WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

FK-IV.431.9.2021

Olsztyn, 22 lipca 2021 r.

Szanowny Pan
Piotr Grzymowicz
Prezydent Olsztyna
Plac Jana Pawła II nr 1
10-101 Olsztyn

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 Miasta Olsztyna[1], Plac Jana Pawła II 1, 10-101 Olsztyn, NIP: 7390504751, REGON: 000594169.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Piotr Grzymowicz** – Prezydent, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 4 listopada 2018 roku.

W dniu rozpoczęcia czynności kontrolnych odpowiedzialnymi za realizację zadania objętego kontrolą w Urzędzie byli:

- [redacted] - Kierownik referatu, [redacted],
- [redacted] - Inspektor ds. ochrony danych osobowych, [redacted],
- [redacted] - Inspektor ds. dokumentacji i monitorowania systemu zarządzania jakością, [redacted],
- [redacted] - Inspektor ds. udostępnienia usług elektronicznych oraz nadzoru merytorycznego nad BIP, [redacted].

[1] Zwanym dalej: Urzędem

Osobą bezpośrednio nadzorującą pracowników odpowiedzialnych za realizację zadania był Pan Stanisław Gorczyca - Sekretarz Miasta, [redacted].

[akta kontroli str. 76]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko-Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – 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.0030.158.2021 z 10 maja 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.159.2021 z 10 maja 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 16-21]

Kontrolę przeprowadzono w dniach 24 maja – 25 czerwca 2021 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, 1/2021 str. 7.

Kontrola prowadzona była w trybie zdalnym, tj. bez osobistej obecności kontrolerów, 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. Rozpoczęcie kontroli nastąpiło podczas wideokonferencji, w trakcie której okazano legitymacje służbowe kontrolerów, poinformowano o zasadach kontroli w trybie zdalnym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania. Upoważnienia kontrolerów do kontroli zostały przekazane do kontrolowanej jednostki za pośrednictwem platformy e-PUAP.

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. 670 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 50-61]

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 2019 r., poz. 1464), 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 tekst jednolity (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r., Dz.U. z 2019 r. poz. 700 ze zm. - akt prawny obowiązujący do 04.03.2020 r., Dz.U. z 2020 r., poz. 346 ze zm. - akt prawny obowiązujący do 12.04.2021 r. oraz Dz.U. z 2021 r., poz. 670 ze zm.)[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, 50-70]

Do kontaktu w okresie trwania czynności kontrolnych upoważniona została dyrektor Biura Kontroli Urzędu Miasta Olsztyna.

[akta kontroli str. 77]

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 nieprawidłowościami.**
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 (zał. nr 2 do programu kontroli) oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywanych jest **11** systemów teleinformatycznych:

[redacted]

[2] Zwanej dalej: ustawą
[3] Zwanego dalej: rozporządzeniem KRI

[redacted]

[akta kontroli str. 39-46]

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 /urzadmiastaolsztyn/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 – Strona główna. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

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.
Bezpośrednie linki do najczęściej wykorzystywanych usług w kontakcie z Urzędem Miasta Olsztyna, w których istnieje możliwość złożenia wniosku elektronicznego za pomocą ESP w przypadku posiadania profilu zaufanego, opublikowane są w BIP.

Ponadto na portalu edeklaracje.olsztyn.eu zostały wdrożone e-usługi dotyczące podatków i opłat lokalnych. W ramach modernizacji portalu zakres e-usług poszerzył się o kolejne usługi związane z gospodarowaniem odpadami komunalnymi.

Jednocześnie na stronie BIP Urzędu, w zakładce *Przyjmowanie i załatwianie spraw* opublikowane zostały opisy procedur obowiązujących przy załatwianiu spraw w Urzędzie, w formie kart usług oraz wniosku w postaci edytowalnej.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 540-542]

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 prowadzonych czynności kontrolnych ustalono, że w okresie objętym kontrolą Urząd nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, jednocześnie Urząd na bieżąco wykorzystywał usługi centralne (ePUAP).
Należy zaznaczyć, iż na stronie BIP Urzędu opublikowano w wersji „do pobrania" formularze wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 1350-1356]

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://olsztyn.eu/, a strona internetowa BIP Urzędu – pod adresem https://umolsztyn.bip.gov.pl/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu w zakładce E-Urząd - E-usługi UMO zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.

