania danej sprawy oraz wzory wniosków i formularzy, będących w zakresie działania poszczególnych departamentów w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 25-35]

1.3. Model usługowy

– Z § 15 ust. 2 rozporządzenia KRI wynika, że zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

Strona internetowa Urzędu działa pod adresem https://www.elblag.eu/, a strona internetowa BIP Urzędu – pod adresem http://um-elblag.samorzady.pl/
Na portalu internetowym Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w lewej górnej części panelu strony. Zarówno na stronie głównej BIP Urzędu jak i na portalu internetowym Urzędu zawarto odnośniki do ESP oraz do zakładki e-Urząd gdzie część spraw można załatwić on-line, za pomocą formularzy ePUAP.

[akta kontroli str. 74-75]

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych realizowanych przez systemy teleinformatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej ze względu na fakt, że jednostka nie świadczyła usług elektronicznych na zewnątrz za pomocą tych systemów. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

- § 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;
- § 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.

Wiele rejestrów w urzędach administracji publicznej przechowuje i przetwarza identyczne informacje, np. o obywatelu/podmiocie, takie jak PESEL, REGON, NIP, dane adresowe itp. Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu będzie sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego postulatu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „Kontrolowane systemy teleinformatyczne współpracują z publicznymi systemami teleinformatycznymi, są to m.in. Źródło, CBB, CZIS, CEIDG, KRS, Epodatki, Pesel, EKSMOoN, NFZ, KRUS, ZUS.JB. Współpraca systemów teleinformatycznych użytkowanych w Urzędzie odbywa się na zasadzie korzystania z rejestrów referencyjnych systemów publicznych, a w niewielkim zakresie na wymianie danych. Komunikacja przebiega protokołem TCP/IP poprzez urządzenia umożliwiające komunikację między sieciami Urzędu Miejskiego – Systemem Rejestrów Państwowych. Pomiędzy nimi znajduje się mechanizm pobierania i wysyłania danych zabezpieczony certyfikatem wystawianym przez systemy publiczne udostępniające dane. Certyfikaty odnawiane są co dwa lata. Serwery zabezpieczone są systemem antywirusowym. Komunikacja zabezpieczona jest poprzez system Codziennie tworzone są kopie baz danych."

[akta kontroli str. 406-408]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.5. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności 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.

Zasady obsługi klientów oraz obiegu korespondencji w Urzędzie Miejskim w Elblągu określone zostały Zarządzeniem Nr 34/2018 Prezydenta Miasta Elbląg z dnia 31 stycznia 2018 r. Zgodnie z powyższym zarządzeniem sprawy wpływające do Urzędu załatwiane są w formie pisemnej (papierowej) oraz w formie dokumentu elektronicznego w rozumieniu przepisów ustawy. W Urzędzie funkcjonują: EOD – Elektroniczny System Obiegu Dokumentów oraz ERP – Elektroniczny Rejestr Przesyłek. Opracowano podstawowe zasady elektronicznego obiegu dokumentów, obejmujące swym zakresem również dokumentację wpływającą do Urzędu poprzez skrzynkę ESP - ePUAP oraz pocztę elektroniczną. Opracowanie procedur dotyczących wykonywania czynności kancelaryjnych, w których określone są szczegółowe zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP oraz poczta elektroniczna), zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Opracowanie zasad postępowania z dokumentacją elektroniczną (wnioski elektroniczne, e-maile) oraz wymagań organizacyjno-technicznych dotyczących zarządzania tą dokumentacją pozwala właściwie dbać o jej bezpieczeństwo.

[akta kontroli str. 76-82]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 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;
- § 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;
- § 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.

Istotą współdzielenia informacji w urzędach jest stworzenie możliwości wymiany danych pomiędzy różnymi systemami informatycznymi oraz umożliwienie odbiorcom swobodnego dostępu do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików.

