WOJEWODA MAZOWIECKI

Warszawa, 23 kwietnia 2024 r.

WK-I.431.2.3.2023

Pani
Elżbieta Sadowska
Starosta Sokołowski

Starostwo Powiatowe
w Sokołowie Podlaskim
ul. Wolności 23
08-300 Sokołów Podlaski

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 28 ust. 1 pkt 2 ustawy o wojewodzie i administracji rządowej w województwie[1], art. 6 ust. 4 pkt. 3 ustawy o kontroli w administracji rządowej[2] oraz art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[3], kontrolerzy: Iwona Parys – starszy inspektor wojewódzki oraz Paulina Domagała – inspektor wojewódzki w Oddziale Kontroli Jednostek Samorządu Terytorialnego Wydziału Kontroli, a także Łukasz Plaskot – kierownik Oddziału Serwisu Informatycznego oraz Mariusz Zmuda – specjalista w Oddziale Serwisu Informatycznego w Biurze Informatyki Mazowieckiego Urzędu Wojewódzkiego w Warszawie, przeprowadzili w dniach od 28 grudnia 2023 r. do 16 lutego 2024 r. kontrolę problemową w Starostwie Powiatowym w Sokołowie Podlaskim (dalej Starostwo).

Przedmiot kontroli obejmował realizację zadań w zakresie działania systemów teleinformatycznych używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących

[1] Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2023 r. poz. 190).
[2] Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224).
[3] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307).

zadania publiczne pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej[4] – w okresie od 1 stycznia 2023 r. do 20 grudnia 2023 r.

Nawiązując do projektu wystąpienia pokontrolnego z 26 marca 2024 r., do którego nie wniesiono zastrzeżeń, przekazuję wystąpienie pokontrolne.

Ocenie poddano trzy główne obszary kontroli, tj. wymianę informacji w postaci elektronicznej, w tym współpracę z innymi systemami informatycznymi oraz wspomaganie usług drogą elektroniczną, zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych oraz zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych.

Kontroli poddano system teleinformatyczny XXXXXX używany w Starostwie do realizacji zadań zleconych z zakresu administracji rządowej, przy pomocy którego prowadzona jest XXXXXXXX stanowiąca rejestr publiczny, o którym mowa w art. 3 pkt 5 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

I. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami (rejestrami) teleinformatycznymi oraz wspomaganie usług drogą elektroniczną.

Starostwo udostępnia elektroniczną skrzynkę podawczą (dalej ESP) umożliwiającą doręczanie pism w formie dokumentów elektronicznych.

Na stronie internetowej Starostwa, w ramach której w oddzielnej zakładce prowadzony jest również Biuletyn Informacji Publicznej (dalej BIP), poinformowano o adresie skrzynki podawczej podanym w formie identyfikatora URI, zgodnie z § 3 ust. 1 pkt 1 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[5]. Starostwo umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw w formatach

---

[4] Zgodnie z art. 25 ust. 3 przedmiotowej ustawy kontrola dotyczyła wyłącznie systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej.

[5] Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. z 2018 r. poz. 180).

danych określonych w załączniku nr 2 rozporządzenia w sprawie KRI[6,7].

Na stronie internetowej Starostwa wskazano na możliwość złożenia 2 wniosków[8] w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym za pomocą elektronicznej skrzynki podawczej ePUAP. W zakładce *Załatw sprawę → Załatw sprawę w Urzędzie*, po wybraniu Wydziału Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami Starostwa, a następnie poszczególnych spraw – następuje przekierowanie do strony, na której zamieszczono wzór wniosku w postaci pliku PDF z możliwością jego pobrania oraz zamieszczono informacje o podstawie prawnej, wymaganych dokumentach, opłatach, miejscu i sposobie złożenia wniosku, terminie załatwienia sprawy, trybie odwoławczym.

Ustalono, że Starostwo nie przekazywało wzorów dokumentów elektronicznych do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, jak również nie korzysta z zasobów ww. repozytorium.

W rejestrze prowadzonym za pomocą programu XXXXXX Starostwo stosuje odwołania do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań, zgodnie z § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI oraz wyposażył ww. system teleinformatyczny w składniki umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanawianych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną UE, zgodnie z § 16 ust. 1 rozporządzenia w sprawie KRI oraz formatach danych określonych w załączniku nr 2 i 3 rozporządzenia w sprawie KRI[9].

Ustalono, że w Starostwie obowiązuje jako podstawowy tradycyjny system obiegu dokumentów, a funkcjonujący system XXXXXXX pełni funkcje wspomagające wykonywanie czynności kancelaryjnych w systemie tradycyjnym[10].

---

6 Zgodnie z pisemnym wyjaśnieniem Starosty Sokołowskiego.

7 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).

