WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

FK-IV.431.19.2020

Olsztyn, 8 lutego 2021 r.

Szanowny Pan
Adam Szczepkowski
Wójt Gminy Grunwald
Gierzwałd 33
14-107 Gierzwałd

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 Gminy Grunwald[1], Gierzwałd 33, 14-107 Gierzwałd, NIP: 741-209-03-87, Regon: 510743232.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był:

- Pan Henryk Kacprzyk – Wójt Gminy, wybrany na stanowisko w wyniku wyborów bezpośrednich – pełnił swoją funkcję do 22 listopada 2018 roku (nadzorujący bezpośrednio pracownika realizującego zadania objęte kontrolą).
- Pan Adam Szczepkowski – Wójt Gminy, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 7 listopada 2018 roku (nadzorujący bezpośrednio pracownika realizującego zadania objęte kontrolą).

Odpowiedzialnymi za realizację zadania objętego kontrolą w Urzędzie byli:

- Pan [redacted] - pracownik Urzędu Gminy Grunwald (informatyk), Inspektor Ochrony Danych w Urzędzie Gminy Grunwald od dnia 24.05.2018 r. Zatrudniony do dnia 31 maja 2020 r.
- Pan [redacted] – pracownik biurowy – zatrudniony na podstawie umowy o pracę od 21.02.2020 r.

[akta kontroli str. 70, 74-76, 456-471, 499]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko-Mazurskiego Urzędu Wojewódzkiego w Olsztynie:

[1] Zwanym dalej: Urzędem

Radosław Gazda – St. 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.0030.393.2020 z 9 grudnia 2020 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – St. 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.0030.394.2020 z 9 grudnia 2020 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 41-42]

Kontrolę przeprowadzono w dniach 17 grudnia 2020 r. – 15 stycznia 2021 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją OR.1714.18/2020, Nr 3/2020.
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 2018 r. do dnia 17 grudnia 2020 r. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1-2, 25, 68]

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.

[2] Zwanej dalej: ustawą

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, 25, 53-63]

Wójt Gminy Grunwald upoważnił pracownika biurowego (odpowiedzialnego za realizację zadania) do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 416]

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, rejestr wyborców),
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:

[3] Zwanego dalej: rozporządzeniem KRI

meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego - gromadzenia i dostępu do danych historycznych mieszkańców.

Moduł Wyborcy - kompleksowa obsługa wyborów. Moduł Wyborcy umożliwia prowadzenie i aktualizację rejestru wyborców, sporządzanie spisów wyborców uprawnionych do udziału w wyborach i referendum, pozwala na generowanie kwartalnych meldunków dla KBW (Krajowego Biura Wyborczego) o stanie wyborców mieście na podstawie bazy danych ewidencyjnych.

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.

Rejestry publiczne i ewidencje prowadzone w Urzędzie:

- Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości (podstawa prawna - art. 9b ust. 2-3 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, Dz. U. z 2020 r., poz. 1439).
- Ewidencja udzielonych i cofniętych zezwoleń na opróżnianiem zbiorników bezodpływowych i transport nieczystości ciekłych na terenie Gminy (podstawa prawna - art. 7 ust. 6b ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, Dz. U. z 2020 r., poz. 1439).
- Rejestr umów Gminy Grunwald dot. zamówień publicznych o wartości powyżej 30 000 euro zgodnie z ustawą p.z.p.
- Rejestr instytucji kultury, dla których organizatorem jest Gmina.

[akta kontroli str. 36-40, 53-63, 438-441]

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 **/2815032/SkrytkaESP,** znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na głównej stronie internetowej BIP Urzędu. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: ODF, ODS, DOC, RTF, XLS, CSV, TXT, PNG, GIF, TIF, BMP, JPG, PDF, ZIP, RAR, 7zip.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, iż na stronie BIP w zakładce *prawo lokalne - tryb i sposób załatwiania spraw*, opublikowanych jest część procedur niezbędnych do realizacji przy załatwianiu 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 na stronie BIP opublikowane są wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie.

Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do urzędu" oraz „Udostępnianie informacji publicznej na wniosek". Usługi te umożliwiają złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 442-447]

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 Urząd w badanym okresie nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE.
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. 27-35, 456-460]

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 http://www.gminagrunwald.pl/, a strona internetowa BIP Urzędu – pod adresem http://gminagrunwald.biuletyn.net/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu oraz platformy ePUAP, w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu zamieszczono link do skrzynki podawczej ESP na platformie ePUAP. Na stronie BIP w zakładce e-Urząd - *Wnoszenie dokumentów za pośrednictwem Elektronicznej Skrzynki Podawczej na ePUAP,* znajduje się szczegółowa instrukcja postępowania w przypadku przekazywania dokumentu w formie elektronicznej.

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.: „Kontrolowane systemy współpracują z innymi publicznymi systemami teleinformatycznymi. Wymiana informacji odbywa się pomiędzy systemem PUMA i ŹRÓDŁO. Możliwa jest ona dzięki wyposażeniu w odpowiedni sprzęt do transmisji danych po łączu dedykowanym. Wymiana informacji między systemem PUMA, a ŹRÓDŁEM odbywa się poprzez odizolowaną sieć wewnętrzną zgodnie z zaleceniami MSWiA. (...) [redacted] *Logowanie użytkowników do systemu ŹRÓDŁO odbywa się za pomocą kart kryptograficznych z dedykowanymi certyfikatami."*

[akta kontroli str. 27-35, 456-460]

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.*

Zgodnie wyjaśnieniem przekazanym z Urzędu, cyt.: *„W Urzędzie Gminy Grunwald podstawowym sposobem załatwiania wszelkich spraw w urzędzie opiera się na systemie tradycyjnym. Zarządzanie bezpieczeństwem informacji realizowane jest przez zapewnienie warunków umożliwiających realizację i egzekwowanie m.in. zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniknięcie. W Urzędzie przyjęto Zarządzenie nr 1/2017 Wójta Gminy Grunwald z dnia 2.01.2017 r. w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym w oparciu o ustawę o ochronie danych osobowych z dnia 29*

sierpnia 1997 r., oraz 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, w skład której weszła Polityka Bezpieczeństwa oraz Instrukcja Zarządzania Systemem Informatycznym (...).
(...) Opracowane dokumenty zapewniały zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniknięcie Niemniej jednak w związku z planowanym wdrożeniem projektu „Nowoczesne usługi cyfrowe w Gminie Grunwald" zostanie w bieżącym roku wdrożony system w Urzędzie umożliwiający sprawniejsze załatwianie wszelkich spraw, poprzez zarządzanie dokumentami, korespondencją, poszczególnymi sprawami i posiadający wiele innych funkcjonalności."

Z powyższego wyjaśnienia oraz z przedstawionej do kontroli dokumentacji wynika, że w Urzędzie nie został opracowany odrębny dokument regulujący procedury w zakresie wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów w tym wpływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP). Brak przedmiotowych procedur stanowi uchybienie naruszające § 20 ust. 2 pkt 9 rozporządzenia KRI. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

[akta kontroli str. 356-368, 456-460]

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. 27-35]

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 ww. zadań 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. Dokument ten 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.

Zarządzeniem Nr 48/2008 Wójta Gminy Grunwald z dnia 31 grudnia 2008 r. wdrożono

w Urzędzie Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
Zarządzeniem Nr 1/2017 Wójta Gminy Grunwald z dnia 2 stycznia 2017 r. wprowadzono (w wyniku weryfikacji wcześniejszych aktów prawnych) Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym.
Zarządzenia wprowadzono zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. Nr 133, poz. 883 ze zm.), ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. Nr 11 poz. 95 ze zm.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku 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. z 2004 r. Nr 100, poz. 1024).
Powyższe stanowiło dokumentację przetwarzania danych osobowych w rozumieniu §1 pkt 1 rozporządzenia MSWiA z 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych (...). Służyła ona zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

[akta kontroli str. 417-437, 472-498]

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO", w Urzędzie dokonano weryfikacji dokumentacji systemu zarządzania bezpieczeństwem informacji i opracowano zarządzenie Nr 110/2019 Wójta Gminy Grunwald z dnia 12 grudnia 2019 r. r. w sprawie wprowadzenia Polityki Ochrony Danych.

