WOJEWODA WIELKOPOLSKI

Poznań, /elektroniczny znacznik czasu/

OI-VII.1610.4.2022.5

Pani
Justyna Dąbrowska
Wójt Gminy Zaniemyśl
ul. Średzka 9
63-020 Zaniemyśl

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz. U. z 2020, poz. 224), art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 2070 ze zm.), kontrolerzy Maciej Kabaciński – kierownik oddziału w Biurze Obsługi i Informatyki i Ilona Ratajczak – starszy specjalista w Biurze Obsługi i Informatyki Wielkopolskiego Urzędu Wojewódzkiego w Poznaniu, przeprowadzili 8 września 2022 r. kontrolę w Urzędzie Gminy w Zaniemyślu, ul. Średzka 9, 63-020 Zaniemyśl.
Przedmiot kontroli obejmował zagadnienia dot. świadczenia usług drogą elektroniczną – interoperacyjność na poziomie organizacyjnym, dostosowania posiadanych systemów informatycznych wykorzystywanych przy realizacji zadań zleconych z zakresu administracji rządowej do współpracy z innymi systemami/rejestrami informatycznymi oraz stosowanych mechanizmów związanych z zachowaniem poufności, integralności danych i rozliczalności czynności, zarządzania bezpieczeństwem informacji dla systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej, a także dostępności informacji zawartych na stronach internetowych jednostki kontrolowanej dla osób niepełnosprawnych.
Kontrolą objęto okres od 1 stycznia 2021 r. do dnia zakończenia kontroli (a także działania wcześniejsze jeżeli miały one związek z przedmiotem kontroli).

Wojewoda Wielkopolski pozytywnie ocenia działalność kontrolowanej jednostki w zakresie objętym kontrolą pomimo stwierdzonych nieprawidłowości.

Sformułowana ocena została oparta na podstawie poniżej opisanych ustaleń dokonanych w ramach czynności kontrolnych.

al. Niepodległości 16/18, 61-713 Poznań
tel. 61 854 1722, fax 61 854 1500
www.poznan.uw.gov.pl, e-mail: oi@poznan.uw.gov.pl
www.obywatel.gov.pl, infolinia tel. 222 500 117

Podpisane cyfrowo przez Michał Witold Zieliński
Date: 2022.10.11 11:50:26 CEST

1. **Świadczenie usług drogą elektroniczną.**

Przy prowadzeniu czynności kontrolnych w zakresie świadczenia usług elektronicznych sprawdzeniu poddano zagadnienia związane z osiągnięciem interoperacyjności na poziomie organizacyjnym (§ 5 ust. 2 pkt 1 i 4 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych - t.j. Dz. U. z 2017 r. poz. 2247, dalej „KRI") tj.:

- *zamieszczenie w sposób umożliwiający skuteczne zapoznanie się, informacji o dostępności oraz zakresie użytkowym serwisów dla realizowanych usług,*
- *publikowanie i uaktualnianie w BIP opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.*

Sprawdzeniu poddano również problematykę, o której mówi art. 19 b ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne - t.j. Dz. U. z 2021 r. poz. 2070 ze zm. (dalej „ustawa o informatyzacji") w zakresie obowiązku przekazania do centralnego repozytorium wzorów dokumentów elektronicznych.

Jednostka kontrolowana zgodnie z ustawą o informatyzacji, udostępniła Elektroniczną Skrzynkę Podawczą (ESP) na elektronicznej Platformie Usług Administracji Publicznej (ePUAP), która jest środkiem komunikacji elektronicznej, służącym przekazywaniu informacji do podmiotu publicznego w formie elektronicznej **/u0qtn79j46/skrytka**).