8 Dotyczy wniosku o dostęp do Geoportalu oraz wniosku w sprawie zgłoszenia zmiany danych objętych ewidencją gruntów i budynków.

9 Zgodnie z pisemnymi z wyjaśnieniami Starosty Sokołowskiego.

10 Kontrolującym przedłożono Zarządzenie nr 20/2012 Starosty Sokołowskiego z dnia 31 sierpnia 2012 r. w sprawie wprowadzenia instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt i instrukcji w sprawie organizacji i działania archiwum zakładowego.
Zgodnie z pisemnymi z wyjaśnieniami Starosty Sokołowskiego w systemie XXXXXX: *„Nadane użytkownikom uprawnienia nie pozwalają na XXXXXXX”.*

W wyniku kontroli stwierdzono nieprawidłowość polegającą na braku udokumentowanych procedur dotyczących dostarczania usług realizowanych przez systemy teleinformatyczne na deklarowanym poziomie dostępności[11], co jest niezgodne z § 15 ust. 2 rozporządzenia w sprawie KRI, zgodnie z którym: *„Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury”*.

Ponadto stwierdzono, że na stronie internetowej Starostwa, w ramach której w oddzielnej zakładce prowadzony jest również BIP Starostwa, nie zamieszczono informacji określonych w § 3 ust. 1 pkt 2, 4 i 5 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępnia formularzy, wzorów i kopii dokumentów elektronicznych, zgodnie z którym: *„Podmioty publiczne informują na swoich stronach podmiotowych (...), o: 2) maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż 5 megabajtów; (...) 4) rodzajach informatycznych nośników danych, na których może zostać im doręczony dokument elektroniczny; 5) rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru”.*

Przedstawiając powyższe informuję, że realizację zadań dotyczących wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami (rejestrami) teleinformatycznymi oraz wspomagania usług drogą elektroniczną ocenia się **pozytywnie pomimo stwierdzonych nieprawidłowości.**

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

Na funkcjonujący w Starostwie w okresie kontrolowanym system zarządzania bezpieczeństwem informacji składały się udokumentowane procedury określone w drodze zarządzeń Starosty Sokołowskiego, którymi ustanowione zostały:

1) *System Zarządzania Bezpieczeństwem Informacji*[12], w skład którego wchodzą: XXXXXX;

---

[11] Zgodnie z pisemnymi wyjaśnieniami Starosty Sokołowskiego: *„Starostwo nie posiada procedur wewnętrznych, w których określono jaki ma być deklarowany poziom dostępności usług realizowanych przez systemy informatyczne.”*

[12] Ustanowiony Zarządzeniem XXXXXXXXXXX.

2) *Polityka Bezpieczeństwa Przetwarzania Danych Osobowych*[13];
3) *Procedura Pracy Zdalnej z Zasadami przetwarzania danych osobowych przez pracownika w trakcie wykonywania pracy zdalnej*[14].

Ustalono, że pracownicy nowo zatrudnieni[15] w okresie kontrolowanym potwierdzili zapoznanie się z *Polityką Bezpieczeństwa Przetwarzania Danych Osobowych* oraz *Regulaminem Pracy.*

W okresie kontrolowanym przeprowadzone zostały audyty, które służyć mogą doskonaleniu systemu zarządzania bezpieczeństwem informacji oraz aktualizacji regulacji wewnętrznych dotyczących bezpieczeństwa informacji[16] w myśl wymogów § 20 ust. 1 i ust. 2 pkt 1 rozporządzenia w sprawie KRI. Organ podjął także działania[17] w celu opracowania i ustanowienia XXXXXXXXXXXXXXX dokumentacji systemu zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 ww. rozporządzenia.

W związku z wymogiem określonym w § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI stwierdzono, że w okresie kontrolowanym przeprowadzono – z uwzględnieniem takich atrybutów, jak integralność, dostępność i poufność informacji – analizę ryzyka w obszarze danych osobowych[18]. W jej wyniku powstał rejestr ryzyka w przedmiotowym obszarze z proponowanymi działaniami minimalizującymi ryzyko.

Starostwo utrzymuje aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, prowadząc w formie elektronicznej rejestr zasobów teleinformatycznych, zawierający informację o zmianach konfiguracji aktywów informatycznych[19], zgodnie z wymogiem określonym w § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI.

Zgodnie z wyjaśnieniem pisemnym Starosty Sokołowskiego ww. dokument został opracowany w oparciu o Polską Normę PN-ISO/IEC 27001 i stanowi XXXXXX dokumentacji składającej się na system zarządzania bezpieczeństwem informacji – *„Aktualnie opracowana została XXXXXXXXX (...) Trwają prace nad XXXXXXXXX w ramach projektu złożonego w ramach programu Cyberbezpieczny samorząd.”*.