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „Możliwość wymiany danych została zapewniona przez producenta oprogramowania kontrolowanego zgodnie z wytycznymi

komunikacji opisanymi w poszczególnych zewnętrznych systemach teleinformatycznych. Wymiana danych odbywa się poprzez zabezpieczoną sieć informatyczną systemem antywirusowym oraz firewallem. Komunikacja odbywa się poprzez sieć teleinformatyczną za pomocą protokołu TCP/IP i zabezpieczona jest certyfikatem systemu publicznego. Dane z systemów są udostępniane w powszechnie dostępnych formatach plików, które są zawarte w zał. nr 2 do KRI. Dane są udostępniane w formacie XML oraz umożliwiają generowanie danych w formacie .rtf, .txt, .pdf oraz .xls. W przypadku wymiany informacji pomiędzy systemami kontrolującego, a zewnętrznymi systemami używany jest standard kodowania Unicode UTF-8. Systemy teleinformatyczne kontrolowanego umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw w formatach określonych w złącznikach 2 i 3 do rozporządzenia KRI. Są to m.in. .rtf, .txt, .pdf, .doc, .xls. Firma dostarczająca do Urzędu Miejskiego oprogramowanie wykorzystywane do współpracy z publicznymi systemami posiada świadectwo zgodności oprogramowania wydane przez odpowiednie ministerstwo co zapewnia kontrolowanego o zgodności oprogramowania z powszechnie obowiązującymi przepisami."

[akta kontroli str. 406-408]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 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;
- § 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;
- § 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.

Realizacja zadań w zakresie ochrony danych wymaga od podmiotu publicznego opracowania dokumentacji SZBI (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja Systemu Zarzadzania Bezpieczeństwem Informacji (SZBI) jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie. Podstawowym dokumentem SZBI jest Polityka Bezpieczeństwa Informacji. Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji.

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, 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) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO", w celu zapewnienia bezpiecznego przetwarzania informacji w Urzędzie Miejskim w Elblągu opracowano podstawową dokumentację wchodzącą w skład SZBI, obowiązującą w okresie objętym kontrolą, tj.:

- przyjętą Zarządzeniem Nr 320/2019 Prezydenta Miasta Elbląg z dnia 10 lipca 2019 r. Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Elblągu, obowiązującą do dnia 6 maja 2021 r. włącznie.
- przyjętą Zarządzeniem Nr 160/2021 Prezydenta Miasta Elbląg z dnia 7 maja 2021 r. Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Elblągu, w skład której weszła Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych i informacji w Urzędzie Miejskim w Elblągu.

[akta kontroli str. 83-174, 409-501]

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO". Dokumentacja w zakresie bezpieczeństwa informacji dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności oraz integralności ich przetwarzania, jak również monitorowania zdarzeń naruszających ochronę informacji (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa przetwarzanych danych. Przyjęta dokumentacja wchodziła w skład System Zarządzania Bezpieczeństwem Informacji, wymaganego zgodnie z § 20 ust. 1 rozporządzenia KRI, i zapewniała poufność, dostępność i integralność przetwarzanych informacji.

W myśl § 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.
Rola podmiotu nie kończy się tylko i wyłącznie na opracowaniu i wdrożeniu do eksploatacji systemu zarządzania bezpieczeństwem informacji. Obowiązkiem podmiotu jest także monitorować, przeglądać i utrzymywać jak również doskonalić ten system tak, aby zapewniać poufność, dostępność i integralność informacji. Powyższe oznacza, że realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi.
Z dokumentacji przedstawionej kontrolującym wynika, że w celu realizacji monitoringu i doskonalenia SZBI w Urzędzie, powołany został Zespół ds. nadzoru nad Polityką Bezpieczeństwa Informacji. W okresie objętym kontrolą odbyło się jedno spotkania Zespołu. Dotyczyło ono omówienia zagadnień w zakresie bezpieczeństwa informacji w jednostce za rok 2020, gdyż w związku z sytuacją epidemiologiczną w 2020 r. nie odbyło się spotkanie stacjonarne Zespołu.
Kolejne spotkanie Zespołu dotyczyło okresu objętego kontrolą - 2021 roku i odbyło się 24 lutego 2022 r. Podczas spotkania Inspektor Ochrony Danych poruszył następujące zagadnienia:

- Podsumowanie pracy Zespołu ds. Nadzoru nad Polityką Bezpieczeństwa Informacji za rok 2021.
- Omówienie zaleceń audytu bezpieczeństwa informacji z 2021 r.
- Omówienie zadań zrealizowanych przez Inspektora Ochrony Danych.