Na stronie głównej jednostki kontrolowanej http://zaniemysl.pl zamieszczona została zakładka ePUAP, która miała za zadanie przekierować użytkownika na stronę logowania serwisu gov.pl. W dniu przeprowadzania kontroli próba skorzystania z tej funkcji nie zakończyła się sukcesem - wyświetlił się komunikat o błędzie „nieprawidłowe żądania lub odpowiedź http". Ponadto na ww. stronie znajdowała się zakładka „Wnioski do pobrania", gdzie po kliknięciu wyświetlił się katalog spraw z podziałem na Referaty oraz zamieszczone były wzory druków.

Na stronie BIP https://zaniemysl.biuletyn.net/ zamieszczono zakładkę ESP, która przekierowywała użytkownika na stronę główną portalu ePUAP2. Na ww. stronie zakładka „Informacje" zawierała wykaz Referatów Urzędu wraz ze wskazaniem zakresu spraw, którymi się zajmują. Ponadto zamieszczona została zakładka „Karty usług publicznych" z wyszczególnionymi grupami spraw realizowanych przez poszczególne Referaty:

1. Referat Spraw Obywatelskich (12 spraw – dla wszystkich zamieszczone były karty usług).
2. Referat Organizacyjny (6 spraw – dla 1 zamieszona była karta usług, w odniesieniu do 1 udostępniono przekierowanie do portalu CEiDG).
3. Referat Gospodarki Nieruchomościami i Rolnictwa (12 spraw – dla 11 spraw były zamieszczone karty usług, w odniesieniu do 1 sprawy brak było załączonego druku do pobrania – pod linkiem karta usług).

4. Referat Finansów (6 spraw – brak było kart usług).
5. Referat Inwestycji i Gospodarki Komunalnej (9 spraw – dla 2 spraw zamieszczone były karty usług).

W zamieszczonych kartach usług ujęte były podstawowe informacje nt. miejsca złożenia dokumentów, terminu załatwienia sprawy, wymaganych dokumentów, opłat, podstawy prawnej oraz druki do pobrania w formacie .pdf lub .doc.
W kartach usług z wyjątkiem dot. dowodu osobistego, nie było adnotacji o możliwości załatwienia danej sprawy drogą elektroniczną. Nie został również wyszczególniony katalog tych spraw.

Ponadto, na stronie BIP nie była zamieszczona część informacji, o których mowa w rozporządzeniu Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych - t.j. Dz. U. z 2018 r. poz. 180 (dalej „rozporządzenie o doręczaniu dokumentów elektronicznych"), tj. o:

- maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej (§ 3 ust. 1 pkt 2),
- zakresach użytkowych dokumentów elektronicznych tworzonych na podstawie wzorów umieszczonych przez te podmioty w centralnym repozytorium lub repozytorium wzorów dokumentów elektronicznych (§ 3 ust. 1 pkt 3),
- rodzajach informatycznych nośników danych, na których może zostać doręczony dokument elektroniczny (§ 3 ust. 1 pkt 4),
- rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru (§ 3 ust. 1 pkt 5),
- formatach danych, w jakich zapisuje się załączniki dodawane do pism (§ 17 ust. 2 oraz załącznik do rozporządzenia).

W badanym okresie jednostka kontrolowana nie opracowała i nie przekazała do centralnego repozytorium wzorów dokumentów elektronicznych (akta kontroli str. 138-152).

Ogólna ocena kontrolowanego obszaru – negatywna.

2. **Dostosowanie posiadanych systemów informatycznych wykorzystywanych przy realizacji zadań zleconych z zakresu administracji rządowej do współpracy z innymi systemami/rejestrami informatycznymi oraz stosowanych mechanizmów związanych z zachowaniem poufności, integralności danych i rozliczalności czynności.**

Systemy teleinformatyczne użytkowane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności,

niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności - § 15 ust. 1 „KRI". Ponadto 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 - § 16 ust. 1 ww. rozporządzenia.

W okresie objętym kontrolą jednostka kontrolowana wykorzystywała systemy teleinformatyczne do realizacji zadań zleconych z zakresu administracji rządowej. Badaniu poddano jeden z nich, a mianowicie „ELUD+", wspierający wykonywanie zadań związanych z ewidencją ludności, autorstwa RADIX Sp. z o.o. Sp.k., ul. Piastowska 33, 80-332 Gdańsk.

