WOJEWODA MAZOWIECKI

Warszawa, 17 czerwca 2024 r.

WK-I.431.2.1.2024

Pani
Ewa Grażyna Besztak
Starosta Węgrowski

Starostwo Powiatowe w Węgrowie
ul. Przemysłowa 5
07-100 Węgrów

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 5 do 28 marca 2024 r. kontrolę problemową w Starostwie Powiatowym w Węgrowie (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 zadania publiczne pod względem zgodności z minimalnymi wymaganiami dla systemów

[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).

teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej[4] – w okresie od 1 stycznia 2023 r. do 1 marca 2024 r.

Nawiązując do projektu wystąpienia pokontrolnego z 29 maja 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 XXXXXXX używany w Starostwie do realizacji zadań zleconych z zakresu administracji rządowej, przy pomocy którego prowadzona jest XXXXXXXXXXXXX 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 Biuletynu Informacji Publicznej (dalej BIP), poinformowano o warunkach organizacyjno-technicznych doręczania dokumentów elektronicznych wskazanych w § 3 ust. 1 pkt 1, 4 i 5 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 danych określonych w załączniku nr 2 rozporządzenia

[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).

w sprawie KRI[6,7].

Na stronie internetowej Starostwa oraz na stronie BIP Starostwa w zakładce E-formularze zamieszczono wykazy usług świadczonych w Starostwie. Po wybraniu poszczególnych usług następuje przekierowanie do stron zawierających wzory wniosków oraz informacje o podstawie prawnej, wymaganych dokumentach, opłatach, miejscu i sposobie załatwienia sprawy, terminie załatwienia sprawy oraz 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 Starostwie udokumentowane zostały procedury odnoszące się do dostarczenia usług realizowanych za pomocą systemów teleinformatycznych na deklarowanym poziomie dostępności, zgodnie z § 15 ust. 2 rozporządzenia w sprawie KRI.

W rejestrze prowadzonym za pomocą programu XXXXXXX 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 wyposażyło 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[8].

Kodowanie znaków w wysyłanych z systemów lub odbieranych przez te systemy dokumentach odbywa się w standardzie zgodnym z § 17 ust. 1 rozporządzenia w sprawie KRI[9].

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

---

6 Zgodnie z pisemnym wyjaśnieniem Starosty Węgrowskiego.

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 Zgodnie z pisemnymi z wyjaśnieniami Starosty Węgrowskiego.

9 Zgodnie z pisemnymi z wyjaśnieniami Starosty Węgrowskiego.

10 Kontrolującym przedłożono Zarządzenie nr 46/2014 Starosty Węgrowskiego z dnia 31 grudnia 2014 r. w sprawie wykonywania czynności kancelaryjnych w Starostwie Powiatowym w Węgrowie.

W wyniku kontroli stwierdzono uchybienie polegające na niewskazaniu w opisie skrzynki podawczej na stronie podmiotowej BIP maksymalnego rozmiaru dokumentów elektronicznych wraz z załącznikami, które mogą być przesłane do jednostki poprzez elektroniczną skrzynkę podawczą[11]. Powyższym działaniem naruszono postanowienia § 3 ust. 1 pkt 2 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.

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 uchybień.**

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:

1) *Systemie Zarządzania Bezpieczeństwem Informacji PN-ISO/IEC 27001* [12], na który składa się szereg dokumentów, w tym m. in.: *Księga Bezpieczeństwa Informacji*, *Polityka Ochrony Danych Osobowych*, *Polityka Szacowania Ryzyka*[13], *Procedury Audytu Wewnętrznego* czy *Zasady Eksploatacji Systemów Informatycznych*[14],
2) *Procedurze zarządzania incydentami cyberbezpieczeństwa*[15],

---

[11] Wskazano jedynie maksymalny rozmiar wszystkich załączników dołączonych do jednego dokumentu elektronicznego.
Zgodnie z pisemnymi wyjaśnieniami osoby upoważnionej do ich udzielania w zakresie objętym kontrolą: „*Treść nie została odpowiednio zaktualizowana. Maksymalny rozmiar dokumentu elektronicznego wraz z załącznikami i podpisem, możliwy do doręczenia z wykorzystaniem elektronicznej skrzynki podawczej to 5 MB”.*