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO", ustawy dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), w brzmieniu obowiązującym w tym okresie oraz rozporządzenia KRI. 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. Przedmiotowa dokumentacja weszła w życie w dniu 12 grudnia 2019 r.

W powyższym zakresie kontrolujący stwierdzili uchybienie polegające na przyjęciu dokumentu stanowiącego Politykę Ochrony Danych wraz z Instrukcją Zarządzania Systemem Informatycznym w Urzędzie (opracowane na podstawie RODO) dopiero w dniu 12 grudnia 2019 r., natomiast obowiązek stosowania RODO – to dzień 25 maja 2018 r. Z uzyskanego z Urzędu wyjaśnienia wynika, że cyt.: *„Zarządzeniem Wójta Gminy Grunwald nr 68/2014 z dnia 31 grudnia 2014 r. w sprawie wdrożenia kontroli zarządczej w Urzędzie Gminy oraz*

gminnych jednostkach organizacyjnych wprowadzono system kontroli zarządczej w Urzędzie Gminy Grunwald. Wprowadzona Kontrola zarządcza regulowała m.in. ochronę zasobów, w tym ochronę danych osobowych oraz ochronę danych w systemach informatycznych służących do przetwarzania danych osobowych. W Urzędzie funkcjonuje system informacji prawnej z dostępem dla każdego pracownika, w tym do informacji prawnej w zakresie obowiązującego RODO wraz z jego aktualizacją.
(...) Zarządzenie nr 11/2018 Wójta Gminy Grunwald z dnia 21 lutego 2018 r. wprowadzono zasady (polityki) rachunkowości która ma na celu przedstawienie obowiązujących zasad m.in.:
- *systemu służącego ochronie danych w jednostce, w tym: dokumentów stanowiących podstawę dokonywanych zapisów (zał. nr 4 do zarządzenia),*
- *opisu systemu przetwarzania danych - systemu informatycznego.*

Zarządzeniem nr 1/2017 Wójta Gminy Grunwald z dnia 2.01.2017 r. w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym w Urzędzie. W ocenie Organu w/w wskazane uregulowania, w tym zarządzenia jak również „Polityka Prywatności" (modyfikowana w 2018 r., 2019 r., i 2020 r.) oraz stosowane zabezpieczenia spełniały podstawowy cel określony w RODO – ochrona osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych umożliwiających realizację i egzekwowanie m.in. zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniknięcie.
Wprowadzona Polityka Ochrony Danych Osobowych w dniu 12 grudnia 2019 r. jest zbiorem wydanych wcześniej dokumentów w całość z przewołaniem Rozporządzenia Parlamentu Europejskiego Rady (UE) 2016/679, postanowienia określone w RODO na dzień 25 maja 2018 r. obowiązywały w Urzędzie w wielu rozproszonych dokumentach."

Odnosząc się do powyższych wyjaśnień należy zaznaczyć, że (jak już wspomniano na wstępie) Polityka Bezpieczeństwa Informacji jest podstawowym dokumentem Systemu Zarządzania Bezpieczeństwem Informacji w jednostce. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie i jako taka powinna być na bieżąco aktualizowana w trosce o zarządzanie bezpieczeństwem informacji zapewniającym poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Brak aktualizacji dokumentów wchodzących w skład SZBI stanowi uchybienie.
Skutkiem uchybienia był brak wymaganej aktualizacji Polityki zgodnie z § 20 ust. 1 i ust. 2 pkt 1 rozporządzenia KRI, jak również art. 24 ust. 1 i 2 RODO. Osobą odpowiedzialną jest IOD (pełniący funkcję w tym okresie) oraz Kierownik kontrolowanej jednostki.