Kontrolowany system informatyczny wykorzystywał bazę danych MS SQL umieszczoną na serwerze bazodanowym. Użytkownicy łączyli się do systemu z poziomu klienta aplikacji bezpośrednio z komputera w sieci LAN z dostępem do Internetu. System „ELUD+" współdziała na poziomie jednostronnej komunikacji z Systemem Rejestrów Państwowych SI Źródło pracującym w dedykowanej, wydzielonej galwanicznie sieci. Dane przenoszone były za pomocą pamięci zewnętrznej. Badany system współpracował na zasadzie pełnego automatyzmu z innymi aplikacjami autorstwa firmy RADIX S.A. wykorzystywanymi w jednostce kontrolowanej (akta kontroli str. 153).

Poufność, integralność danych i rozliczalność czynności zagwarantowana została poprzez przydzielenie w systemie kont zabezpieczonych hasłem dla poszczególnych użytkowników oraz mechanizm zapisywania zdarzeń (logi systemowe) - akta kontroli str. 154.

Oprogramowanie było na bieżąco aktualizowane (w okresie objętym kontrolą – 12 aktualizacji) - akta kontroli str. 155.

Jednostka kontrolowana zawarła umowę na opiekę autorską z producentem oprogramowania (8.04.2022r.) oraz umowę powierzenia przetwarzania danych osobowych (brak daty zawarcia umowy - zawarta została prawdopodobnie w 2019 r. przez poprzedniego Wójta w 2019 r.) – akta kontroli str. 156-159, 235.

Kontrolowany systemy w badanym zakresie tj. wymiany danych z innymi systemami teleinformatycznymi spełniał minimalne wymagania interoperacyjności oraz gwarantował poufność, integralność danych i rozliczalność czynności .

Ogólna ocena kontrolowanego obszaru – pozytywna.

3. Zarządzanie bezpieczeństwem informacji dla systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej.

Zasady zarządzania bezpieczeństwem informacji regulują przepisy § 20 „KRI". W ust. 1 nałożono na podmiot realizujący zadania publiczne obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądu, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji, zapewniając poufność,

dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Zasady bezpieczeństwa informacji w jednostce kontrolowanej uregulowano Polityką Bezpieczeństwa Danych Osobowych zatwierdzoną przez Wójta Gminy w dniu 25 maja 2018 r., zwaną dalej „PB"- akta kontroli str. 23-100.

Ww. dokument opracowany został na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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 z 4.05.2016) – RODO. W przedłożonej dokumentacji nie ujęto całościowo problematyki bezpieczeństwa informacji, a jedynie skupiono się na ochronie danych osobowych, które stanowią jedną z wielu przetwarzanych informacji. Rozporządzenie w sprawie KRI nałożyło obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji (§ 20 ust. 1), z kolei RODO obowiązek wdrożenia polityk ochrony danych osobowych (art. 24 ust. 2). Ponadto, w „PB" (pkt VI. Zakres Obowiązków Osób odpowiedzialnych za bezpieczeństwo danych osobowych), Inspektorowi Ochrony Danych Osobowych nadano uprawnienia do wydawania „z upoważnienia Administratora Danych upoważnienia do przetwarzania danych osobowych", co stoi w sprzeczności z unormowaniami zawartymi w art. 39 ust. 1 lit. b) RODO, które zobowiązują go do monitorowania przestrzegania ww. rozporządzenia oraz wewnętrznych regulacji administratora danych. Powyższy zapis zrodził konflikt interesów, polegający na sprawowaniu nadzoru nad własną działalnością.

Pracownicy zostali zapoznani z regulacjami w ww. zakresie, co potwierdzili poprzez złożenie oświadczeń o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami – akta kontroli str. 160-161.