[12] Aktualnie w wersji 2.0. Dalej także: SZBI. Zgodnie z *Księgą Bezpieczeństwa Informacji:*
- *Polityka Bezpieczeństwa Informacji* oraz *System Zarządzania Bezpieczeństwem Informacji* zostały ustanowione Zarządzeniem XXXXXXXXX Starosty Węgrowskiego XXXXXXX, którym powołano Pełnomocnika oraz Zespół do spraw Systemu Zarządzania Bezpieczeństwem Informacji, zobowiązując jego członków „*do realizacji zadań opisanych w wprowadzonej dokumentacji SZBI”* (ww. zarządzenie nie zawiera postanowień w sprawie ustanowienia SZBI);
- wdrożony w Starostwie *System Zarządzania Bezpieczeństwem Informacji* jest zgodny z polskimi i międzynarodowymi normami: PN-ISO/IEC 27000:2012P, PN-ISO/IEC 27001:2017-06, PN-ISO/IEC 27002:2017-06, PN-ISO/IEC 27005:2014-01P.

[13] Z załącznikami, które stanowią: XXXXXXXXXXXXXXXXXX.

[14] Z załącznikami, które stanowią: XXXXXXXXXXXXX.

[15] Procedura ustanowiona Zarządzeniem XXXXXXXXXX Starosty Węgrowskiego XXXXXXX.

3) *Procedurze ochrony danych osobowych oraz bezpieczeństwa i higieny pracy przy wykonywaniu pracy zdalnej w Starostwie Powiatowym w Węgrowie*[16].

W okresie kontrolowanym dokonano przeglądu skuteczności SZBI[17] oraz aktualizacji części dokumentacji składającej się na *System Zarządzania Bezpieczeństwem Informacji*[18] w myśl wymogów określonych w § 20 ust. 1 rozporządzenia w sprawie KRI, zgodnie z którym *„Podmiot realizujący zadania publiczne (...) monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji (...)”*.

Stwierdzono, że w Starostwie przeprowadzane są okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji, zgodnie z wymogiem określonym w § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI, jak również udokumentowane zostały procedury w przedmiotowym zakresie[19]. Zgodnie z ustanowionymi regulacjami wewnętrznymi z przeprowadzanych analiz ryzyka opracowywane są raporty z szacowania ryzyka[20] zawierające rejestr ryzyka z rekomendacjami, a także plany postępowania z ryzykiem[21]. W okresie kontrolowanym wdrożono jedną z rekomendacji po przeprowadzonej analizie ryzyka w 2021 r.[22].

Udokumentowane zostały[23] procedury w zakresie zarządzania uprawnieniami użytkowników systemu informatycznego Starostwa, stwarzające warunki sprzyjające realizacji i egzekwowaniu 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. Zakresy czynności losowo wybranych pracowników[24], którym przyznano dostęp do systemu XXXXX,

---

16 Procedura ustanowiona Zarządzeniem XXXXXXX Starosty Węgrowskiego z XXXXXXXX.

17 Przegląd udokumentowany notatką ze spotkania *Zespołu Bezpieczeństwa* z 27.02.2023 r.

18 Dotyczy: SZBI_009_Załącznik 3 XXXXXXX, SZBI_004_Załącznik nr 1 XXXXXXX, SZBI_011 XXXXXXXXXX, które do dnia zakończenia kontroli nie zostały zatwierdzone przez Starostę Węgrowskiego, a także *SZBI_010 XXXXXXXXXX,* zatwierdzonego 26.03.2024 r.

19 Dotyczy *SZBI_004 XXXXXXXXX.*

20 Okazane zostały, opracowane przez Pełnomocnika ds. SZBI, *Raporty z szacowania ryzyka*, datowane na październik 2023 r. i grudzień 2021 r., zatwierdzone przez Starostę Węgrowskiego, odpowiednio: 07.03.2024 r . i 28.03.2023 r.

21 Okazane zostały, opracowane przez Pełnomocnika ds. SZBI, *Plany postępowania z ryzykiem* datowane na październik 2023 r. i grudzień 2021 r., zatwierdzone przez Starostę Węgrowskiego, odpowiednio: 07.03.2024 r. i 28.03.2023 r.

22 Dotyczy rekomendacji dot. XXXXXXXXXXX. Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania rekomendacja w tym zakresie wdrożona została poprzez XXXXXXXXXXXXXXXXXXXXX.

