WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 10 maja 2021 r.

FK-IV.431.8.2021

Szanowny Pan
Grzegorz Mrowiński
Burmistrz Działdowa
ul. Zamkowa 12
13-200 Działdowo

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 Działdowo[1], ulica Zamkowa 12, 13-200 Działdowo, NIP: 5711602078, REGON: 000524358

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan Grzegorz Mrowiński – Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 października 2018 roku.

W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą w Urzędzie był [redacted] - [redacted] zatrudniony na podstawie umowy o pracę od dnia 11 lutego 2008 r. Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania był [redacted] - [redacted], zatrudniony na podstawie umowy o pracę od dnia 27 sierpnia 2020 r.

[akta kontroli str. 64]

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.0030.73.2021 z 11 marca 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[1] Zwanym dalej: Urzędem

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.0030.74.2021 z 11 marca 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 18-19]

Kontrolę przeprowadzono w dniach 24 marca – 14 kwietnia 2021 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 4/2021.

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 2020 r., poz. 346 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 48-59]

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 (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. oraz Dz.U. z 2020 r., poz. 346 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

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

publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 48-59]

Burmistrz Działdowa upoważnił Kierownik Referatu Informatyki Urzędu Miasta Działdowo, do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 65]

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 oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są **3** systemy teleinformatyczne:

1. Źródło (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr Dowodów Osobistych),
2. PUMA (ewidencja ludności),
3. CEIDG (działalność gospodarcza).

Systemy teleinformatyczne wykorzystywane w Urzędzie:

1) **ŹRÓDŁO** – (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr dowodów osobistych) bezpłatna aplikacja, która obsługuje wszystkie wymagane polskim prawem działania w zakresie rejestru PESEL, dowodów osobistych. Dodatkowo umożliwia również realizację zadań Systemu Odznaczeń Państwowych oraz Centralnego Rejestru Sprzeciwów. W efekcie ŹRÓDŁO to uniwersalne narzędzie obsługujące m.in.: Rejestr PESEL, Rejestr Bazy Usług Stanu Cywilnego (BUSC), Rejestr Dowodów Osobistych (RDO), System Odznaczeń Państwowych (SOP), Centralny Rejestr Sprzeciwów (CRS).
2) **PUMA - Moduł Ewidencja Ludności (rejestr mieszkańców)** posiada homologację Ministerstwa Spraw Wewnętrznych, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności. Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie, uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca. Program automatyzuje pracę i drukuje zawiadomienia w zakresie: meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego - gromadzenia i dostępu do danych historycznych mieszkańców.
3) **CEIDG** jest to elektroniczny rejestr przedsiębiorców działających na terenie kraju. Portal ułatwia podatnikom prowadzenie działalności gospodarczej. Umożliwia on założenie firmy, aktualizację danych, jak również zamknięcie czy zawieszenie działalności gospodarczej. Służy również do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.

[akta kontroli str. 37-39]

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 /xys4h3v93c/skrytka, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Pełny adres oraz 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. W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, iż na stronie BIP w zakładce *Na skróty – Jak załatwić sprawę*, opublikowane są procedury niezbędne do realizacji przy załatwianiu danej sprawy. Ponadto na stronie BIP opublikowane są wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie niezbędnych do załatwienia danej sprawy. Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą 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. 25-36, 66-67]

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 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, że Urząd Miasta korzysta ze wzorów dokumentów zamieszczonych w CRWDE opublikowanych przez MSWiA w zakresie realizacji zadań Urzędu Stanu Cywilnego oraz Wydziału Spraw Obywatelskich.
Jednocześnie 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. 25-36, 207-214]

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.dzialdowo.pl/, a strona internetowa BIP Urzędu – pod adresem http://bip.dzialdowo.eu/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej części panelu strony. Na stronie głównej BIP Urzędu zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.

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, 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.

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „[redacted]

[redacted]
[redacted]
[redacted]"

[akta kontroli str. 207-214]

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.*

W Urzędzie w celu zarządzania obiegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do Urzędu zawarte w Instrukcji Kancelaryjnej, stanowiącej załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. Zgodnie z Zarządzeniem Nr 8/2011 Burmistrza - Kierownika Urzędu Miasta Działdowo z dnia 23 lutego 2011 r. w sprawie wskazania systemu wykonywania czynności kancelaryjnych w Urzędzie Miasta Działdowo - podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie jest tradycyjny system wykonywania czynności kancelaryjnych.
Jednocześnie, w okazanej dokumentacji Urzędu brak jest procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP), co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby 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.