Przepis § 20 ust. 2 pkt 1 „KRI" zobowiązuje podmiot publiczny do aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Od dnia wprowadzenia dokumentacja nie była modyfikowana a jej przegląd objął aktualizację Rejestru czynności przetwarzania – akta kontroli str. 162-167

Zgodnie z § 20 ust. 2 pkt 3 „KRI", jednostka kontrolowana przeprowadziła analizę ryzyka. Badaniu poddano zagadnienia związane z doborem środków bezpieczeństwa dla zasobów krytycznych - akta kontroli str. 168-196.

Zarządzanie bezpieczeństwem informacji realizowane jest również poprzez utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację - § 20 ust. 2 pkt 2.

Kontrolowana jednostka prowadziła inwentaryzację sprzętu komputerowego i oprogramowania służącego do przetwarzania informacji obejmującego ich rodzaj i konfigurację w formie elektronicznej przy wykorzystaniu pakietu Office.

Badaniem kontrolnym, pod względem zainstalowanego oprogramowania (pakiet biurowy) poddano 1 zestaw komputerowy – nie stwierdzono nieprawidłowości - akta kontroli str. 197-198, 234.

W ramach prawidłowego zarządzania bezpieczeństwem informacji podmioty realizujące zadania publiczne zobowiązane są do podejmowania 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 oraz bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań - § 20 ust. 2 pkt 4-5.

Zasady obowiązujące przy nadawaniu i cofnięciu uprawnień do przetwarzania informacji uregulowano w Procedurze kontroli dostępu danych osobowych oraz Procedurze nadawania uprawnień do dostępu do danych osobowych.

Do przetwarzania dopuszczono osoby posiadające stosowne pisemne upoważnienie w zakresie nałożonych obowiązków. W systemie informatycznym przetwarzanie danych umożliwiono po założeniu indywidualnego konta dla każdego użytkownika zabezpieczonego hasłem – akta kontroli str. 52-53, 55-56, 80-82, 86-87.

W ramach kontroli powyższego obszaru dokonano przeglądu uprawnień do systemów i zasobów informatycznych dla 2 wybranych pracowników. Stwierdzono, że posiadali oni stosowne uprawnienia, adekwatne do realizowanych zadań określonych w zakresach obowiązków. W poszczególnych aplikacjach pracownicy posiadali indywidualne konta użytkowników, a wykonywane czynności odnotowały się w systemach (logi) - akta kontroli str. 199-208. Przy realizacji zadań związanych z nadawaniem uprawnień korzystano z poczty elektronicznej, aczkolwiek nie stosowano wzorów wniosków przewidzianych w „PB" – akta kontroli str. 235.

Zgodnie z § 20 ust. 2 pkt 6 jednostka podmiotu publicznego zobowiązana jest do zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

- *zagrożenia bezpieczeństwa informacji,*
- *skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,*
- *stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*

Jednostka kontrolowana zapewniła szkolenie pracowników zaangażowanych w proces przetwarzania informacji w zakresie ochrony danych osobowych. Zgodnie z ww. przepisem szkolenia winny obejmować pełen zakres informacji przetwarzanych w jednostce - akta kontroli str. 215-231.

Jednostka podmiotu publicznego ma obowiązek zapewnić ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, o czym mowa w § 20 ust. 2 pkt. 7, przez:

- *monitorowanie dostępu do informacji,*

- *czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,*
- *zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji*

oraz zabezpieczyć w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie - § 20 ust. 2 pkt 9. Ponadto do obowiązków jednostki podmiotu publicznego należy:

- *ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość (§ 20 ust. 2 pkt 8),*
- *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych (§ 20 ust. 2 pkt 11).*

Zasady postępowania mające na celu ochronę informacji w ww. zakresie jednostka kontrolowana zawarła w Procedurze kontroli dostępu danych osobowych.