23 Dotyczy: *SZBI_003 XXXXXXXXXX, SZBI_009 XXXXXXXXXXX, SZBI_009_załącznik 2 XXXXXXXXXXX.*

24 Dotyczy 6 pracowników Starostwa.

obejmują zadania, w realizacji których może być wykorzystywana XXXXXXXXXX[25].

W związku z wymogiem określonym w § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI osobom zaangażowanym w proces przetwarzania informacji zapewnione zostały w okresie kontrolowanym 2 szkolenia z zakresu cyberbezpieczeństwa[26] oraz 3 szkolenia z zakresu ochrony danych osobowych[27].

Ustanowione zostały zasady[28] 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 – w okresie kontrolowanym ustanowiona została *Procedura zarządzania incydentami cyberbezpieczeństwa.* W ww. okresie nie zostały zgłoszone incydenty naruszenia bezpieczeństwa informacji.

Udokumentowane zostały[29] zasady przeprowadzania w Starostwie audytów wewnętrznych. W związku z wymogiem określonym w § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI, w 2023 r. przeprowadzony został audyt podatności systemów teleinformatycznych[30] oraz audyt w zakresie weryfikacji ochrony fizycznej, określony w planie

---

[25] Uwzględniono w tym zakresie także wyjaśnienia osoby upoważnionej do ich udzielania w zakresie objętym kontrolą. Powyżej wskazanym pracownikom udzielono także upoważnień do przetwarzania danych osobowych w ramach realizowanych zadań.

[26] W tym 1 szkolenie zewnętrzne dla kadry kierowniczej, w którym wzięło udział 9 osób oraz szkolenie przeprowadzone przez Inspektora Ochrony Danych, w którym wzięło udział 11 osób, stanowiące, zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą, szkolenie uzupełniające dla osób, które nie brały udziału w szkoleniu zorganizowanym 30.11.2022 r. (w szkoleniu tym wzięło udział 57 osób). *„Pozostało 7 osób do przeszkolenia z zakresu bezpieczeństwa informacji, które nie brały udziału w szkoleniach w listopadzie 2022 r. i lutym 2023 r., które przebywają na długotrwałych nieobecnościach XXXXXXXXXX”.* Zgodnie z zatwierdzonym 07.03.2024 r. *Planem postępowania z ryzykiem* – na lata 2024-2025 zaplanowano szkolenia pracowników z zakresu procedur bezpiecznej pracy w systemach informatycznych oraz w zakresie cyberbezpieczeństwa w ramach programu *„Cyberbezpieczny samorząd”*. Programy szkolenia obejmowały takie zagadnienia, jak zagrożenia i ryzyko związane z cyberatakami, techniki socjotechniczne cyberprzestępców, metody rozpoznawania podejrzanych wiadomości czy linków, bezpieczne praktyki korzystania z systemów informatycznych, aktualizacja systemów operacyjnych i oprogramowania, stosowanie oprogramowania antywirusowego i zapór sieciowych, procedury zgłaszania incydentów, a zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą – na szkoleniu *„były poruszane zagadnienia dotyczące odpowiedzialności prawnej organizacji oraz pracowników za naruszenie zasad bezpieczeństwa informacji, w tym danych osobowych. Omawiano przykłady kar nakładanych przez UODO.”*.

[27] Szkolenia dla stażystów, w których wzięło udział ogółem 5 osób.

[28] Dotyczy dokumentów: XXXXXXXXXX stanowiące załącznik nr 1 do XXXXXXXXXXXX, XXXXXXXXXXXXX stanowiące załącznik nr 2 do XXXXXXXXXXXXXXXXX, Zarządzenie XXXXXXXXX Starosty Węgrowskiego z XXXXXXXXXX w sprawie ustalenia procedury ochrony danych osobowych oraz bezpieczeństwa i higieny pracy przy wykonywaniu pracy zdalnej.

[29] Dotyczy: *SZBI_007 XXXXXXXXXX.*

[30] Audyt przeprowadził pentester firmy zewnętrznej, z którą łączą Starostwo umowy m.in. w zakresie wykonywania audytu zabezpieczeń fizycznych i informatycznych.

kontroli jako audyt zgodności w zakresie ochrony danych osobowych[31], a także diagnoza cybezpieczeństwa[32, 33]. W planie audytów na 2024 r. zaplanowano audyty *„procesu Systemu Zarządzania Bezpieczeństwem Informacji”*, w tym audyt podatności systemów IT oraz audyt wewnętrzny SZBI[34].