13 Ustanowiona Zarządzeniem XXXXXXXXX.

14 Stanowiąca załącznik do *XXXXXX,* ustanowionego Zarządzeniem XXXXXXXXX

15 Dotyczy 11 osób wskazanych jako nowo zatrudnione w okresie kontrolowanym (próba nie obejmowała osób, które rozpoczęły w tym okresie staż).

16 Dotyczy w szczególności:
1) audytu realizacji wymagań Krajowych Ram Interoperacyjności w kontekście normy ISO/IEC 27001, w związku z którym przeprowadzono także badanie podatności zasobów informatycznych,
2) audytu w obszarze kryptografii, przeprowadzonego w oparciu o normę ISO 27001 oraz rozporządzenie w sprawie KRI.

17 Dotyczy złożenia w okresie kontrolowanym projektu do konkursu grantowego *„Cyberbezpieczny Samorząd”*, w ramach którego – zgodnie z wyjaśnieniem Starosty Sokołowskiego – planowane jest XXXXXXXXXXX.

18 Dotyczy analizy przeprowadzonej przez Inspektora Ochrony Danych, uwzględniającej takie aktywa, jak: XXXXXXXXXX. Zgodnie z wyjaśnieniem pisemnym Starosty Sokołowskiego *„IOD realizuje szacowanie ryzyka obejmującego przede wszystkim obszar ochrony danych, jednak zawiera ono elementy (...) analizy ryzyka utraty integralności, dostępności lub poufności informacji.”*.

19 Rejestr prowadzony przy pomocy oprogramowania XXXXXXXXX.

Udokumentowane zostały[20] procedury w zakresie zarządzania uprawnieniami użytkowników systemu informatycznego Starostwa, stwarzające warunki umożliwiające realizację i egzekwowanie działań, o których mowa w § 20 ust. 2 pkt 4 i 5 rozporządzenia w sprawie KRI. Nadawanie oraz odbieranie uprawnień do systemu teleinformatycznego odbywało się w okresie kontrolowanym zgodnie z ustalonymi procedurami, tj. na pisemny wniosek przełożonego, który określał zakres niezbędnych do pracy uprawnień. Stwierdzono, że zakresy czynności losowo wybranych pracowników[21], którym przyznano dostęp do systemu XXXXXX, obejmują zadania, w realizacji których może być wykorzystywana XXXXXXXX[22]. Osobom, które zakończyły w okresie kontrolowanym pracę w Starostwie[23] dostęp do systemu informatycznego Starostwa odebrany został niezwłocznie[24].

W związku z wymogiem określonym w § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI osobom zaangażowanym w proces przetwarzania informacji zapewnione zostało w okresie kontrolowanym 1 szkolenie obejmujące głównie obszar ochrony danych osobowych[25].

Ustanowione zostały zasady[26] mające na celu zagwarantowanie bezpiecznej pracy przy przetwarzaniu informacji z wykorzystaniem urządzeń przenośnych i pracy na odległość, w myśl wymogu określonego w § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI.

W związku z wymogiem określonym w § 20 ust. 2 pkt 13 rozporządzenia w sprawie KRI – stwierdzono udokumentowanie procedur zgłaszania naruszeń bezpieczeństwa informacji przez Administratora Systemów Informatycznych[27] oraz niezwłocznego zgłaszania zdarzeń mogących stanowić naruszenie ochrony danych osobowych[28]. W okresie kontrolowanym nie zostały zgłoszone incydenty naruszenia bezpieczeństwa informacji.

Spełniony został, określony w § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI, wymóg zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

---

[20] Dotyczy dokumentów: XXXXXXXXX.

[21] Dotyczy 6 pracowników Wydziału XXXXXXXXXXX.

[22] Pracownikom tym udzielono upoważnień do przetwarzania danych osobowych w ramach realizowanych zadań.

[23] Dotyczy 10 osób.

[24] Dotyczy dostępu do domeny, który odebrany został w badanych przypadkach z dniem zakończenia pracy lub z dniem kolejnym, a w 1 przypadku – 2. dnia roboczego, co ustalono – wobec nieprzedstawienia innych dowodów – na podstawie adnotacji dokonanych przez Administratora Systemu Informatycznego na wnioskach w tym zakresie. Przedmiotowe ustalenie nie dotyczy dostępu do XXXXXXXXXX.

[25] Program szkolenia obejmował m.in. zasady bezpiecznej pracy z danymi osobowymi, zasadę *„czystego”* biurka i ekranu, bezpieczeństwo fizyczne, bezpieczeństwo komputerów przenośnych i nośników, podstawowe metody ataków cyberprzestępców i sposoby postępowania w przypadku próby wyłudzenia danych.

[26] Dotyczy dokumentów: XXXXXXXXXXX.

[27] Dotyczy dokumentu: XXXXXX.

[28] Dotyczy dokumentu: XXXXXX.