W jednostce kontrolowanej nie wdrożono usług katalogowych Active Directory. Dostęp do systemów informatycznych i aplikacji posiadały jedynie osoby upoważnione z wykorzystaniem odpowiednich parametrów logowania - identyfikator i hasło. Pracowników zobligowano do tworzenia haseł o odpowiedniej złożoności i do zachowania ich w tajemnicy. Zastosowano mechanizm określający okres ważności hasła. Użytkownicy komputerów nie posiadali uprawnień administratorskich (akta kontroli str. 232-233).

Jednostka kontrolowana nie wdrożyła centralnego zbioru logów. Zdarzenia są zapisywane w poszczególnych aplikacjach przez określony czas, w zależności od możliwości technicznych i programowych. Przegląd logów wykonywany był w razie potrzeby. Czynność nie była dokumentowana - akta kontroli str. 234.

Kopie parametrów logowania do kluczowych elementów infrastruktury sieciowej były przechowywane w bezpieczny sposób w siedzibie jednostki w formie papierowej - akta kontroli str. 234.

W badanym okresie w jednostce kontrolowanej świadczona była praca zdalna przy wykorzystaniu VPN, zgodnie z procedurami określonymi w „PB". Prowadzona była lista użytkowników zdalnych, na laptopach zainstalowane było oprogramowanie umożliwiające bezpieczne połączenie. Stosowana była zasada szyfrowania dysków (BitLocker) - akta kontroli str. 138-240.

Jednostka kontrolowana posiada jedną lokalizację przy ul. Średzkiej 9. Dostęp do budynku uregulowano w Zarządzeniu Nr 498 Wójta Gminy Zaniemyśl z dnia 6 września 2022 r. w sprawie: wprowadzenia „Polityki kluczy w Urzędzie Gminy Zaniemyśl" (wcześniej Zarządzenie Nr 342 Wójta Gminy Zaniemyśl z dnia 18 listopada 2021 r). Stały dostęp do budynku posiadali wyznaczeni pracownicy, którzy dysponowali kodami dostępowymi do systemu alarmowego. Klucze do pomieszczeń biurowych były pobierane i zdawane na koniec dnia przez pracowników w sekretariacie (przechowywane były w bezpieczny sposób). Budynek wyposażono w zabezpieczenia przeciwwłamaniowe oraz przeciwpożarowe. Pomieszczenia biurowe oraz wyposażenie, w których przechowywano/

przetwarzano dane były chronione przed nieuprawnionym dostępem. Monitory ustawione były w sposób uniemożliwiający podgląd danych. Stosowana była zasada czystego biurka oraz wygaszacze ekranu – akta kontroli str. 236-237, 241.
Serwerownia zlokalizowana była w piwnicy budynku. Dostęp do pomieszczenia posiadały upoważnione osoby (informatyk). Serwerownia nie była wyposażona w system wentylacyjny oraz klimatyzację. Zabezpieczenie przeciwpożarowe stanowiła gaśnica. Przez pomieszczenie przebiegały rury co. Pomieszczenie nie miało również urządzeń do monitorowania i sygnalizowania wzrostu temperatury, co przy braku klimatyzacji i odpowiedniej wentylacji obniża poziom bezpieczeństwa informacji.
Dla zapewnienia bezpieczeństwa danych i zachowania ciągłości działania przy awariach zasilania z sieci elektrycznej (dla kluczowych elementów infrastruktury teleinformatycznej) serwerownię wyposażono w UPS. Kable sieciowe poprowadzone były natynkowo w korytkach. Dostęp do sieci Internet odbywał się poprzez łącze światłowodowe. Sieć Wi-Fi zabezpieczona była hasłem - akta kontroli str. 236-237.
Ponadto, w trakcie czynności kontrolnych ustalono, że uszkodzony sprzęt przekazywany był do naprawy bez dysku. Dane z dysków komputerów przeznaczonych do likwidacji zostały trwale usunięte. Dyski przechowywane były w bezpieczny sposób. W okresie objętym kontrolą jednostka nie przeprowadziła procedury likwidacyjnej.
Pracownicy użytkują wyłącznie służbowe pamięci zewnętrzne, które dopuszczone zostały do użytkowania, jednakże nie stosuje się mechanizmu kontroli podłączanych urządzeń, co wpływa na obniżenie poziomu bezpieczeństwa informacji - akta kontroli str. 234-235.