W Starostwie udokumentowane zostały procedury odnoszące się do wykonywania i odtwarzania kopii zapasowych[35] 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 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[36], 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 sieciowej i zasilania awaryjnego[37], przeprowadzanie badań podatności systemu informatycznego, szyfrowanie przenośnych nośników danych oraz dysków urządzeń

---

[31] Audyt przeprowadził Inspektor Ochrony Danych, który dokonał sprawdzenia stosowania zabezpieczeń fizycznych przy przechowywaniu dokumentów oraz zabezpieczeń nowej siedziby jednego z wydziałów Starostwa.

[32] Czynności dokonał certyfikowany audytor wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001, w związku z umową z firmą zewnętrzną na pełnienie funkcji Inspektora Ochrony Danych oraz określonych czynności w zakresie ochrony danych osobowych. W jej wyniku powstała *Ocena zgodności z KRI/UoKSC* oraz *Ocena wybranych aspektów bezpieczeństwa systemów informatycznych.*

[33] Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą – *„Rozporządzenie w sprawie KRI nie określa, że audyt wewnętrzny musi obejmować całość SZBI (...) wobec tego przyjęto, że badane będą co roku poszczególne obszary, nie rzadziej niż raz na 3 lata każdy z obszarów (...)”,* przy czym opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 *System Zarządzania Bezpieczeństwem Informacji* jest audytowany w oparciu o wytyczne normy PN-ISO/IEC 27001 pkt. 9.2, 9.3, zarządzanie ryzykiem odbywa się w oparciu o wytyczne normy PN-ISO/IEC 27005, a ustanawianie zabezpieczeń na podstawie deklaracji stosowania *„SZBI_013_XXXXXXX”.*

[34] Do dnia zakończenia kontroli plan ten nie został zatwierdzony przez Starostę Węgrowskiego.

[35] Dotyczy dokumentów: *Zasady zarządzania bezpieczeństwem zasobów informatycznych* stanowiące załącznik nr 2 do XXXXXXXXXXXXX stanowiąca załącznik nr 3 do XXXXXXXXXXXX.

[36] Dotyczy XXXXXXX.

[37] Dotyczy XXXXXXX.

mobilnych wykorzystywanych przy pracy zdalnej czy ustanowienie regulacji wewnętrznych określających m.in. zasady bezpiecznej pracy w systemach teleinformatycznych dla użytkowników, zasady zarządzania bezpieczeństwem zasobów informatycznych, procedurę zarzadzania incydentami cyberbezpieczeństwa czy plan działań na wypadek sytuacji katastrofalnych.

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.

Zgodnie z prowadzonym w jednostce *Dziennikiem Administratora Systemów* – w okresie kontrolowanym dokonywano przeglądu logów systemu antywirusowego oraz systemu wykorzystywanego do archiwizacji danych[38], a także logów UTM, urządzeń sieciowych i serwerów[39]. Informacje w dziennikach systemów przechowywane są przez 2 lata[40], zgodnie z wymogiem określonym w § 21 ust. 4 rozporządzenia w sprawie KRI.

Rozliczalność działań poszczególnych użytkowników systemu XXXXXXX w zakresie wydawania informacji z prowadzonego rejestru publicznego zapewniona jest poprzez generowanie na wydawanych XXXXXXXXXXXXX danych personalnych osoby, która dokonała operacji w tym zakresie[41].

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Niezapewnienie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację[42], pomimo że zgodnie z § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI – *„Zarządzanie bezpieczeństwem*

[38] Z częstotliwością wynoszącą XXXXXXXX.

[39] XXXXXXXXXX. Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą – w roku 2024 w jednostce planowane jest wdrożenie oprogramowania XXXXXXXXXXX.

[40] Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą – *„Logi przechowywane są 2 lata lub więcej”*, razem z kopiami zapasowymi danych, baz danych i systemów.