W okresie poddanym kontroli przeprowadzony został audyt w obszarze kryptografii[29] oraz audyt realizacji wymagań Krajowych Ram Interoperacyjności w zakresie procesów związanych z zarządzaniem organizacją w zakresie bezpieczeństwa informacji oraz bezpieczeństwa systemów teleinformatycznych[30]. Stwierdzono także przeprowadzenie czynności sprawdzających wykonania zaleceń z audytu przeprowadzonego w obszarze bezpieczeństwa informacji w roku poprzednim[31].

W Starostwie udokumentowane zostały procedury odnoszące się do wykonywania i odtwarzania kopii zapasowych[32] oraz podejmowano działania związane z wykonywaniem i przechowywaniem kopii zapasowych, w związku z wymogiem minimalizowania ryzyka utraty informacji w wyniku awarii, określonym w § 20 ust. 2 pkt 12 lit. b rozporządzenia w sprawie KRI. W okresie kontrolowanym w każdym przypadku zaistnienia konieczności odtworzenia danych z kopii zapasowych został złożony stosowny wniosek oraz sporządzony raport z odzyskania danych, zgodnie z ustalonymi w jednostce procedurami.

W związku z wymogiem zapewnienia ochrony informacji i środków jej przetwarzania, określonym w § 20 ust. 2 pkt 7, 9, 11 i 12 rozporządzenia w sprawie KRI, Starostwo stosuje rozwiązania służące ochronie przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem oraz ochronie środków przetwarzania informacji, jak również rozwiązania służące zachowaniu bezpieczeństwa w systemach teleinformatycznych, w tym: środki ochrony fizycznej budynków i pomieszczeń, wyznaczenie pomieszczeń z ograniczonym dostępem[33], ustanowienie zasad monitorowania zasobów sprzętowych i aplikacyjnych oraz aktywności użytkowników w systemie informatycznym, systemach operacyjnych i bazach danych, stosowanie haseł przez użytkowników systemu informatycznego i nadawanie im uprawnień do zasobów tego systemu, tworzenie kopii zapasowych, automatyczne sprawdzanie dostępności poprawek systemów operacyjnych serwerów i dokonywanie aktualizacji pod kontrolą administratora, stale aktualizowany system antywirusowy, stosowanie zapory

---

[29] Audyt przeprowadzony w ramach umowy zlecenia przez Audytora Wewnętrznego w oparciu o normę ISO/IEC 27001 i rozporządzenie w sprawie KRI. Audyt objął ocenę działań w zakresie kryptografii pod kątem zapewnienia bezpieczeństwa systemów informacyjnych.

[30] Audyt przeprowadzony przez podmiot zewnętrzny na podstawie zawartej umowy o pełnienie funkcji Inspektora Ochrony Danych, w której zawarto zobowiązanie do przeprowadzenia w zakresie ochrony danych osobowych XXXXXX. Zgodnie z wyjaśnieniem Starosty Sokołowskiego – *„Audyt wykonany został przez firmę zewnętrzną ale (...) klasyfikowany powinien być jako audyt wewnętrzny w formie usługi outsourcingowej.”*. Audyt przeprowadzony został w oparciu o normę ISO/IEC 27001.

[31] Dotyczy audytu: *Bezpieczeństwo zasobów ludzkich,* przeprowadzonego przez Audytora Wewnętrznego w 2022 r.

[32] Dotyczy: XXXXXX.

[33] W tym XXXXXX.

sieciowej i zasilania awaryjnego[34] czy przeprowadzenie badania podatności systemu informatycznego.

W okresie objętym kontrolą nie wystąpiły przypadki projektowania i wdrażania systemów teleinformatycznych, wobec czego spełnienie warunków określonych w § 15 ust. 1 rozporządzenia w sprawie KRI nie było przedmiotem kontroli.

Stwierdzono, że rozliczalność działań poszczególnych użytkowników systemu XXXXX w zakresie XXXXXXX z prowadzonego rejestru publicznego zapewniona jest poprzez generowanie na wydawanych XXXXXXXXXX danych personalnych osoby, która dokonała operacji w tym zakresie[35].

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Nieudokumentowanie procedur wewnętrznych w zakresie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji[36], pomimo wymogu określonego w § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI, zgodnie z którym *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie (...) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji (...)”*. W okresie kontrolowanym analiza ryzyka z uwzględnieniem powyższych atrybutów udokumentowana została w obszarze ograniczonym do danych osobowych[37].
2. Niestworzenie warunków umożliwiających egzekwowanie zapewnienia wymaganego

---

[34] Dotyczy XXXXXX.