Z uzyskanego w ramach prowadzonych czynności kontrolnych wyjaśnienia wynika, że cyt.: *„Obecnie jesteśmy w trakcie przygotowania zarządzenia regulującego obieg dokumentów wpływających i wypływających w formie elektronicznej. Obecnie wiodącym systemem obiegu dokumentów jest system papierowy. Urząd przygotowuje się do wprowadzenia systemu elektronicznego jako jedynego funkcjonującego w urzędzie. Związane jest to z kosztownymi inwestycjami w sprzęt, oprogramowanie i szkolenia, które zostaną opłacone w ramach realizowanego projektu „Rozwoju e-usług publicznych w Gminie-Miasto Działdowo"*

finansowanego z Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020 [redacted] *Równolegle rozpoczęliśmy prace na stworzeniem niezbędnych dokumentów."*

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 68, 207-214]

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.: „[redacted]"

[akta kontroli str. 207-214]

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.*

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", zarządzeniem 11/2018 Kierownika Urzędu Miasta Działdowo z dnia 24 maja 2018 roku wprowadzono do stosowania w Urzędzie Miasta Działdowo **Politykę ochrony danych osobowych**.

[akta kontroli str. 69-87]

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 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. PBI może określać aktywa oraz ich właścicieli, oraz sposób szacowania ryzyka i postępowania z ryzykiem.
Zazwyczaj w ramach SZBI funkcjonują inne polityki, regulaminy i procedury np.:

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.

- Procedura zarzadzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywaniem testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.

Dokumentację SZBI stanowią także:

- Dokumentacja z przeglądów SZBI;
- Dokumentacja z szacowania ryzyka BI;
- Dokumentacja postępowania z ryzykiem;
- Dokumentacja akceptacji ryzyka;
- Dokumentacja audytów z zakresu BI;
- Dokumentacja incydentów naruszenia BI;
- Dokumentacja zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Dokumentacja zarządzania sprzętem i oprogramowaniem teleinformatycznym;
- Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Na podstawie przekazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą w Urzędzie nie została opracowana pełna dokumentacja ustanawiająca System Zarzadzania Bezpieczeństwem Informacji, wymagana zgodnie z § 20 ust. 1 rozporządzenia KRI zapewniająca poufność, dostępność i integralność informacji. Przyjęta zarządzeniem nr 11/2018 Kierownika Urzędu Miasta Działdowo z dnia 24 maja 2018 roku Polityka ochrony danych osobowych stanowi tylko jedną ze składowych dokumentacji ustanawiającej SZBI w jednostce i nie dopełnia obowiązku wynikającego z cytowanych powyżej przepisów.

Z wyjaśnienia Burmistrza w powyższej sprawie wynika, że, cyt.: *„Pracownik odpowiedzialny za opracowanie SZBI w Urzędzie Miasta Działdowo, pomimo ciążącego na nim obowiązku nie zrealizował wyznaczonego mu zadania. Po dokonaniu nieformalnego audytu w trakcie którego stwierdzono braki w dokumentacji podjęto decyzję o rozwiązaniu umowy z pracownikiem, który pełnił funkcję inspektora ochrony danych osobowych i zarazem*

administratora bezpieczeństwa informacji. Rozpoczęto działania zmierzające do wyeliminowania braków."

Powyższe stanowi nieprawidłowość, skutkującą naruszeniem § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

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.
Kontrolujący stwierdzili na podstawie udostępnionej do kontroli dokumentacji, że w Urzędzie nie były prowadzone działania w zakresie monitoringu i przeglądu systemu zarządzania bezpieczeństwem informacji, co stanowi uchybienie.

Z wyjaśnienia Burmistrza w powyższej sprawie wynika, że, cyt.: *„Pracownik odpowiedzialny za opracowanie SZBI w Urzędzie Miasta Działdowo, pomimo ciążącego na nim obowiązku nie zrealizował wyznaczonego mu zadania (...)".*
„Pomimo braku sformalizowanej procedury w formie SZBI z przyczyn, o których pisałem wyżej, w naszej jednostce na bieżąco utrzymywaliśmy aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji oraz podejmowaliśmy różnorodne działania zmierzające do zminimalizowania ryzyka utraty danych między innymi: nadawanie i kontrolę uprawnień w procesie przetwarzania informacji, zmiany uprawnień wymaganej zmianą statusu pracownika, szkoleń, zabezpieczenia aktywów informatycznych w odpowiednią ochronę na poziomie systemów operacyjnych, usług sieciowych i aplikacji."