[akta kontroli str. 317, 320-349, 456-460]

Od dnia 25 maja 2018 r. zaczęły obowiązywać nowe przepisy, tj. art. 37 ust 1 RODO, który przewidywał obowiązek wyznaczenia Inspektora Ochrony Danych dla administratorów

i podmiotów przetwarzających dane osobowe wówczas, gdy przetwarzania dokonują organ lub podmiot publiczny. Mając powyższe na uwadze Wójt Gminy Grunwald wyznaczył w jednostce Inspektora Ochrony Danych (IOD).

[akta kontroli str. 393-411, 461]

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 otrzymanego z Urzędu w przedmiotowej sprawie wynika, że cyt.: *(...) Pracownik zatrudniony w Urzędzie IOD* [redacted] *(jednocześnie informatyk w Urzędzie) odpowiedzialny za realizację zadania objętego kontrolą, przeprowadzał w sprawdzał i wykonywał przeglądy Infrastruktury IT Urzędu tj.: serwera, stacji roboczych i urządzeń sieciowych. W wyniku czynności nie wykryto istotnych nieprawidłowości (...).*"

Kontrolującym oprócz wyjaśnienia nie przedstawiono dowodów w postaci notatek lub protokołów świadczących o podjęciu i prowadzeniu działań w zakresie monitorowania i dokonywania przeglądów system zarządzania bezpieczeństwem informacji. Prowadzenie powyższych czynności powinno zostać udokumentowane, co w sposób niepodważalny świadczyłoby o spełnieniu ustawowego obowiązku. W związku z brakiem dowodów świadczących o realizacji i dokonywaniu przeglądów system zarządzania bezpieczeństwem informacji, powyższe ocenia się jako nieprawidłowość, która stanowi naruszenie § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

[akta kontroli str. 456-460]

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.

Z dokumentacji przedstawionej kontrolującym wynika, że wymóg wynikający z § 20 ust. 2 pkt 3 rozporządzenia KRI, spełniony został w 2020 r. Brak jest dokumentacji stwierdzającej przeprowadzenie analizy ryzyka w 2018 i 2019 r.
Z wyjaśnienia otrzymanego z Urzędu w przedmiotowej sprawie wynika, że cyt.: *„Pracownik zatrudniony w Urzędzie IOD* [redacted] *(jednocześnie informatyk w Urzędzie) odpowiedzialny za realizację zadania objętego kontrolą przeprowadził w 2018 r. i 2019 r. okresową analizę ryzyka utraty integralności, poufności dostępności oraz podejmował działania minimalizujące ryzyko, analizował wyniki (kontrolował zabezpieczenia serwerowni, stacji roboczych, poczty elektronicznej). Opisane w pkt.3 firmy również dokonywali analizy utraty integralności, poufności informacji oraz opieka autorska podejmowała działania minimalizujące ryzyko stosownie do wyników analizy."*

Kontrolującym oprócz wyjaśnienia nie przedstawiono dowodów w postaci przeprowadzonych analiz ryzyka świadczących o podjęciu działań w tym zakresie. Prowadzenie powyższych czynności powinno zostać udokumentowane, co w sposób niepodważalny świadczyłoby o spełnieniu ustawowego obowiązku. W związku z brakiem dowodów w zakresie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, powyższe ocenia się jako nieprawidłowość, która stanowi naruszenie § 20 ust. 2 pkt 3 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

[akta kontroli str. 261-289, 456-460]

Jednocześnie należy wskazać, iż w jednostce jest opracowany i prowadzony rejestr czynności przetwarzania danych osobowych.

[akta kontroli str. 80-83]

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. 185-247]

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 110/2019 Wójta Gminy Grunwald z dnia 12 grudnia 2019 r. r. w sprawie wprowadzenia Polityki Ochrony Danych.

[akta kontroli str. 320-349]

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).

[akta kontroli str. 311-316, 369-371]

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 trzech szkoleniach dotyczącym ochrony danych osobowych (25 luty 2019 – szkolenie prowadził radca prawny, 19 sierpnia 2019 – szkolenie prowadził IOD powołany w jednostce, 11 stycznia 2021 - szkolenie prowadził IOD - w formie wideokonferencji).