[35] Nie została przedstawiona do kontroli przykładowa dokumentacja w postaci elektronicznych zapisów w dzienniku XXXXXXX. Starosta Sokołowski nie wskazał:
- jakie działania użytkowników są odnotowywane w postaci logów – *„Nie jesteśmy w stanie wygenerować tego rodzaju danych. Możliwe jest to z pozycji producenta oprogramowania.”,*
- ile czasu przechowywane są logi – *„W tej kwestii może wypowiedzieć się producent oprogramowania.”.*

Wobec powyższego nie jest w pełni możliwe wypowiedzenie się w zakresie zapewnienia rozliczalności ww. systemu, o której mowa w § 21 ust. 1 i 2 rozporządzenia w sprawie KRI.

[36] Zgodnie z wyjaśnieniem pisemnym Starosty Sokołowskiego – *„Trwają prace XXXXXXXX.*

[37] Do analiz, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI nie zaliczono innych analiz ryzyka, które przeprowadzone zostały w okresie kontrolowanym, tj.:
- analizy ryzyka przeprowadzonej w ramach kontroli zarządczej (ze stanowiącego jej udokumentowanie *Rejestru ryzyka na 2023 r.* nie wynika czy analiza została dokonana z uwzględnieniem takich atrybutów, jak integralność, dostępność i poufność informacji, a zgodnie z ustanowionym zarządzeniem Nr 50/2020 Starosty Sokołowskiego z 2 października 2020 r. *Regulaminem kontroli zarządczej w Starostwie Powiatowym w Sokołowie Podlaskim* – podczas identyfikacji ryzyka stosowana jest następująca kategoryzacja: XXXXXXXX),
- analizy ryzyka przeprowadzonej na potrzeby opracowania planu audytu wewnętrznego na 2024 r. oraz analizy ryzyka przeprowadzonej w ramach przeglądu wstępnego audytu w obszarze kryptografii (zgodnie z XXXXXXXXX przeprowadzana na jej podstawie analiza ryzyka uwzględnia takie kryteria ryzyka, jak: XXXXXXXXXXX).

szkolenia dla osób zaangażowanych w proces przetwarzania informacji, pomimo wymogu określonego w § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI, zgodnie z którym *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających (...) egzekwowanie (...) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:* (…) *zagrożenia bezpieczeństwa informacji, (...) skutki naruszeń zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, (...) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich*". Szkolenie przeprowadzone w okresie kontrolowanym ograniczone było co do zasady do obszaru danych osobowych[38], którego program nie obejmował części ww. problematyki[39].

3. Niepodjęcie działań mających na celu zagwarantowanie umową odpowiedniego poziomu bezpieczeństwa informacji w związku z serwisowaniem systemu XXXXXX przez podmiot zewnętrzny[40], pomimo że zgodnie z § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI – *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie (...) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji".*
4. Przechowywanie informacji w dziennikach systemów (logów) przez okres krótszy niż 2 lata, czym naruszono postanowienia § 21 ust. 4 rozporządzenia w sprawie KRI, zgodnie z którym *„Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez*

---

[38] Wymóg organizowania co najmniej raz w roku szkolenia z zakresu ochrony danych osobowych określono w XXXXXXXXXX.

[39] Z programu szkolenia nie wynika, czy obejmował on skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawną, czy stosowanie urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich. Także zgodnie z przeprowadzoną w okresie kontrolowanym *Oceną zgodności z KRI* – jednostka nie przedstawiła audytorowi dokumentów *„potwierdzających wykonywanie szkoleń pracowników i administratorów w rozumieniu KRI"*.

[40] Dotyczy XXXXXXXXX, który zgodnie z XXXXXXX jest jednym z serwisantów *„systemów dziedzinowych w Starostwie".* Organ nie dysponuje żadną formą umowy, która regulowałaby powyższe kwestie. Okazane licencje na korzystanie z ww. systemu nie zawierają zapisów, które uznać można za gwarantujące odpowiedni poziom bezpieczeństwa informacji w związku z usługami serwisowymi świadczonymi przez licencjodawcę, stanowiąc że wszelkie usługi związane z oprogramowaniem będą dokonywane na podstawie odrębnych zleceń. Zgodnie z wyjaśnieniami pisemnymi Starosty Sokołowskiego – w kontrolowanym okresie nie zawierano pisemnych zleceń serwisu tego oprogramowania, problemy zgłaszane są licencjodawcy telefonicznie. XXXXXXX, zawierająca postanowienia dotyczące zarządzania licencjami, nie ustanawia procedur w przedmiotowym zakresie.

okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata"[41].