Przegląd strony internetowej ujawnił, że w ramach zarzadzania usługami i infrastrukturą wdrożony został projekt „Cyfrowy Olsztyn", który stanowił kolejny etap rozbudowy infrastruktury teleinformatycznej Gminy Olsztyn (Urzędu Miasta Olsztyna) oraz jednostek podległych o nowe rozwiązania systemowe, aplikacyjne oraz sprzętowe, zapewniające możliwość wdrożenia jakościowo nowych, elektronicznych usług publicznych, wspomagających realizację zadań ustawowych będących w kompetencji Gminy Olsztyn. W ramach projektu wdrożono specjalnie przygotowane narzędzia ułatwiające kontakt klienta z urzędem.

W okazanej dokumentacji kontrolujący nie stwierdzili 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, iż 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.

[redacted]

[akta kontroli str. 1350-1356]

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.

Z zarządzenia Nr 15 Prezydenta Miasta Olsztyn z dnia 3 lutego 2011 r. *w sprawie wskazania sposobu wykonywania czynności kancelaryjnych w Urzędzie Miasta Olsztyn* wynika, że podstawowym sposobem wykonywania czynności kancelaryjnych w Urzędzie jest tradycyjny system dokumentowania przebiegu załatwiania i rozstrzygania spraw.
W przypadku spraw wpływających do Urzędu drogą elektroniczną, przyjęto Zarządzenie Nr 71 Prezydenta Miasta Olsztyna z dnia 22 września 2010 roku (zmienione Zarządzeniami Nr 211 z 3 lipca 2013 r. oraz Nr 486 z 19 grudnia 2014 r.) *w sprawie Elektronicznego Systemu obsługi spraw i dokumentów w Urzędzie Miasta Olsztyna oraz świadczenia przez Urząd Miasta Olsztyna usług administracji publicznej drogą elektroniczną.*
Zgodnie z zarządzeniem, elektroniczny system obiegu dokumentów realizowany jest za pomocą aplikacji Mdok działającej w oparciu o instrukcję kancelaryjną i Jednolity Rzeczowy Wykaz Akt. Składanie dokumentu w postaci elektronicznej umożliwia Elektroniczna Skrzynka Podawcza oraz specjalnie wydzielony na stronie BIP Urzędu moduł „E-Urząd".

Wprowadzenie szczegółowych zasad obiegu dokumentacji elektronicznej pozwala na realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 519-539]

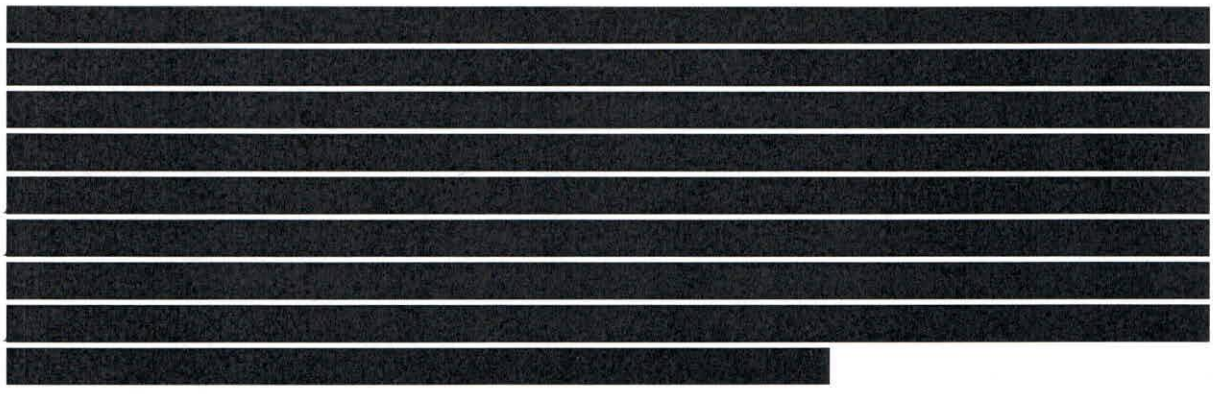
1.6. Formaty danych udostępniane przez systemy teleinformatyczne

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.



[akta kontroli str. 1350-1356]

Mając powyższe na uwadze 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 SZBI jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie. Podstawowym dokumentem SZBI jest Polityka Bezpieczeństwa Informacji. Polityka zawiera zazwyczaj wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji.