– Omówienie proponowanych zmian do Polityki Bezpieczeństwa Informacji.

[akta kontroli str. 183-228]

Z informacji uzyskanych z Urzędu w przedmiotowej sprawie wynika, że, cyt.: „(...) Zgodnie z § 14 Polityki Bezpieczeństwa Informacji Inspektor Ochrony Danych przygotowuje plan sprawdzeń systemu ochrony danych osobowych i informacji w cyklu rocznym – załącznik nr 20. W trakcie sprawdzeń wykorzystywana jest lista kontrolna – załącznik nr 21. Załącznik nr 21a dotyczy sprawdzenia, które przeprowadzane byłoby w komórce IT (w 2021 r. takiego sprawdzenia nie było). Po dokonaniu sprawdzenia IOD przekazuje sprawozdanie ze sprawdzenia planowego Administratorowi Danych Osobowych – załącznik nr 22. Zgodnie z zapisem w § 14 pkt. 10 PBI do dnia 30 marca każdego roku, na podstawie zgromadzonych materiałów o których mowa w § 14 ust. 2 Inspektor Ochrony Danych sporządza za poprzedni rok Sprawozdanie roczne (o zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i informacji) i przedstawia je Administratorowi Danych Osobowych w sposób uniemożliwiający zapoznanie się z jego treścią innym osobom, którego wzór stanowi Załącznik nr 23 do PBI. Kontrola w zakresie systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej nie obejmuje sprawdzenia realizacji zadań wykonywanych przez Inspektora Ochrony Danych."

Z dokumentacji przedstawionej kontrolującym wynika, że w okresie objętym kontrolą dokonywano sprawdzeń w ramach przeglądu SZBI w jednostce zgodnie z § 20 ust. 1 rozporządzenia KRI.

[akta kontroli str. 406-408, 502-532]

Prezydent Elbląga, Zarządzeniem Nr 111\2020 z dnia 17 marca 2020 r. zmieniającym zarządzenie w sprawie realizacji zadań wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/ WE (ogólnego rozporządzenia o ochronie danych) wyznaczył w Urzędzie Inspektora Ochrony Danych oraz jego zastępcę. W jednostce powołano również Administratora Sieci Teleinformatycznej.

[akta kontroli str. 175-177]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Z § 20 ust. 2 pkt 3 rozporządzenia KRI wynika, że 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.

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu. Analiza ryzyka jest ważnym wymaganiem

nałożonym na administratorów i podmioty przetwarzające. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie bezpieczeństwem informacji, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowo przebiegająca analiza ryzyka nie jest jednorazowym działaniem, lecz regularnie i ciągle monitorowanym procesem.

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko.

Z informacji uzyskanych z Urzędu w przedmiotowej sprawie wynika, że, cyt.: „(...) monitorowanie ryzyka przy przetwarzaniu danych osobowych i informacji realizowane jest poprzez aktualizację rejestrów szacowania ryzyka (...)."
Zgodnie z §10 pkt 6-8 załącznika Nr 3 do PBI – Procedura szacowania ryzyka przy przetwarzaniu danych osobowych i informacji, Dyrektorzy komórek organizacyjnych Urzędu, pracownicy na Samodzielnych stanowiskach oraz Pełnomocnicy, do 30 marca każdego roku dokonują przeglądu ryzyka za cały rok (...). Po dokonaniu przeglądu Dyrektorzy komórek organizacyjnych Urzędu, pracownicy na Samodzielnych stanowiskach oraz Pełnomocnicy dokonują aktualizacji rejestru szacowania ryzyka ochrony danych osobowych i informacji, następnie przekazują go do Zespołu ds. Nadzoru nad Polityką Bezpieczeństwa Informacji do dnia 30 czerwca każdego roku. Na podstawie przekazanych rejestrów szacowania ryzyka ochrony danych osobowych i informacji Zespół dokonuje aktualizacji Zbiorczego rejestru szacowania ryzyka ochrony danych osobowych
i informacji.

Kontrolującym przedstawiono dokumentację (stanowiącą akta kontroli) świadczącą o przeprowadzeniu analizy ryzyka utraty integralności, dostępności lub poufności informacji w 2021 roku.