[41] Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą logi systemu XXXXXXXXX dotyczące użytkowników nie były w okresie kontrolowanym monitorowane *„ponieważ nie wiedzieliśmy że jest możliwość monitorowania takich logów. Producent nie zapewnia tego w standardzie (…) Gromadzenie tego typu logów jest opcją dodatkową, której chęć instalacji wyraziliśmy w mailu do producenta oprogramowania i aktualnie oczekujemy na wdrożenie”. „Oprogramowanie XXXXXXX korzysta z systemu bazodanowego XXXXXXXXXX, a system XXXXXXXXXX,. o tym który użytkownik korzystał z oprogramowania. Logi programu XXXXXXXXXX były gromadzone w okresie kontrolowanym.”* Okazany został mail z 06.03.2024 r. skierowany do licencjodawcy z prośbą o *„przesłanie pliku oraz instrukcji do (…) programu umożliwiającego śledzenie logów szczegółowych XXXXXXXX.”*.

[42] Zgodnie z udokumentowaną protokołem rozmową z informatykiem Starostwa – XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX. W ankiecie dotyczącej działania systemów teleinformatycznych wykorzystywanych do realizacji zadań z zakresu administracji rządowej wskazano, że w jednostce planowane jest wdrożenie w 2024 r. oprogramowania XXXXXXXXXXXXXXX.

informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie (...) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację (...)".

2. Niezagwarantowanie umową odpowiedniego poziomu bezpieczeństwa informacji w związku z serwisowaniem systemu XXXXXX przez podmiot zewnętrzny[43], 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"*. Powyższe może być konsekwencją braku udokumentowanych procedur w zakresie zawierania w umowach serwisowych podpisywanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji[44].

Ponadto w wyniku kontroli ustalono, że:

a) część osób nowo zatrudnionych[45] zaangażowanych w proces przetwarzania informacji nie potwierdziło faktu zapoznania się z dokumentacją *Systemu Zarządzania Bezpieczeństwem Informacji,* jak również część pracowników Starostwa zaangażowanych

---

[43] 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. Zleceń pisemnych w przedmiotowym zakresie nie przedstawiono do kontroli.
Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą – w przedmiotowym przypadku nie ma podstaw do zawarcia umowy powierzenia przetwarzania danych, gdyż licencjodawca świadczący pomoc techniczną *„nie ma dostępu do danych osobowych", „Pomoc techniczna ma dostęp tylko do danych konfiguracyjnych"*. Na poparcie wyjaśnień przedstawiono także oświadczenie licencjodawcy z 10.04.2024 r., zgodnie z którym *„w ramach wsparcia technicznego programu XXXXXXXXX nie ma dostępu do danych zgromadzonych w bazie XXXXXXXX"*. Odnosząc się do powyższego wyjaśnienia podkreślić należy, że bezpieczeństwo informacji należy rozpatrywać biorąc pod uwagę poszczególne jej atrybuty, w tym m.in. dostępność. Przedstawione licencje nie zawierają zapisów dot. szybkości udzielania pomocy w ramach wsparcia technicznego.

[44] W przyjętej dokumentacji *Systemu Zarządzania Bezpieczeństwem Informacji* zasady współpracy z podmiotami trzecimi ograniczone zostały do zawierania umów powierzenia przetwarzania danych osobowych (dotyczy *SZBI_003 XXXXXXXX*). Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą *„podczas omówienia (...) raportu z audytu SZBI z 2021 r. ustalono, że zasady współpracy z podmiotami zewnętrznymi będą określać indywidualnie XXXXXXXXXX"*.

[45] Dotyczy 3 z 6 osób wskazanych jako nowo zatrudnione w okresie poddanym kontroli. Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą – zostały one *„zapoznane z Systemem Bezpieczeństwa Informacji. Aktualne dokumenty SZBI są dostępne XXXXXXXXXXXXXXXXXXX. Podpisy wymienionych osób zostały przeoczone i zostaną uzupełnione."*.

w przedmiotowy proces[46] nie potwierdziło faktu zapoznania się z ustanowioną w okresie kontrolowanym *Procedurą zarządzania incydentami cyberbezpieczeństwa*;

b) dla 3 osób, które zakończyły pracę w Starostwie, a następnie w krótkim odstępie czasu[47] zostały ponownie zatrudnione – nie zostały złożone wnioski o odebranie uprawnień do systemu informatycznego po zakończeniu pierwszego z tych okresów zatrudnienia[48], a wniosek o odebranie dostępu do systemu informatycznego dla 1 osoby, która zakończyła pracę w Starostwie w okresie kontrolowanym został złożony 13. dnia od rozwiązania stosunku pracy[49], co należy ocenić krytycznie wobec postanowień art. § 20 ust. 2 pkt. 5 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 (...) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji."*;

c) w dokumentacji tworzącej *System Zarządzania Bezpieczeństwem Informacji* wskazano nieobowiązujący już dokument dotyczący procedur archiwizacji i replikacji zasobów informatycznych Starostwa, stanowiący załącznik do nieobowiązującej *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych*[50].