Mając powyższe na uwadze, Zarządzeniem Nr 107 Prezydenta Olsztyna z dnia 25 marca 2015 r. wprowadzono w Urzędzie System Zarządzania Bezpieczeństwem Informacji oraz związaną z nim dokumentację. W skład dokumentacji SZBI w Urzędzie weszły:

[redacted]

[redacted]

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. rozporządzenia KRI, ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2014.1182, ze zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024). System Zarządzania Bezpieczeństwem Informacji w Urzędzie wprowadzono zgodnie z normą ISO/IEC 27001:2007.
Dokumentacja w zakresie ochrony danych dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowania zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa danych osobowych.

Jednocześnie należy zaznaczyć, że przedmiotowa dokumentacja obowiązująca w jednostce, 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" została w części zaktualizowana, co ma swoje odzwierciedlenie w kartach zmian do poszczególnych polityk i procedur. Jednakże kontrolujący zwracają uwagę na konieczność bardziej szczegółowej weryfikacji przyjętych zapisów, gdyż część z nich pozostała i funkcjonuje w niezmienionej formie. Przykładem może tu być instytucja Administratora Bezpieczeństwa Informacji (ABI), która wprowadzona została do ustawy o ochronie danych osobowych z dniem 1 stycznia 2015 r., a następnie w związku z wejściem w życie RODO (od 25 maja 2018 r.), zastąpiona została przez Inspektora Ochrony Danych (IOD). W przedstawionych politykach brak jest np. umiejscowienia IOD (pomimo że został on wyznaczony i powołany), w strukturze organizacyjnej administratora danych.

[akta kontroli str. 155-518, 1524-1686]

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.

Z wyjaśnienia uzyskanego z Urzędu w powyższej sprawie wynika że, cyt.: [redacted]

Odnosząc się do powyższych wyjaśnień jak również mając na uwadze przedłożoną do kontroli dokumentację można uznać, że w Urzędzie były prowadzone działania w zakresie monitoringu i przeglądu systemu zarządzania bezpieczeństwem informacji. Jednocześnie należy stwierdzić, że nie były one wykonywane zgodnie z przyjętą *Procedurą* [redacted]

Jednocześnie, przywołany w wyjaśnieniach jednostki utworzony przez Prezydenta Olsztyna zespół do oceny wdrożenia reformy ochrony danych osobowych wynikającej z RODO nie został powołany *stricte* do dokonania przeglądu SZBI, a do organizacyjnej i merytorycznej oceny wdrożenia reformy ochrony danych osobowych wynikającej z RODO. Jednocześnie z dwóch przedstawionych kontrolującym protokołów z posiedzeń zespołu (13.03.2019 oraz 17.04.2019) wynika, że działania zespołu jedynie częściowo obejmowały przegląd dokumentacji SZBI.
W przypadku wspomnianego w wyjaśnieniach dokumentu dotyczącego *wykonania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych w Urzędzie Miasta Olsztyna* - sporządzonego przez IOD, stanowi on głównie sprawozdanie z dotychczasowej działalności IOD w Urzędzie Miasta Olsztyna. Ponadto, z treści przedmiotowego dokumentu (pkt 2.1.2) wynika również, że IOD podejmował działania w zakresie doskonalenia SZBI w jednostce.

Mając powyższe na uwadze należy stwierdzić, że podejmowane działania dotyczące monitorowania i przeglądu SZBI, były przeprowadzone w jednostce, w sposób odbiegający od przyjętych do realizacji procedur w ramach Polityki Bezpieczeństwa Informacji, [redacted] Przyczyną powstania uchybienia jest niestosowanie przyjętych procedur, osobą odpowiedzialną zgodnie z cyt. powyżej procedurą jest GABI.

[akta kontroli str. 186-197, 1350-1356, 1368-1402]

W okresie objętym kontrolą w Urzędzie pełnił swoja funkcję Inspektor Ochrony Danych

(IOD) wyznaczony przez Prezydenta Olsztyna. Stosowne zgłoszenie przesłane zostało do Prezesa Urzędu Ochrony Danych Osobowych.

[akta kontroli str. 545-559]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

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.