Ponadto w wyniku kontroli ustalono, że:

a) nie zapewniono rozliczalności w zakresie zapoznawania nowo zatrudnionych pracowników[42] z dokumentacją składającą się na ustanowiony *System Zarządzania Bezpieczeństwem Informacji*[43] w ramach jego wdrażania, o którym mowa w § 20 ust. 1 rozporządzenia w sprawie KRI, co utrudniać może egzekwowanie stosowania procedur mających gwarantować odpowiedni poziom bezpieczeństwa informacji;

b) w przypadku 1 osoby, której miejsce zatrudnienia w Starostwie uległo w okresie kontrolowanym zmianie[44] – nie zastosowano procedury określonej XXXXXXX[45], zgodnie z którą: *„W przypadku (...) zmiany komórki organizacyjnej przełożony użytkownika zobowiązany jest złożyć nowy wniosek w celu weryfikacji lub zmiany uprawnień oraz aktualizacji danych w systemie. W przypadku niedostarczenia wniosku konto zostanie zablokowane"*[46]. Ponadto 1 osoba posiada dostęp do systemu XXXXXXXX, pomimo że jedyny okazany wniosek, na podstawie którego dostęp został jej nadany dotyczył nadania uprawnień na czas określony – do XXXXXX[47], a zgodnie z ustanowionymi w jednostce procedurami nadawanie uprawnień odbywa się na podstawie wniosku pisemnego;

c) w 6 przypadkach dostęp do jednego z systemów dziedzinowych[48] został zablokowany w okresie od 4 miesięcy do ponad roku od dnia zakończenia pracy w Starostwie przez

---

[41] Zgodnie z wyjaśnieniem pisemnym Starosty Sokołowskiego – *„XXXXXXX pozwalają Starostwu na przechowywanie kopii serwerów wraz z ewentualnymi logami przez okres XXXXXXXX".*

[42] Dotyczy okresu poddanego kontroli.

[43] Zgodnie z pisemnym wyjaśnieniem Starosty Sokołowskiego – *„pracownicy zapoznają się (...) we własnym zakresie"* z *Systemem Zarządzania Bezpieczeństwem Informacji* – osobom rozpoczynającym pracę przekazywane są do zapoznania się *„wszelkie instrukcje/regulaminy i procedury (...) w wersji papierowej, a także udostępniane na XXXXXXXX"*. Z wyjaśnień oraz ustaleń kontroli wynika, że pracownicy nowo zatrudnieni nie potwierdzali zapoznania się z *Systemem Zarządzania Bezpieczeństwem Informacji* w jakiejkolwiek formie.

[44] Dotyczy osoby zatrudnionej pierwotnie na czas określony w Wydziale XXXXXX, dla której przyznany został na czas nieokreślony dostęp do dysku sieciowego tej komórki organizacyjnej oraz systemów dziedzinowych z zakresu XXXXXXX. Z dniem kolejnym po ustaniu ww. zatrudnienia osoba ta została zatrudniona w Wydziale XXXXXXXX. Zgodnie z wyjaśnieniem pisemnym Starosty Sokołowskiego – po miesiącu osoba ta została oddelegowana do Wydziału XXXXXXXX, a *„Aktualnie stanowi wsparcie również tego wydziału."*.

[45] Dokument składający się na przyjęty *System Zarządzania Bezpieczeństwem Informacji*.

[46] Zgodnie z wyjaśnieniami Starosty Sokołowskiego – uprawnienia do systemu informatycznego pracownika *„nie zostały zmienione, ponieważ pracodawca planował docelowo przeniesienie pracownika do Wydziału XXXXXXXXXX"*, a *„W trakcie pracy w Wydziale XXXXXXXXX zlecane były pracownikowi różnego rodzaju czynności przez kierownika Wydziału XXXXXXX".*

[47] Zgodnie z wyjaśnieniem pisemnym Starosty Sokołowskiego – „*uprawnienia* [tej osoby] *nie uległy zmianie. Zaistniała sytuacja spowodowana jest złym sformułowaniem wniosku, który (...) planujemy zmienić podczas XXXXXXXX*."

[48] Dotyczy systemu XXXXXX.

osoby, którym został on przyznany, tj. w trakcie trwania niniejszej kontroli, co skutkowało brakiem aktualności posiadanych danych w zakresie faktycznej liczby użytkowników tego systemu[49];

d) występują różnice w procedurach nadawania i odbierania uprawnień do systemu informatycznego, które ustanowione zostały zarówno XXXXXXXX, jak i *XXXXXXXX*, w tym w zakresie obowiązujących wzorów wniosków[50];

e) nie wykonywano okresowych testów odtworzeniowych kopii systemów, a kopie zapasowe przechowywano XXXXXXX[51], co ocenia się jako działanie niedostatecznie minimalizujące możliwość utraty informacji w wyniku awarii, w związku z wymogiem określonym w § 20 ust. 2 pkt 12 lit. b rozporządzenia w sprawie KRI.

Ponadto XXXXXXX XXXXXXX[52] XXXXXXXXXXXX[53], w związku z wymogami określonymi w § 20 ust. 2 pkt 7 i 9 rozporządzenia w sprawie KRI.