Należy zaznaczyć, że termin, rozpoczęcia stosowania RODO to 25 maja 2018 r., a pracownicy uczestniczący w procesie przetwarzania danych osobowych w Urzędzie przeszkoleni zostali pierwszy raz z tematyki bezpieczeństwa danych osobowych dopiero w dniu 25 lutego 2019 r. Z informacji przekazanej z Urzędu w powyższej sprawie wynika, że cyt.: *„Na mocy Zarządzenia Nr 30/2018 wydanego przez Wójta Gminy Grunwald z dniem 24 maja 2018 r. w Urzędzie Gminy Grunwald Pan* [redacted] *został powołany na Inspektora Danych Osobowych. W 2018 r. jak również w 2019 r. zatrudniony IOD prowadził szkolenia na stanowiskach pracy przy jednostkach roboczych z każdym pracownikiem odrębnie z tematyki RODO udzielając instruktarzu stanowiskowego."*

Kontrolującym wraz z udzielonym wyjaśnieniem nie przekazano dokumentacji świadczącej o prowadzonych innych szkoleniach. Tak późne przeprowadzenie szkoleń stanowi uchybienie. Skutkiem uchybienia było niedoinformowanie oraz brak wiedzy pracowników uczestniczących w procesie przetwarzania danych osobowych w zakresie nowych przepisów prawa regulujących powyższą tematykę (do dnia szkolenia). Osobą odpowiedzialną jest Inspektor Ochrony Danych Osobowych pełniący funkcję w tym okresie.

[akta kontroli str. 184, 456-460, 499]

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.*

W zarządzeniu Nr 110/2019 Wójta Gminy Grunwald z dnia 12 grudnia 2019 r. r. w sprawie wprowadzenia Polityki Ochrony Danych, opracowana została (rozdział 11.9) *Procedura pracy na odległość i mobilnego przetwarzania danych*, której stosowanie gwarantuje zachowanie bezpieczeństwa mobilnego przetwarzania danych w Urzędzie.
Z informacji uzyskanych z Urzędu wynika, że z uwagi na stacjonarny charakter i tryb pracy nie istniały przypadki przetwarzania danych osobowych na odległość.

[akta kontroli str. 320-349, 456-460]

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.

Procedura wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych ujęta została w zarządzeniu Nr 110/2019 Wójta Gminy Grunwald z dnia 12 grudnia 2019 r. r. w sprawie wprowadzenia Polityki Ochrony Danych – rozdział 13.2 str. 26
W Urzędzie użytkowany jest jeden system teleinformatyczny przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupiony u zewnętrznego dostawcy, tj.: [redacted] umowa licencyjna umożliwiająca prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu. Z [redacted] zawarta została również 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. 297-307, 456-460]

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 110/2019 Wójta Gminy Grunwald z dnia 12 grudnia 2019 r. r. w sprawie wprowadzenia Polityki Ochrony Danych – zał. Nr 16.

[akta kontroli str. 320-349, 381]

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 2018 r. do dnia rozpoczęcia czynności kontrolnych (17 grudnia 2020 r.), w jednostce przeprowadzono 2 zadania audytowe w zakresie bezpieczeństwa informacji, tj.:

- w 2019 r. certyfikat AC/1548/2019,
- w 2020 r. RAP/2020/KJ/10/51.

[akta kontroli str. 99-182]

Kontrolujący stwierdzili, że w 2018 r. nie przeprowadzono audytu wewnętrznego wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Powyższe stanowi nieprawidłowość.