Zgodnie z dokumentacją wchodzącą w skład SZBI, przyjętą Zarządzeniem Nr 107 Prezydenta Olsztyna z dnia 25 marca 2015 r. wprowadzającym w Urzędzie System Zarządzania Bezpieczeństwem Informacji oraz związaną z nim dokumentację, zarządzanie ryzykiem w jednostce odbywa się w oparciu o 3 główne dokumenty, tj.:

[redacted]

Zgodnie z PBI pkt. 6.1.1 strategicznym elementem zarządzania aktywami i bezpieczeństwem informacji w Urzędzie Miasta Olsztyna jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem. Wyniki analizy ryzyka stanowią podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia zabezpieczeń informacji Urzędu Miasta Olsztyna.
Zgodnie z udostępnioną kontrolującym dokumentacją w jednostce oszacowano ryzyka związane z zarządzaniem bezpieczeństwem informacji oraz przeprowadzono ich analizę.

[akta kontroli str. 159-169, 299-303, 345-372, 1357-1367, 1471-1475, 1698-1701, 1705-1768]

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.

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 aktualną inwentaryzację sprzętu komputerowego użytkowanego w Urzędzie sporządzoną zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja zgodnie z cyt. powyżej przepisami obejmowała między innymi rodzaj i konfigurację sprzętu.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 153-154]

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 i odbierania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym) określone zostały w dokumentacji wchodzącej w skład SZBI, przyjętej Zarządzeniem Nr 107 Prezydenta

Olsztyna z dnia 25 marca 2015 r. wprowadzającym w Urzędzie System Zarządzania Bezpieczeństwem Informacji oraz związaną z nim dokumentację. Szczegółowe regulacje w powyższym zakresie opisane zostały w dokumentach – [redacted]

[akta kontroli str. 198-210, 310-339, 420-438]

W Urzędzie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym). Upoważnienia nadawane są przez Administratora Danych Osobowych (lub z jego upoważnienia).

[akta kontroli str. 310-337, 544]

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 (zorganizowanych przez IOD), dotyczących systemu zarządzania bezpieczeństwem informacji w jednostce. Przedmiotowe szkolenia zgodnie z przekazaną prezentacją, obejmowały swym zakresem następujące zagadnienia:

- System Zarządzania Bezpieczeństwem Informacji,
- Krajowe Ramy Interoperacyjności (KRI),
- Norma ISO 27001,
- zarządzenie Prezydenta Olsztyna nr 107 z dnia 25.03.2015 r.,
- ochrona danych osobowych (RODO),
- podstawowe zagadnienia w zakresie ochrony danych osobowych,
- obowiązki w organizacji.

W załączeniu przedstawiono prezentację dotyczącą tematyki szkolenia oraz listy obecności pracowników uczestniczących w szkoleniach.

Ponadto zgodnie z przekazanymi kontrolującym wykazami osobowymi, pracownicy zostali zapoznani z dokumentacją dotyczącą ochrony danych osobowych, a w szczególności z Polityką Bezpieczeństwa Danych Osobowych, Regulaminem Użytkowania Systemów

Teleinformatycznych oraz Instrukcją Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych.

[akta kontroli str. 77-136]

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.*

Z dokumentacji wchodzącej w skład SZBI przyjętej w Urzędzie wynika, że w załączniku nr 2 do [redacted] opracowane zostały szczegółowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, w tym praca zdalnej.

[akta kontroli str. 217-230]

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.

Na podstawie przedstawionej dokumentacji kontrolujący stwierdzili, że umowy serwisowe zakupionych 4 systemów teleinformatycznych umożliwiają prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu. Zawarte stosowne umowy powierzenia danych gwarantująca właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[redacted]

[redacted]

[akta kontroli str. 439-455, 560-1345]

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 ochrony danych osobowych oraz podejmowanych działań korygujących została uregulowana w dokumentacji wchodzącej w skład SZBI, przyjętej Zarządzeniem Nr 107 Prezydenta Olsztyna z dnia 25 marca 2015 r. wprowadzającym w Urzędzie System Zarządzania Bezpieczeństwem Informacji oraz związaną z nim dokumentację. Szczegółowe regulacje w powyższym zakresie opisane zostały w dokumencie – [redacted]

[akta kontroli str. 278-288]