Brak okresowych przeglądów i monitoringu SZBI w jednostce stanowi naruszenie § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną jest IOD jednostki pełniący funkcję w okresie objętym kontrolą.

[akta kontroli str. 207-214]

Burmistrz Działdowa wyznaczył Administratora Systemu Informatycznego w Urzędzie (ASI). Zarządzeniem 11/2018 Kierownika Urzędu Miasta Działdowo z dnia 24 maja 2018 roku wyznaczył w jednostce Inspektora Ochrony Danych (IOD). W celu kontynuacji zadania podpisał stosowna umowę z firmą zewnętrzną na świadczenie usługi IOD w jednostce.

[akta kontroli str. 88-97]

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

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 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.
Zgodnie z przekazaną dokumentacją wymagane oszacowanie i analiza ryzyka utraty integralności, dostępności lub poufności informacji w jednostce, przeprowadzona została w czerwcu 2020 roku. Jednocześnie należy zaznaczyć, iż kontrolującym nie przedstawiono dokumentacji świadczącej o przeprowadzeniu okresowej analiz ryzyka utraty integralności, dostępności lub poufności informacji w 2019 roku.

Z przekazanego w powyższej sprawie wyjaśnienia wynika, że cyt.: *„Pracownik odpowiedzialny za przeprowadzenie analizy ryzyka w oparciu o załącznik nr 3, pomimo ciążącego na nim obowiązku nie zrealizował wyznaczonego mu zadania. Po stwierdzeniu zaniechania ciążącego na nim obowiązku podjęto decyzję o rozwiązaniu umowy o pracę z pracownikiem. Rozpoczęto działania zmierzające do wyeliminowania braków."*

[akta kontroli str. 204-205, 207-220]

Odnosząc się do wyjaśnienia należy stwierdzić, że 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.
W związku z powyższym brak przeprowadzonej okresowej analizy ryzyka należy uznać za nieprawidłowość skutkującą naruszeniem § 20 ust. 2 pkt 3 rozporządzenia KRI. Osobą odpowiedzialną jest pracownik pełniący obowiązki IOD w tym okresie.

W toku prowadzonych czynności kontrolnych stwierdzono również, iż w jednostce w 2019 r. nie prowadzono rejestru czynności przetwarzania danych osobowych. Przedmiotowy rejestr został opracowany i jest prowadzony przez kolejnego IOD, z którym jednostka podpisała umowę w 2020 r.
Z przekazanego w powyższej sprawie wyjaśnienia wynika, że cyt.: *„Prace nad stworzeniem rejestru czynności przetwarzania danych osobowych zostały rozpoczęte wraz z zatrudnieniem w 2020 roku Inspektora Danych Osobowych. Rezultatem działań jest powstały i na bieżąco uaktualniany rejestr."*

Brak w 2019 r. rejestru czynności przetwarzania danych osobowych stanowi nieprawidłowość skutkującą naruszeniem art. 30 RODO oraz §10 ust. 4 przyjętej w jednostce PODO. Osobą odpowiedzialną jest pracownik pełniący obowiązki IOD w tym okresie.

[akta kontroli str. 204-205, 207-214, 221-342]

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

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. 98-148]

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 Zarządzeniem nr 11/2018 Kierownika Urzędu Miasta Działdowo z dnia 24 maja 2018 roku w sprawie ochrony danych osobowych w Urzędzie Miasta Działdowo – Rozdział 6 PODO.

[akta kontroli str. 70-87]

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienie. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym). Upoważnienia nadawane były przez Administratora Danych Osobowych – Burmistrza kontrolowanej jednostki (lub z jego upoważnienia przez zastępcę Burmistrza).

[akta kontroli str. 158-175]

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 6 szkoleniach (zorganizowanych przez IOD), dotyczących ochrony danych osobowych. Szkolenia przeprowadzono w okresie maj-czerwiec 2020 r. Przedmiotowe szkolenia zgodnie z uzyskaną informacją, obejmowały swym zakresem następujące zagadnienia:

- RODO podstawowe zagadnienia;
- Naruszenie ochrony danych osobowych - zasady zgłaszania naruszeń, terminy,

konsekwencje;

- Bezpieczeństwo danych osobowych w systemach informacyjnych oraz w infrastrukturze IT;
- Hasła, zasady tworzenia, dostępność, konsekwencje złamania bądź zagubienia;
- Metody szyfrowania dokumentacji elektronicznej;
- Obowiązki ADO w zakresie technicznych (elektronicznych i fizycznych) zabezpieczeń ochrony danych osobowych.