[akta kontroli str. 406-408, 555-561]

W toku prowadzonych czynności kontrolnych stwierdzono również, że w jednostce zgodnie z art. 30 RODO, prowadzony jest rejestr czynności przetwarzania danych osobowych. Przedmiotowy rejestr został opracowany i jest prowadzony przez IOD wyznaczonego w Urzędzie.

[akta kontroli str. 178-182]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Z § 20 ust. 2 pkt 2 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu

i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Kontrolującym przedstawiono inwentaryzację sprzętu komputerowego użytkowanego w Urzędzie sporządzoną w formie pliku Excel. Przekazana inwentaryzacja w większości nie obejmowała konfiguracji sprzętu zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI.
Z informacji uzyskanych z Urzędu w przedmiotowej sprawie wynika, że cyt.: „Przekazana kontrolującym inwentaryzacja prowadzona jest ręcznie w systemie informatycznym i odzwierciedla aktualny stan i lokalizację sprzętu IT na dzień wydruku. Szczegółowe parametry konfiguracji sprzętu sporządzane są ręcznie w postaci arkusza Excel w okresach rocznych. Pozycje dopisywane są każdorazowo po zakupie sprzętu. Dołączam do pisma plik pdf. ze sprzętem z 2021 r. (...) Pozycje: Licencje Office, Klucz z konta Microsoft, Licencje systemu oraz Właściciel zostały zanonimizowane do celów kontroli."
Przekazane dodatkowe zestawienie sprzętu informatycznego, zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI, zawierało między innymi rodzaj i konfigurację urządzeń.

Jednocześnie należy wspomnieć, że Urząd zakupił i wdraża specjalistyczny system do automatycznej inwentaryzacji sprzętu IT - System Axence nVision do kompleksowego zarządzania w IT - planowane uruchomienie systemu 4 kwartał br.

[akta kontroli str. 406-408, 533-535]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 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;
- § 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.

Istotnym elementem polityki BI (bezpieczeństwa informacji) jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, 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, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

Zasady nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), określone zostały Zarządzeniem Nr 160/2021 Prezydenta Miasta Elbląg wprowadzającym Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Elblągu, w skład której weszła Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych i informacji w Urzędzie Miejskim w Elblągu - §5 pkt 1 ppkt 14 oraz załącznik Nr 1 do Instrukcji zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych i informacji w Urzędzie Miejskim w Elblągu.

[akta kontroli str. 83-174]

Osoby posiadające dostęp do danych osobowych i pracujące w określonym systemie posiadały pisemne upoważnienie. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych i pracy w określonym systemie teleinformatycznym zgodnie z przekazanym wyjaśnieniem, cyt.: „W Urzędzie jest prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych. Ewidencja prowadzona jest w systemie informatycznym SPEKTRUM. Upoważnienia/uprawnienia do pracy w określonym systemie lub module systemu informatycznego dla wszystkich użytkowników także podlegają ewidencjonowaniu. Ewidencja prowadzona jest w Departamencie Innowacji i Informatyki w formie papierowej, chronologicznie dla wszystkich pracowników."

[akta kontroli str. 230-232, 406-408]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że 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.

Z dokumentacji przedstawionej kontrolującym wynika, że pracownicy Urzędu zaangażowani w proces przetwarzania informacji, uczestniczyli w okresie objętym kontrolą w szkoleniach dotyczących bezpieczeństwa informacji oraz ochrony danych osobowych.
W załączeniu przedstawiono prezentację oraz listy pracowników uczestniczących w szkoleniach.

[akta kontroli str. 233-295]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.6. Praca na odległość i mobilne przetwarzanie danych

Zgodnie z § 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.

Zbiór podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość określono Zarządzeniem Nr 160/2021 Prezydenta Miasta Elbląg wprowadzającym Politykę Bezpieczeństwa Informacji (PBI) w Urzędzie Miejskim w Elblągu, w skład której weszła Instrukcja zarządzania systemem teleinformatycznym (IZST) służącym do przetwarzania danych osobowych i informacji w Urzędzie Miejskim w Elblągu - §5 pkt 1 ppkt 15 PBI oraz §5 IZST. Zgodnie z wyjaśnieniem przekazanym w przedmiotowej sprawie, w okresie objętym kontrolą 186 pracowników świadczyło pracę zdalną.