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, iż w okresie objętym kontrolą tj. od 1 stycznia 2019 r. do dnia 31 grudnia 2020 r., w jednostce przeprowadzono 1 zadanie audytowe (marzec 2020 r.) w zakresie bezpieczeństwa informacji. Zgodnie z okazaną dokumentacją cele szczegółowe przeprowadzonego zadania audytowego obejmowały:

[redacted]

Audyt bezpieczeństwa informacji przeprowadzony został przez audytora wewnętrznego Urzędu Miasta Olsztyna. Z ogólnego podsumowania przeprowadzonego zadania audytowego wynikało, że przyjęty w Urzędzie system ochrony danych osobowych daje racjonalne zapewnienie, że dane osobowe będące w zasobach Urzędu będą właściwie chronione.
Mając powyższe na uwadze, należy stwierdzić, że w 2020 roku dopełniono obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI.

Jednocześnie na podstawie okazanej dokumentacji kontrolujący stwierdzili, że w przypadku 2019 r., audyt w zakresie bezpieczeństwa informacji nie został przeprowadzony, w sposób wymagany § 20 ust. 2 pkt 14 rozporządzenia KRI.
Z wyjaśnienia uzyskanego z jednostki w powyższej sprawie wynika, że cyt.: „[redacted]".

Odnosząc się do powyższego wyjaśnienia należy stwierdzić, że w związku z koniecznością realizacji w 2019 r. obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, tj. zapewnienia w jednostce okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, [redacted]

[akta kontroli str. 137-150, 1350-1356]

Brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji w 2019 r. skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, jak również obowiązku wynikającego z zapisów [redacted], która stanowi załącznik do Zarządzenia Nr 107 Prezydenta Olsztyna z dnia 25 marca 2015 r. *w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Olsztyna oraz związanej z nim Dokumentacji.* Osobą odpowiedzialną za powstanie nieprawidłowości jest zgodnie z zapisami [redacted] GABI kontrolowanej jednostki.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.

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.

[redacted]

[akta kontroli str. 1476-1523, 1698-1704]

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.:

[redacted]

oraz systemy wspierające zakupione u dostawców zewnętrznych tj.:

[redacted]

Na obsługę aktualnie zainstalowanego oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupione systemy teleinformatyczne, w razie awarii podlegają ekspertyzie technicznej zlecanej firmie dostarczającej.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 39-46, 560-1345]

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.

[redacted]

[akta kontroli str. 25-38, 1350-1356]

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.*

[redacted]

[redacted]

[akta kontroli str. 25-38, 1350-1356]

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).

[redacted]

[redacted]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 25-38, 72-73, 1687-1697]

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 niepełnosprawne w tym niedowidzące. Zastosowane ułatwienia to:

- możliwość zmiany rozmiaru tekstu,
- moduł wyszukiwania,
- widoczny fokus wokół elementów nawigacyjnych,
- wyróżnienie odnośników.

Ponadto z informacji zawartych na stronie wynika, że umożliwiono komunikowanie się z Urzędem osobom uprawnionym, poprzez organizację świadczenia usług:

- polskiego języka migowego (PJM) – naturalny wizualno-przestrzenny język komunikowania się osób uprawnionych;
- systemu językowo-migowego (SJM) – podstawowy środek komunikowania się osób uprawnionych, w którym znaki migowe wspierają wypowiedź dźwiękowo-artykulacyjną;
- komunikowania się osób głuchoniewidomych (SKOGN) – należy przez to rozumieć podstawowy środek komunikowania się osób uprawnionych, w którym sposób przekazu komunikatu jest dostosowany do potrzeb wynikających z łącznego występowania dysfunkcji narządu wzroku i słuchu.

Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strony BIP i www. spełniają poniższe zasady:

- postrzeganie – informacje oraz komponenty interfejsu strony były przedstawione użytkownikom w sposób dostępny dla jego zmysłów,
- funkcjonalność – komponenty interfejsu stron umożliwiały korzystanie z nich,
- zrozumiałość – informacje oraz obsługa interfejsu były zrozumiałe.
- kompatybilność – strony wyświetlały się zawsze poprawnie.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP i strony www. nie wykazała błędów.

[akta kontroli str. 151-152]

Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Przeprowadzanie okresowych przeglądów i monitoringu SZBI, zgodnie z § 20 ust. 1 rozporządzenia KRI, w oparciu o pkt 8.2 [redacted].

2. Zapewnienie w jednostce okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.

Proszę Pana Prezydenta o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości i 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