Stwierdzono także, że w okresie kontrolowanym nie stosowano niektórych wewnętrznych procedur określonych XXXXXXXX*[54]* oraz *XXXXXXXXXX*[55].

---

[49] Zgodnie z wyjaśnieniem pisemnym Starosty Sokołowskiego na ww. okoliczność – *„W pierwszej kolejności odbierany jest dostęp do domeny (...) Użytkownik i tak nie mógłby korzystać z jakiejkolwiek aplikacji jeżeli ma zablokowany dostęp do domeny.”*.

[50] Zgodnie z wyjaśnieniem pisemnym Starosty Sokołowskiego: *„jesteśmy cały czas w fazie prac XXXXXXX stąd niektóre XXXXXXX mogą mieć jeszcze rozbieżności.”*.

[51] Zgodnie z protokołem z przeprowadzonej w dniu 26 stycznia 2024 r. rozmowy z administratorem systemu informatycznego Starostwa: „*Kopie bezpieczeństwa serwerów (...) wykonywane są XXXXXXX. (...) Okresowe testy odtworzeniowe XXXXXXXXX”*.

[52] Dotyczy XXXXXXX.

[53] XXXXXXX.

[54] Dotyczy okresowych przeglądów realizacji wniosków o nadanie lub odebranie uprawnień do zasobów Starostwa oraz uprawnień w systemie zdalnego dostępu VPN, dokumentowania protokołem XXXXXXX oraz przeglądu XXXXXXXXXX. Zgodnie z ww. dokumentem *„XXXXXXX”*, sporządzając, odpowiednio: XXXXXX.
Odnosząc się do powyższego, Starosta Sokołowski wskazał w wyjaśnieniach pisemnych, że:
- *„Żadna zmiana uprawnień nie jest realizowana bez akceptacji XXXXXXXXXX”,*
- *„XXXXXXX są zabezpieczone i nie mają do nich dostępu osoby postronne. Przeglądy są dokonywane regularnie. XXXXXXXXX”,*
- *„Program XXXXXXXXXX monitoruje w czasie rzeczywistym stacje robocze i serwery (...) Zgodnie z aktualnie wdrożonymi zabezpieczeniami nie ma możliwości nieuprawnionego dostępu do systemu i we własnym zakresie instalowania jakiegokolwiek oprogramowania naruszającego bezpieczeństwo. Dodatkowym wsparciem jest oprogramowanie XXXXXXXX.”,*
- *„Uprawnienia VPN są przyznawane na czas określony i po jego zakończeniu są odbierane. Nie ma użytkowników którzy posiadają aktywny VPN.”*.

[55] Dotyczy wykazów osób uprawnionych do otwierania budynków oraz wyznaczenia osoby odpowiedzialnej za zabezpieczenie fizyczne pomieszczeń stanowiących obszar przetwarzania danych. Zgodnie z ww. dokumentem: *„XXXXXXXXX”*.
Odnosząc się do powyższego Starosta Sokołowski wskazał w wyjaśnieniach pisemnych, że osoba taka nie została wyznaczona, a *„XXXXXX.”*

Przedstawiając powyższe informuję, że realizację zadań w zakresie działania systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych ocenia się **pozytywnie pomimo stwierdzonych nieprawidłowości.**

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

W związku z wymogiem określonym w § 19 rozporządzenia w sprawie KRI - stronę internetową Starostwa działającą pod adresem: https://samorzad.gov.pl/web/powiat-sokolowski wraz zakładką Biuletynu Informacji Publicznej Starostwa: https://samorzad.gov.pl/web/powiat-sokolowski/mapa-strony?show-bip=true poddano weryfikacji zgodności ze standardem WCAG 2.0 za pomocą walidatorów http://validator.w3.org oraz http://jigsaw.w3.org/css-validator/.

Przeprowadzona przez kontrolujących w dniu 22 stycznia 2024 r. walidacja ww. stron wykazała przypadki błędów, ostrzeżeń i komunikatów informacyjnych[56], przy czym nie stwierdzono, aby miały one wpływ na prezentowane treści[57].

Powyższe strony internetowe spełniają wymagania WCAG 2.0 określone w załączniku nr 4 rozporządzenia w sprawie KRI. W wyniku kontroli stwierdzono, że dostępna strona internetowa wraz z zakładką Biuletynu Informacji Publicznej Starostwa – zawierają rozwiązania techniczne umożliwiające osobom niepełnosprawnym zapoznanie się z treścią informacji. Starostwo zamieściło na swojej stronie internetowej deklarację dostępności, zgodnie z którą ww. strona umożliwia korzystnie ze standardowych skrótów klawiaturowych oraz przeglądanie treści na urządzeniach mobilnych. Ponadto poinformowano o możliwości wystąpienia z żądaniem zapewnienia dostępności cyfrowej strony internetowej, aplikacji mobilnej lub jakiegoś ich elementu, a także możliwości udostępnienia informacji w formach alternatywnych, jeżeli zapewnienie dostępności nie jest możliwe. W Starostwie powołano