Stwierdzono także przypadki rozbieżności pomiędzy udokumentowanymi procedurami *Systemu Zarządzania Bezpieczeństwem Informacji* a faktycznie stosowaną praktyką[51].

---

[46] Dotyczy 6 z wykazanych na liście pracowników Starostwa. Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania w zakresie objętym kontrolą – *„(...) osoby na liście osób zapoznanych z procedurą zostały przeoczone jedynie na liście do podpisu. Osoby te zostały w pełni zapoznane z procedurą, a ich podpisy zostaną uzupełnione (...)"*.

[47] Dotyczy okresu do 2 tygodni.

[48] Zgodnie z wyjaśnieniami pisemnymi osoby upoważnionej do ich udzielania osobom tym *„nie zostały odebrane uprawnienia do systemu teleinformatycznego z powodu kontynuacji pracy w Starostwie Powiatowym w Węgrowie na takim samym bądź podobnym stanowisku nie wymagającym zmian uprawnień. (...) pracownicy zostali ponownie zatrudnieni i zakres ich czynności się nie zmienił."*. Odnosząc się do kwestii nieodebrania uprawnień bezpośrednio po zakończeniu zatrudnienia pomimo wystąpienia okresu przerwy pomiędzy zakończeniem i ponownym nawiązaniem stosunku pracy z danych pracownikiem – wskazano: *„Data ponownego zatrudnienia pracowników planowana jest bezpośrednio po rozwiązaniu stosunku pracy. Niekiedy zdarza się przerwa, co uzależnione jest od procedury dotyczącej przeprowadzenia naboru."*

[49] Dostęp do systemu został zablokowany tego samego dnia.

[50] W dokumencie XXXXXXXXXX, załączniku nr 2 XXXXXXXXXXX, w pkt 9 wskazano: *„Archiwizacja i replikacja odbywa się XXXXXXXXXXXXXXXXXXX"*.
Zgodnie z pisemnymi wyjaśnieniami osoby upoważnionej do ich udzielania w zakresie objętym kontrolą: *„Ponieważ do 2023 r. nie było opracowanych technicznych instrukcji XXXXXXX stary zapis pozostał, powinien być zaktualizowany w zeszłym roku – przeoczenie. Instrukcja określająca sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych z 2017 r. przestała obowiązywać w momencie stworzenia nowej dokumentacji ochrony danych zgodnie z RODO"*.

[51] Dotyczy:

Zwrócić należy także uwagę na brak XXXXXXXXXXXXXXXXXXXXXXXXXXX.

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 – strony internetowe Starostwa działające pod adresami https://powiatwegrowski.pl/ oraz https://bip.powiatwegrowski.pl/ 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 marca 2024 r. walidacja ww. stron wykazała przypadki błędów, ostrzeżeń i komunikatów informacyjnych[52], przy czym nie stwierdzono, aby miały one wpływ na prezentowane treści[53].

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 oraz strona BIP Starostwa zawierają rozwiązania techniczne umożliwiające osobom niepełnosprawnym zapoznanie się z treścią informacji. Starostwo zamieściło na swojej

---

- częstotliwości dokonywania przeglądów szacowania ryzyka, które zgodnie z *Księgą Bezpieczeństwa Informacji* mają być dokonywane raz na rok, podczas gdy jako dowody w przedmiotowym zakresie okazano *Raporty z szacowania ryzyka* z roku 2023 i 2021;
- częstotliwości dokonywania przeglądów SZBI, które zgodnie z *Księgą Bezpieczeństwa Informacji* mają być dokonywane raz w roku, podczas gdy w okresie kontrolowanym przegląd SZBI nie był zrealizowany, a zgodnie z wyjaśnieniem pisemnym osoby upoważnionej do ich udzielania w zakresie objętym kontrolą – *„Ostatni pełny audyt SZBI został wykonany w 2021 r. (...)”,* a kolejny zaplanowany został na 2024 r.;
- dokumentacji sporządzanej z audytów wewnętrznych – z przeprowadzonych audytów wewnętrznych w obszarze bezpieczeństwa informacji nie okazano dokumentów, o których mowa w *Procedurach Audytu Wewnętrznego*, tj. *Raportu z audytu* i *Propozycji działań korygujących*;
- długości haseł do systemów informatycznych, która zgodnie z XXXXXXXXXXXX wynosić ma *XXXXXXXXXXXX,* podczas gdy faktycznie obowiązuje w jednostce zasada nadawania haseł składających się z minimum z XXXXXX znaków.