[akta kontroli str. 83-174, 406-408, 536]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 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.

W przypadku systemów informatycznych niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii oraz gwarantującymi bezpieczeństwo informacji (BI) dla informacji uzyskanych przez wykonawców w związku z ich realizacją.

W Urzędzie użytkowanych jest sześć modułów systemu teleinformatycznego przeznaczonych do realizacji zadań zleconych z zakresu administracji rządowej, zakupionych u zewnętrznego dostawcy, tj.:

1) OTAGO SWR Asseco Data Systems – moduł w zakresie świadczeń rodzinnych, zasiłków opiekuńczych, zaliczek alimentacyjnych, jednorazowych świadczeń z tytułu urodzenia dziecka,
2) OTAGO OFA Asseco Data Systems – moduł w zakresie świadczeń z funduszu alimentacyjnego, postępowań wobec dłużników alimentacyjnych,
3) OTAGO RODZINA+ Asseco Data Systems - moduł w zakresie świadczeń wychowawczych, świadczeń Dobry start,
4) OTAGO SWR Asseco Data Systems (Dodatek osłonowy),
5) OTAGO SWR Asseco Data Systems - moduł czyste powietrze – wydawanie zaświadczeń o wysokości przeciętnego miesięcznego dochodu,
6) OTAGO ELUD Asseco Data Systems – moduł w zakresie prowadzenia rejestru mieszkańców,

W związku z zakupem ww. modułów systemu podpisane zostały z dystrybutorami stosowne umowy licencyjne, umożliwiające prawidłową eksploatację i rozwój, poprzez możliwość zgłaszania błędów pytań i roszczeń, dotyczących użytkowanego systemu. Zawarte zostały również stosowne umowy powierzenia danych gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

Procedura zgłaszania awarii oraz procedura zapewnienia ciągłości działania zawarta została w Instrukcja zarządzania systemem teleinformatycznym (IZST) służącym do przetwarzania danych osobowych i informacji w Urzędzie Miejskim w Elblągu.

[akta kontroli str. 83-174, 296-360]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia bezpieczeństwa informacji oraz podejmowanych działań korygujących została uregulowana Zarządzeniem Nr 160/2021 Prezydenta Miasta Elbląg wprowadzającym Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Elblągu - §9.

[akta kontroli str. 83-174]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Zgodnie z § 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.

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą przeprowadzono w Urzędzie jedno audytowe zadanie zapewniające w zakresie bezpieczeństwa informacji, zgodnie ze standardami audytu wewnętrznego. Zakresem przedmiotowym zadania zapewniającego było bezpieczeństwo systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych wg. KRI. Podsumowaniem wykonanego zadania audytowego były opracowane wnioski, w których audytor wewnętrzny stwierdził, że: *Urząd Miejski w Elblągu ustanowi!, wdrożył, eksploatuje, monitoruje i dokonuje przeglądów oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji z uwzględnieniem przepisów prawa w tym zakresie. Stwierdzone uchybienia należą do tych kryteriów bezpieczeństwa, których wyeliminowanie spowoduje, że system będzie bardziej efektywny a koszty pracy oraz wydatki będą niższe.*

Mając powyższe na uwadze, należy stwierdzić, że obowiązek wynikający z § 20 ust. 2 pkt 14 rozporządzenia KRI który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok – w 2021 r. został zrealizowany.

[akta kontroli str. 387-405]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.10. Kopie zapasowe

Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii.

Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Tworzenie kopi zapasowych jest elementem planu ciągłości działania. Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system, np. w bazie danych. Wymóg ten można osiągnąć wykonując regularnie kopie zapasowe całego środowiska pracy danego systemu

teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych.