Elementem zachowania właściwego stopnia bezpieczeństwa informacji przez jednostkę podmiotu publicznego jest również stosowanie w umowach serwisowych ze stronami trzecimi odpowiednich zapisów gwarantujących jego poziom (§ 20 ust. 2 pkt 10).
Jednostka kontrolowana zawarła w odniesieniu do badanego systemu umowę opieki autorskiej oraz powierzenia przetwarzania danych osobowych (opisane w pkt 2). W umowie serwisowej nie zawarto zapisów dotyczących zachowaniu poufności i tajemnicy wszelkich informacji uzyskanych w trakcie realizacji umowy – akta kontroli str. 158-159.

Zapewnienie przez jednostkę podmiotu publicznego odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, o którym mowa w § 20 ust. 2 pkt 12, polega w szczególności na:

- *dbałości o aktualizację oprogramowania,*
- *minimalizowaniu ryzyka utraty informacji w wyniku awarii,*
- *ochronie przed błędami, utratą, nieuprawnioną modyfikacją,*
- *stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,*
- *zapewnieniu bezpieczeństwa plików systemowych,*
- *redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,*

- *niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,*
- *kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.*

W trakcie prowadzenia czynności kontrolnych w powyższym obszarze ocenie poddano działalność jednostki kontrolowanej w zakresie dbałości o aktualizację oprogramowania oraz minimalizacji utraty danych w wyniku awarii.

Jednostka kontrolowana użytkowała komputery z systemami operacyjnymi dla których producent zapewnił wsparcie/aktualizacje. Zabezpieczenie przed złośliwym oprogramowaniem zapewniał system antywirusowy. Programy dziedzinowe aktualizowane były przy instalacji nowej wersji oprogramowania. W ramach kontroli badaniu poddano system operacyjny i program antywirusowy na 1 komputerze oraz 1 serwerze - sygnatury wirusów były aktualne - akta kontroli str. 155, 242-244.

Jednostka kontrolowana posiadła brzegowe urządzenia sieciowe klasy UTM tj. FortiGate 30E na styku sieci Internet, na którym występuje główne zarządzanie dostępem do sieci i usług - sygnatury wirusów były aktualne - akta kontroli str. 245.

Jednostka kontrolowana zabezpieczyła kluczowe dane poprzez wykonywanie kopii zapasowych. Bazy danych kopiowane były codziennie na dodatkowym dysku w serwerze oraz urządzeniu NAS Qnap z funkcjonalnością migawkowania. Dodatkowo raz na dwa tygodnie dane zgrywano na dysk zewnętrzny, który był przechowywany w szafie pancernej w innym pomieszczeniu. Procedury sprawdzania poprawności wykonania kopii zapasowych nie były dokumentowane – akta kontroli str. 235, 246.

Spośród innych procedur istotnych z punktu widzenia bezpieczeństwa informacji nie opracowano szczegółowych procedur zachowania ciągłości działania, które są środkiem minimalizującym ryzyko utraty informacji np. w wyniku awarii - § 20 ust. 2 pkt 12 lit. b. W jednostce kontrolowanej funkcjonowała procedura „Zarządzanie ciągłością działania" na dużym poziomie ogólności i nie można jej traktować jako planu awaryjnego – akta kontroli str. 247.

Przepis § 20 ust. 2 pkt 13 nakłada obowiązek bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Jednostka kontrolowana określiła zasady postępowania w ww. zakresie wyłącznie w odniesieniu do naruszenia ochrony danych osobowych – Procedura Zarządzania incydentami związanymi z bezpieczeństwem danych osobowych - załącznik Nr 4 do „PB". W przyjętych regulacjach sklasyfikowano incydenty i naruszenia oraz opracowano zasady postępowania w przypadku ich zaistnienia (obowiązek zgłoszenia, zabezpieczenie dowodów zdarzenia, raportowanie). W okresie objętym kontrolą nie odnotowano naruszeń ochrony danych osobowych – akta kontroli str. 69-73, 234.