---

[56] Dla walidatora https://validator.w3.org/:
- dla strony: https://samorzad.gov.pl/web/powiat-sokolowski – XXXXXXXX,
- dla strony BIP: https://samorzad.gov.pl/web/powiat-sokolowski/mapa-strony?show-bip=true – XXXXXX;

zaś dla walidatora http://jigsaw.w3.org/css-validator:
- dla strony: https://samorzad.gov.pl/web/powiat-sokolowski – XXXXXXXX,
- dla strony BIP: https://samorzad.gov.pl/web/powiat-sokolowski/mapa-strony?show-bip=true – XXXXXX.

[57] Zgodnie z pisemnym wyjaśnieniem Starosty Sokołowskiego: „*Stwierdzone XXXXXXXX nie mają wpływu na prawidłowe działanie strony internetowej*" oraz *„prawidłowe wyświetlanie informacji na stronie internetowej. (...)* XXXXXXXXX *dotyczą dostawcy treści XXXXXXl, nie wpływają one na użytkowaną przez nas stronę".*

koordynatora oraz zespół ds. dostępności[58].

Przedstawiając powyższe informuję, że realizację zadania w przedmiocie zapewnienia dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych ocenia się **pozytywnie**.

Mając na uwadze powyższe ustalenia zobowiązuję Panią Starostę do podjęcia działań w celu wyeliminowania stwierdzonych nieprawidłowości, a w szczególności do:

1. Udokumentowania procedur dotyczących dostarczania i zarządzania usługami realizowanymi przez systemy teleinformatyczne na deklarowanym poziomie dostępności, zgodnie z wymogami § 15 ust. 2 rozporządzenia w sprawie KRI.
2. Określenia procedur w zakresie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz ich przeprowadzania zgodnie z wymogiem określonym w § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI.
3. Zapewnienia osobom zaangażowanym w proces przetwarzania informacji szkoleń ze szczególnym uwzględnieniem takich zagadnień, jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji i odpowiedzialność prawna czy stosowanie środków zapewniających bezpieczeństwo informacji, zgodnie z wymogiem § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI.
4. Zamieszczania w umowach serwisowych zawieranych z podmiotami zewnętrznymi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z wymogiem § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI.
5. Przechowywania informacji w dziennikach systemów (logów) przez okres zgodny z określonym w § 21 ust. 4 rozporządzenia w sprawie KRI.

Ponadto zwracam uwagę na konieczność:

a) zamieszczenia na stronie BIP informacji określonych w § 3 ust. 1 pkt 2, 4 i 5 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępnia formularzy, wzorów i kopii dokumentów elektronicznych;
b) zapewnienia rozliczalności w zakresie zapoznawania nowo zatrudnionych pracowników z dokumentacją składającą się na ustanowiony system zarządzania bezpieczeństwem informacji, mając na uwadze wymogi § 20 ust. 1 rozporządzenia w sprawie KRI;

[58] Zarządzeniem Nr 46/2020 Starosty Sokołowskiego z dnia 16 września 2020 r.

c) stosowania ustanowionych procedur systemu zarządzania bezpieczeństwem informacji, w tym w szczególności w zakresie nadawania, weryfikacji, zmiany i odbierania uprawnień w systemie informatycznym,
d) przeglądu ustanowionych procedur systemu zarządzania bezpieczeństwem informacji pod kątem różnic pomiędzy procedurami określonymi w różnych dokumentach, w tym w szczególności w zakresie nadawania i odbierania uprawnień do systemu informatycznego, jak również procedur faktycznie niestosowanych pod kątem oceny ich roli w zapewnieniu bezpieczeństwa informacji;
e) wykonywania testów odtworzeniowych kopii zapasowych oraz nieprzechowywania kopii zapasowych w tej samej lokalizacji co serwery, w celu minimalizacji możliwości utraty informacji w wyniku awarii, zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia w sprawie KRI;
f) poprawy XXXXXXXXXXXX, mając na uwadze wymogi określone w § 20 ust. 2 pkt 7 i 9 rozporządzenia w sprawie KRI.

Przedstawiając powyższe informuję, że od wystąpienia pokontrolnego nie przysługują środki odwoławcze oraz zobowiązuję Panią Starostę do przekazania, w terminie 14 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, pisemnej informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków pokontrolnych lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości. Proszę o udzielenie powyższej informacji za pośrednictwem platformy ePUAP.

Z up. WOJEWODY MAZOWIECKIEGO

Artur Subda
Dyrektor Wydziału Kontroli

/podpisano kwalifikowanym
podpisem elektronicznym/