Zasady tworzenia i przechowywania kopii zapasowych zostały uregulowane Zarządzeniem Nr 160/2021 Prezydenta Miasta Elbląg wprowadzającym Politykę Bezpieczeństwa Informacji (PBI) w Urzędzie Miejskim w Elblągu, w skład której weszła Instrukcja zarządzania systemem teleinformatycznym (IZST) służącym do przetwarzania danych osobowych i informacji w Urzędzie Miejskim w Elblągu - §7 IZST. W Urzędzie wykonywanie kopii zapasowych, przywracanie po awarii oraz odzyskiwanie danych odbywa się automatycznie za pomocą oprogramowania

Na podstawie udostępnionej dokumentacji (zrzuty ekranowe) kontrolujący stwierdzili, że w Urzędzie wykonywane są kopie zapasowe z poszczególnych systemów, jak również przeprowadzane są testy w celu sprawdzenia poprawności oraz przydatności wykonywanych kopii zapasowych.

[akta kontroli str. 361-383]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 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.

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej, dzieliły się na systemy centralne tj. **Źródło, RDO, BUSC** oraz systemy wspierające zakupione u dostawców zewnętrznych – **moduły OTAGO**. Na obsługę aktualnie zainstalowanego oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 83-174, 296-360]

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Z § 20 ust. 2 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:

- 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;
- pkt 9 zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;

- pkt 11 ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego bieżącego dostępu uprawnionym użytkownikom, stosowany jest szereg zabezpieczeń technicznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji. Z informacji uzyskanych podczas kontroli wynika, że cyt.: „W Urzędzie Miejskim w Elblągu stosowanych jest wiele zabezpieczeń techniczno-organizacyjnych. Zastosowane zostały: ochrona fizyczna budynku, monitoring budynku - korytarze i zewnątrz budynku, system alarmowy – serwerownia, Departament Spraw Obywatelskich, pomieszczenia podczas nieobecności pracowników zamykane są na klucz, dokumentacja w formie papierowej przechowywana jest w szafach zamykanych na klucz, dostęp i nadawanie uprawnień do systemów informatycznych nadawany jest zgodnie z zasadami opisanymi w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Elblągu, osoby upoważnione do przetwarzania danych osobowych zostają przeszkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedurach przetwarzania danych i informacji funkcjonujących w Urzędzie Miejskim w Elblągu, oraz poinformowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym, wykonywane kopie zapasowe, wszystkie komputery mają zainstalowany program antywirusowy na bieżąco aktualizowany, użytkownicy pracują na kontach użytkownika z ograniczeniami w dostępie do systemów i stron www, systemy operacyjne są aktualne i na bieżąco aktualizowane. (...) Budynek wyposażony jest w generator prądu i automatyczny system załączania. Tworzone są kopie zapasowe, także poza budynkiem UM."

Ponadto w celu określenia zasad zabezpieczenia dostępu do biur i pomieszczeń Urzędu, w których przetwarzane są informacje, w tym dane osobowe, przyjęto do stosowania *Instrukcję postępowania z kluczami i zabezpieczeniem pomieszczeń*, stanowiącą załącznik do BPI.

[akta kontroli str. 83-174, 406-408]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosownie do:

- § 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;

– § 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.

W punkcie 2.12 wykazano mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Zapewniono również środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej, wszystkie systemy i sieć chronione są przez nowoczesny

[akta kontroli str. 406-408]

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w Urzędzie. Oględzin dokonano w obecności Pana Jacka Boruszki - Dyrektora Departamentu Innowacji i Informatyki Urzędu Miejskiego w Elblągu oraz Pana Grzegorza Mierzwy - Starszego informatyka w Departamencie Innowacji i Informatyki Urzędu Miejskiego w Elbląg.

[akta kontroli str. 64-65]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

– § 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 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;

- § 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.

Zgodnie z § 21 ust. 1 KRI, rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Podczas kontroli ustalono, że Urząd dla kluczowych aplikacji i systemów teleinformatycznych gromadzi logi zdarzeń i aktywności użytkowników. Zgodnie z § 21 ust. 4 rozporządzenia KRI, informacje (logi użytkowników) w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres minimum 2 lat.

[akta kontroli str. 537-554, 406-408]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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

Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z § 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 KRI.

Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej w Urzędzie, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.