Zawężenie procedury zgłaszania incydentów jedynie do ochrony danych osobowych, ogranicza ilość informacji o zagrożeniach jakie winny być zgłaszane przez pracowników

w związku z wystąpieniem niepożądanych zdarzeń przy przetwarzaniu informacji i może skutkować brakiem działań dot. nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, o których mowa w § 20 ust. 2 pkt 12 lit. f.

W badanym okresie jednostka kontrolowana przeprowadziła audyt wewnętrzny w zakresie bezpieczeństwa informacji w 2021 r. Do listopada 2022 r. zaplanowane zostało przeprowadzenie audytu pn. „Diagnoza cyberbezpieczeństwa"- jednostka kontrolowana była na etapie przeprowadzenia procedury mającej na celu wyłonienie wykonawcy, tym samym została wypełniona dyspozycja § 20 ust. 2 pkt 14, która nakłada dokonanie ww. czynności nie rzadziej niż raz na rok – akta kontroli str. 235, 248-261.

Ogólna ocena kontrolowanego obszaru – pozytywna z nieprawidłowościami.

4. Dostosowanie stron dla osób niepełnosprawnych.

*Zgodnie z § 19 „KRI", w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące do prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines *WCAG 2.1), z uwzględnieniem poziomu AA.*

W ramach czynności kontrolnych dokonano weryfikacji zgodności strony internetowej jednostki kontrolowanej oraz BIP ze standardem WCAG 2.1, w zakresie zasady 4 – Kompatybilności (Parsowanie) z uwzględnieniem poziomu AA, poprzez wykorzystanie narzędzia dostępowego na stronie http://validator.w.3.org. Badanie wykazało[1]:

- na stronie głównej: 0 błędów i 0 ostrzeżeń (zał. Nr 1),
- na stronie BIP: 0 błędów i 0 ostrzeżeń (zał. Nr 2) - akta kontroli str. 262-264.

Ponadto, przetestowaniu poddano następujące obszary:

STRONA GŁÓWNA				
Obszar	Wyniki testu			Uwagi
	Spełnia wymogi	Nie spełnia wymogów	Nie dotyczy	
1.1.1 Zapewnione są opisy lub teksty alternatywne dla treści nietekstowych, głównie zdjęć i innych obrazów niosących treść		X		zał. Nr 3
1.4.3 Tekst posiada kontrast wynoszący przynajmniej 4,5:1 (3:1 w przypadku dużych	X			zał. Nr 4 (spełnia jedynie w

[1] Raport z badania dostosowania stron internetowych dla osób niepełnosprawnych (WCAG 2.1) przekazany jednostce kontrolowanej w dniu przeprowadzenia czynności kontrolnych tj. 8.09.2022 r.

tekstów) w stosunku do elementów sąsiadujących i tła. Nie dotyczy logotypów lub części logotypów.				wersji kontrastowej)
2.4.7 Fokus elementów jest wyraźnie widoczny.	X			zał. Nr 5

STRONA BIP

Obszar	Wyniki testu			Uwagi
	Spełnia wymogi	Nie spełnia wymogów	Nie dotyczy	
1.1.1 Zapewnione są opisy lub teksty alternatywne dla treści nietekstowych, głównie zdjęć i innych obrazów niosących treść			X	
1.4.3 Tekst posiada kontrast wynoszący przynajmniej 4,5:1 (3:1 w przypadku dużych tekstów) w stosunku do elementów sąsiadujących i tła. Nie dotyczy logotypów lub części logotypów.	X			zał. Nr 6
2.4.7 Fokus elementów jest wyraźnie widoczny.	X			zał. Nr 7

-akta kontroli str. 262, 265-269.