Z wyjaśnienia Wójta Gminy w powyższej sprawie wynika, że cyt.: *„Pełny audyt wewnętrzny w zakresie bezpieczeństwa informacji nie został przeprowadzony w 2018 r. z uwagi na powołanie dopiero w maju 2018 r. Inspektora Danych Osobowych w tutejszej jednostce, niemniej jednak Pan* [redacted] *jako powołany IOD na mocy Zarządzenia Nr 30/2018 wydanego przez Wójta Gminy Grunwald z dniem 24 maja 2018 r. w Urzędzie Gminy Grunwald przeprowadzał działania wewnętrzne prowadzonego audytu:*

Rok 2018:

- zabezpieczenia komputerów,

- audyt Strony BIP pod kątem anonimizacji danych osobowych publikowanych na BIP.

- audyt zdalny strony internetowej Urzędu oraz strony BIP,

- audyt zabezpieczeń serwera.

- audyt poczty elektronicznej wszystkich pracowników."

[akta kontroli str. 456-460]

Odnosząc się do powyższego wyjaśnienia należy stwierdzić, że przeprowadzone przez IOD w Urzędzie „czynności sprawdzające" mogłyby jedynie w stopniu częściowym spełnić wymagania wynikające z § 20 ust. 1 KRI, który stanowi, że *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji* (...). Warunkiem spełnienia powyższego jest udokumentowanie prowadzenia czynności w postaci protokołów lub notatek służbowych. Kontrolującym oprócz wyjaśnienia nie przedstawiono dowodów

świadczących o realizacji opisanych działań.
Opisane w wyjaśnieniach działania nie spełniają jednak wymogów § 20 ust. 2 pkt 14 rozporządzenia KRI, które stanowi, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.* Brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

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.

Zasady tworzenia kopii zapasowych uregulowane zostały zarządzeniem Nr 110/2019 Wójta Gminy Grunwald z dnia 12 grudnia 2019 r. r. w sprawie wprowadzenia Polityki Ochrony Danych – rozdział 11.3.

[akta kontroli str. 320-349]

Ponadto z wyjaśnienia przekazanego z Urzędu w powyższej sprawie wynik, iż, cyt.: „[redacted] *(...).”*

[akta kontroli str. 183, 248]

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]".

[akta kontroli str. 183]

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, w odległości niezbędnej do uniknięcia uszkodzeń spowodowanych przez katastrofę, która dotknęłaby podstawowy ośrodek przetwarzania danych.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 15 ust. 1 rozporządzenia KRI *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.*

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej dzieliły się na systemy centralne tj. ŹRÓDŁO i CEiDG oraz system wspierający zakupiony u dostawcy zewnętrznego – PUMA. Na obsługę aktualnie zainstalowanego oprogramowania z firmą dostarczającą dany system informatyczny zawarta została stosowna umowa licencyjna (opieka autorska), gwarantująca 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. 302-304]

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 do nich dostępu przez uprawnionych użytkowników stosowany jest szereg zabezpieczeń informatycznych. 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, zastosowano następujące zabezpieczenia:

[redacted]

[akta kontroli str. 467-471]

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:

- w systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe,
- w systemie: PUMA, logowanie odbywa się za pomocą przyznanego loginu i hasła, które wymaga okresowej wymiany,
- w systemie CEIDG logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła.

Ponadto zgodnie z dokumentacja uzyskaną w trakcie kontroli, *na każdej stacji roboczej zainstalowane jest oprogramowanie* [redacted].

[akta kontroli str. 249, 467-471]

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.*

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. 467-471]

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 zmianę wielkości czcionki oraz kontrastu w celu ułatwienia korzystania z treści na niej zawartych przez osoby niedowidzące. 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. Urzędu **nie wykazała błędów**.

[akta kontroli str. 448-451]

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. Każdorazową terminową aktualizację dokumentacji SZBI zgodnie z § 20 ust. 1 i ust. 2 pkt 1 rozporządzenia KRI, jak również art. 24 ust. 1 i 2 RODO.
3. Zgodnie z § 20 ust. 1 rozporządzenia KRI monitorowanie i dokonywanie cyklicznych przeglądów systemu zarządzania bezpieczeństwem informacji, w celu jego doskonalenia i utrzymywania go na odpowiednio wysokim poziomie.
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 zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.

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

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

WOJEWODA
WARMIŃSKO-MAZURSKI

Artur Chojecki