Każda strona dostępna w Internecie powinna zapewniać maksymalne wsparcie wszystkim grupom wiekowym jak i społecznym. Warunkiem dostępności strony jest dobry kontrast zapewniający swobodny odczyt przedstawionych informacji. Im wyższy jest kontrast, tym łatwiej odróżnić obiekt, zdjęcie czy tekst pierwszego planu od tła. Niski poziom kontrastu utrudnia korzystanie z witryny przede wszystkim użytkownikom o mniejszej ostrości wzroku, a także osobom niedowidzącym. Celem ułatwienia postrzegania tekstu użytkownikom niedowidzącym można również umożliwić zmianę wielkości tekstu bez utraty jego czytelności lub funkcjonalności serwisu internetowego. Zarówno strona internetowa BIP, jak i strona www. Urzędu zawierają elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niedowidzące. Zastosowane ułatwienia to:

- możliwość doboru odpowiedniego kontrastu,
- możliwość powiększenia wielkości liter na stronie,
- moduł wyszukiwania.

Brak było możliwości walidacji stron w zakresie zgodności z WCAG 2.0 za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0, gdyż w przypadku portalu internetowego Urzędu walidator WAVE-WCAG 2.0 generował błąd wstrzymujący proces sprawdzenia. Walidacji dokonano za pomocą innego dostępnego narzędzia tj. https://validator.utilitia.pl. Portal Internetowy Urzędu spełniał wymogi dostępności, natomiast walidacja strony BIP wykazała że częściowo spełnia ona wymogi dostępności.
Niespełnianie wszystkich kryteriów dostępności, w tym niepełne dostosowanie portalu do standardów WCAG 2.0, należy ocenić jako uchybienie. Przyczyną uchybienia jest brak pełnej dostępności cyfrowej strony internetowej. Skutek uchybienia - brak zapewnienia maksymalnego wsparcia osobom niepełnosprawnym. Odpowiedzialnym za powstanie uchybienia jest osoba nadzorująca działanie strony BIP w Urzędzie.

[akta kontroli str. 562-563]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny, wnoszę o dostosowanie strony BIP Urzędu do wymogów dostępności, w tym standardów WCAG 2.0.

Proszę Pana Prezydenta o podjęcie działań mających na celu usunięcie stwierdzonych uchybień oraz o poinformowanie Wojewody Warmińsko – Mazurskiego w terminie 14 dni od dnia otrzymania niniejszego wystąpienia, o sposobie wykorzystania uwag i wniosków oraz wykonania zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Jednocześnie informuję, że stosownie do art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki
/podpisano podpisem elektronicznym/

1507734.URZĄD MIEJSKI W ELBLĄGU ePUAP-UPP88135871 Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie WMURZADWOJ URZĄD MIEJSKI W ELBLĄGU 974x3yyiku 2022-08-09T09:10:16.855 2022-08-09T09:10:16.855 DOK127793737 Poświadczenie wystawione przez platformę ePUAP 127793737 Zgodnie z art 39¹ par. 1 k.p.a. pisma powiązane z przedłożonym dokumentem będą przesyłane za pomocą środków komunikacji elektronicznej. Zgodnie z art 39¹ par. 1d k.p.a. istnieje możliwość rezygnacji z doręczania pism za pomocą środków komunikacji elektronicznej. not(ancestor-or-self::ds:Signature) uDqXsw3KzazQ5frtkiLxqiEFHQtxBmorY8fmqnRCSZw=not(ancestor-or-self::*[local-name() = 'UnsignedProperties' and namespace-uri() = 'http://uri.etsi.org/01903/v1.3.2#'])
ZvIzdeCoE+/3Z2ZpMwIZ5XfXXKTalGyYZUHBwPANDgI=Shy3s467pBR2ZflqfiEKujPtw2N0y5Ym6A4JwRdl1OI=XNHQ19ggDKKNzvxhN1s6FQMP9J8K58+Dy
08-09T07:10:17Zop46oe6YzXRH3IkntNXXg5K7kYg=CN=Centrum Kwalifikowane EuroCert,O=EuroCert Sp. z
o.o.,C=PL,2.5.4.97=#0c10564154504c2d393531323335323337393608542112950280699735612080302546574667474text/xmltext/xmlhttp://uri.etsi.org/01903/v1.2.2#