[52] Dla walidatora https://validator.w3.org/:
- dla strony: https://powiatwegrowski.pl/ – ponownie 9 ostrzeżeń oraz 61 komunikatów informacyjnych,
- dla strony BIP: https://bip.powiatwegrowski.pl/ – 3 błędy, 7 ostrzeżeń oraz 21 komunikatów informacyjnych;

zaś dla walidatora http://jigsaw.w3.org/css-validator:
- dla strony: https://powiatwegrowski.pl/ – 157 ostrzeżeń,
- dla strony BIP: https://bip.powiatwegrowski.pl/ – 1 błąd oraz 36 ostrzeżeń.

[53] Zgodnie z pisemnymi wyjaśnieniami osoby upoważnionej do ich udzielania w zakresie objętym kontrolą: „*Wyżej wymienione ostrzeżenia, komunikaty i błędy nie mają wpływu na funkcjonowanie strony*”.

stronie internetowej deklarację dostępności oraz informację 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. Ponadto w Starostwie powołano koordynatorów oraz zespół ds. zapewnienia dostępności[54].

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. Utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, zgodnie z wymogiem § 19 ust. 2 pkt 2 aktualnie obowiązującego rozporządzenia w sprawie KRI[55].
2. Zawierania w umowach serwisowych podpisywanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z wymogiem § 19 ust. 2 pkt 10 aktualnie obowiązującego rozporządzenia w sprawie KRI.

Ponadto zwracam uwagę na konieczność:

a) wskazania w opisie skrzynki podawczej na stronie podmiotowej BIP maksymalnego rozmiaru dokumentów elektronicznych wraz z załącznikami, które mogą być przesłane do jednostki poprzez elektroniczną skrzynkę podawczą, zgodnie z wymogiem § 3 ust. 1 pkt 2 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych;
b) zapewnienia rozliczalności w zakresie zapoznawania pracowników zaangażowanych w proces przetwarzania informacji, w tym pracowników nowo zatrudnionych, z dokumentacją składającą się na ustanowiony system zarządzania bezpieczeństwem

---

[54] Zarządzeniem Nr 30/2020 Starosty Węgrowskiego z dnia 2 września 2020 r. w sprawie wyznaczenia koordynatorów do spraw dostępności w Starostwie Powiatowym w Węgrowie, zmienionym Zarządzeniem Nr 3/2022 Starosty Węgrowskiego z dnia 17 stycznia 2022 r. w sprawie wyznaczenia koordynatorów do spraw dostępności w Starostwie Powiatowym w Węgrowie.

[55] Dotyczy Rozporządzenia Rady Ministrów z dnia 21 maja 2024 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 2024 r. poz. 773), obowiązującego od 23 maja 2024 r., dalej: aktualnie obowiązujące rozporządzenie w sprawie KRI.

informacji, mając na uwadze wymogi § 19 ust. 1 aktualnie obowiązującego rozporządzenia w sprawie KRI;

c) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji, zgodnie z wymogiem § 19 ust. 2 pkt 5 aktualnie obowiązującego rozporządzenia w sprawie KRI, w tym mając na uwadze osoby, których zatrudnienie w Starostwie ustało;
d) przeglądu dokumentacji tworzącej system zarządzania bezpieczeństwem informacji pod kątem jego aktualności oraz rozbieżności pomiędzy udokumentowanymi procedurami tego systemu a faktycznie stosowaną praktyką, w tym w celu wdrożenia ustanowionych procedur mających gwarantować odpowiedni poziom bezpieczeństwa informacji;
e) dokonania analizy ryzyka XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, a następnie podjęcia działań stosownych do wyników analizy w tym zakresie.

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 e-Doręczeń lub przez ePUAP.

Z up. WOJEWODY MAZOWIECKIEGO

Lesław Kuczyński
Zastępca Dyrektora Wydziału Kontroli

/podpisano kwalifikowanym
podpisem elektronicznym/