W załączeniu przedstawiono listy obecności pracowników uczestniczących w szkoleniach.

[akta kontroli str. 176-189]

Na zadane przez kontrolujących pytanie dotyczące podania przyczyny braku przeprowadzonych szkoleń pracowników Urzędu w zakresie dotyczącym ochrony danych osobowych w 2019 r., Burmistrz wyjaśnił, że cyt.: *„W roku 2019 Inspektor Danych Osobowych nie wywiązał się z określonych zdań. W roku 2020 szkolenia pracowników przeprowadzał nowo zatrudniony Inspektor Danych Osobowych (...) ODA Ochrona Danych Audyt."*

Odnosząc się do powyższych wyjaśnień należy stwierdzić, że przeprowadzenie szkoleń osób zaangażowanych w proces przetwarzania informacji dopiero w 2020 r. stanowi uchybienie. Skutkiem uchybienia jest naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI, a co za tym idzie niedoinformowanie oraz brak wiedzy pracowników uczestniczących w procesie przetwarzania danych osobowych w zakresie nowych przepisów prawa regulujących powyższą tematykę. Osobą odpowiedzialną jest Inspektor Ochrony Danych Osobowych pełniący funkcję w tym okresie.

[akta kontroli str. 204-205, 207-214]

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

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 wyjaśnienia Burmistrza Działdowa wynika, że cyt.: *„Systemy teleinformatyczne, będące przedmiotem kontroli, ze względu na swoją specyfikę nie umożliwiają przetwarzania danych osobowych na odległość. Zasady pracy zdalnej zostały określone w nowej polityce bezpieczeństwa danych osobowych w 2021 r."*

[akta kontroli str. 205-206, 207-214]

Przedmiotowe cząstkowe zagadnienie ze względu na wykorzystywanie sprzętu w zakresie systemów teleinformatycznych tylko w siedzibie jednostki (stacjonarny tryb pracy) nie podlegało ocenie.

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 użytkowany jest jeden system teleinformatyczny przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupiony u zewnętrznego dostawcy, tj.: [redacted].

W związku z zakupem ww. systemu podpisane zostały z firmą [redacted] stosowne umowy licencyjne umożliwiające prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu. Zawarta została również stosowna umowa powierzenia danych gwarantująca właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli str. 190-203]

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 Zarządzeniem nr 11/2018 Kierownika Urzędu Miasta Działdowo z dnia 24 maja 2018 roku w sprawie ochrony danych osobowych w Urzędzie Miasta Działdowo – Rozdział 10.

[akta kontroli str. 70-87]

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 (06.03-10.06.2020 r.) w zakresie bezpieczeństwa informacji. Zgodnie z okazaną dokumentacją cele szczegółowe przeprowadzonego zadania audytowego obejmowały:

- Ocenę zapewnienia zgodności działań z przepisami RODO poprzez analizę wdrożonej dokumentacji i procesów pozyskiwania danych osobowych oraz badanie poziomu wiedzy z zakresu danych osobowych pracowników urzędu;
- Analizę prawidłowości powierzania przetwarzania danych osobowych;
- Analizę uregulowań dotyczących statusu Inspektora Ochrony Danych Osobowych;
- Ocenę organizacji bezpieczeństwa informacji;
- Zdiagnozowanie poziomu świadomości pracowników z zakresu bezpieczeństwa informacji;
- Analizę zagrożeń związanych z przetwarzaniem danych przez pracowników.

Mając powyższe na uwadze należy stwierdzić, że w 2020 roku dopełniono obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI.

[akta kontroli str. 149-157]

W przypadku 2019 r. kontrolujący na podstawie okazanej dokumentacji stwierdzili, że audyt w zakresie bezpieczeństwa informacji nie został przeprowadzony. Z wyjaśnienia Burmistrza Działdowa wynika, że cyt.: *„Przyczyną zaistniałej sytuacji jest wspomniany wcześniej pracownik, który nie wywiązywał się ze swoich obowiązków."*

[akta kontroli str. 205-206, 207-214]

Brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji w 2019 r. skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD 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.

Urząd w powyższej sprawie wyjaśnił, że cyt.: „[redacted]"

[akta kontroli str. 205-206, 207-214, 343]

W dokumentacji PODO przyjętej w Urzędzie brak jest opracowanych ogólnych procedur regulujących proces wytwarzania kopii zapasowych z systemów użytkowanych w jednostce. Dla każdego elementu będącego przedmiotem wykonywania kopii zapasowych, administrator systemu informatycznego określa częstotliwość tworzenia kopii zapasowych, nośnik na jakim wykonywano kopię, sposób wykonywania oraz miejsce i okres przechowywania kopii zapasowych. Przedmiotowe ustalenia muszą zostać udokumentowane w postaci przyjętego harmonogramu wykonywania kopii zapasowych.
Brak powyższych informacji w PODO należy zakwalifikować jako uchybienie. Osobą odpowiedzialną za powstanie uchybienia jest IOD kontrolowanej jednostki pełniący swe obowiązki w tym okresie.

W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenia przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu Urząd wyjaśnił, że cyt.: „[redacted]"

Na podstawie udostępnionej dokumentacji oraz wyjaśnień kontrolujący stwierdzili, że w Urzędzie nie są wykonywane (oprócz jednego przypadku opisanego w wyjaśnieniach), testy w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenie przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu.

Jednocześnie należy zaznaczyć, iż brak potwierdzenia w dokumentacji czynności w zakresie wykonywania testów w celu sprawdzenia poprawności kopii zapasowych oraz sprawdzenia przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia, nie pozwala kontrolującym jednoznacznie stwierdzić, że sprawdzenia poprawności tworzonych kopii zapasowych było faktycznie wykonane. W dokumentacji PODO przyjętej w Urzędzie brak jest również opracowanych procedur regulujących proces testowania wytworzonych kopii zapasowych. Powyższe działania należy zakwalifikować jako uchybienie.
Osobami odpowiedzialnymi za powstanie uchybienie są: pracownik realizujący zadanie oraz osoba bezpośrednio go nadzorująca.

[akta kontroli str. 205-206, 207-214]

Należy wskazać, że regularne testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Wskazane jest przechowywanie kopii zapasowych w innej lokalizacji niż miejsce ich tworzenia.

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

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 i CEiDG oraz systemy wspierające zakupione u [redacted]. 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. 190-199]

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.

Zgodnie z wyjaśnieniem uzyskanym w trakcie kontroli, cyt.: „[redacted]"

[akta kontroli str. 205-206, 207-214]

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, poprzez:

[redacted]

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).
Z wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że cyt.: „[redacted]".

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 204-205, 207-214]

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:

- odpowiedni kontrast,

- możliwość powiększenia wielkości liter na stronie,
- moduł wyszukiwania,
- focus wokół elementów nawigacyjnych,
- skróty klawiszowe - na stronie internetowej można używać standardowych skrótów klawiaturowych.

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.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP i strony www. wykazała błędy, które nie mają wpływu na przedmiot kontroli. Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby również zasady obiegu dokumentów wpływających i wypływających z Urzędu drogą elektroniczną.
2. Opracowanie i stosowanie w Urzędzie pełnej dokumentacji (w postaci regulacji wewnętrznych), ustanawiającej System Zarzadzania Bezpieczeństwem Informacji, wymaganej zgodnie z § 20 ust. 1 rozporządzenia KRI.
3. Przeprowadzanie okresowych przeglądów i monitoringu SZBI w jednostce zgodnie z § 20 ust. 1 rozporządzenia KRI.
4. Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI przeprowadzanie okresowej analiza ryzyka utraty integralności, dostępności lub poufności informacji, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, wprowadzenie działań minimalizujących to ryzyko.
5. W przypadku zmiany przepisów prawnych lub dokonywania aktualizacji dokumentacji SZBI, przeprowadzanie szkoleń osób zaangażowanych w proces przetwarzania informacji, zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI bez zbędnej zwłoki.
6. Zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.

7. Zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI regularne testowanie jakości wytworzonych kopii zapasowych poprzez odtworzenie danych systemu informatycznego z wytworzonej kopii. Ponadto każdorazowe dokumentowanie wykonywanych testów poprawności tworzonych kopii zapasowych.
8. Uzupełnienie przyjętej w Urzędzie dokumentacji BI poprzez zawarcie w niej opracowanych ogólnych procedur regulujących proces wytwarzania i testowania kopii zapasowych z systemów użytkowanych w jednostce.

W związku ze stwierdzoną podczas realizacji czynności kontrolnych nieprawidłowością, tj. brakiem w 2019 r. rejestru czynności przetwarzania danych osobowych wymaganego zgodnie z art. 30 RODO oraz §10 ust. 4 przyjętej w jednostce Polityki ochrony danych osobowych, odstępuje się od wydania zaleceń pokontrolnych w tym zakresie, ze względu na opracowanie przez IOD w 2020 r. tj. jeszcze w okresie objętym kontrolą przedmiotowego rejestru.

Proszę Pana Burmistrza 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