Ogólna ocena kontrolowanego obszaru – pozytywna z nieprawidłowościami.

W wyniku kontroli stwierdzono następujące uchybienia i nieprawidłowości:

1. Niedostateczny poziom informacji w zakresie usług świadczonych drogą elektroniczną, na który składa się nieumieszczenie w serwisach internetowych wyodrębnionego katalogu usług świadczonych drogą elektroniczną wraz z opisem procedur obowiązujących przy ich załatwianiu oraz danych dot. maksymalnego rozmiaru dokumentu elektronicznego wraz załącznikami, wyrażonym w magabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, zakresach użytkowych dokumentów elektronicznych tworzonych na podstawie wzorów umieszczonych przez te podmioty w centralnym repozytorium, rodzaju informatycznych nośników danych, na których może zostać doręczony dokument elektroniczny i zapisane urzędowe poświadczenie odbioru, co stanowi niewykonanie obowiązku nałożonego przez § 3 ust. 1 pkt 2-6 „rozporządzenia o doręczaniu dokumentów elektronicznych" i uniemożliwia

skuteczne zapoznanie się z obowiązującymi regułami przy realizacji usług elektronicznych.

2. Opracowane i wdrożone regulacje dotyczące zagadnień związanych z zarządzaniem bezpieczeństwem informacji nie obejmowały wszystkich informacji jakie są przetwarzane w jednostce, lecz dotyczyły głównie danych osobowych, tym samym nie została wypełniona dyspozycja § 20 ust. 1 KRI.
3. Nadanie w wewnętrznych regulacjach IOD, uprawnień sprzecznych z zapisami art. 39 ust. 1 lit. b) RODO, co skutkuje konfliktem interesów i godzi w zasadę niezależności jego funkcjonowania.
4. Niestosowanie przyjętych w „PB" wzorów dokumentów związanych z nadawaniem dostępów do systemów informatycznych i upoważnień do przetwarzania danych osobowych.
5. Nieobjęcie tematyką szkoleń wszystkich rodzajów przetwarzanych informacji może skutkować wzrostem incydentów związanych z ich bezpieczeństwem informacji i tym samym obniżać jego poziom.
6. Obniżenie poziomu bezpieczeństwa fizycznego ze względu na brak w serwerowni klimatyzacji.
7. Brak mechanizmu kontrolującego użytkowanie pamięci zewnętrznych obniża poziom bezpieczeństwa informacji i może skutkować wyciekiem danych.
8. Brak w umowie dot. serwisu oprogramowania zapisów o poufności i zachowaniu w tajemnicy wszelkich udostępnionych informacji, co jest niezgodne z § 20 ust. 2 pkt 10 KRI i skutkuje obniżeniem poziomu bezpieczeństwa informacji.
9. Ograniczenie procedury zgłaszania incydentów do naruszeń ochrony danych osobowych, może uniemożliwić szybkie podjęcie działań korygujących w zakresie szeroko rozumianych incydentów teleinformatycznych.
10. Brak szczegółowej procedury ciągłości działania. Nieopracowanie zasad w tym zakresie może skutkować zaburzeniem płynności procesu przywracania do działania kluczowych aktywów jednostki po awarii lub katastrofie.
11. Nie zapewniono prawidłowych opisów dla treści nietekstowych w zakresie spełnienia wymagań WCAG 2.1., o których mowa w ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2019 r., poz. 848).

Biorąc pod uwagę oceny zawarte w wystąpieniu pokontrolnym wnoszę o:

1. Zamieszczenie w serwisach internetowych opisów procedur obowiązujących przy załatwianiu spraw drogą elektroniczną i informacji dot. maksymalnego rozmiaru dokumentu elektronicznego wraz załącznikami, wyrażonym w magabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, zakresach użytkowych dokumentów elektronicznych tworzonych na podstawie wzorów umieszczonych przez te podmioty w centralnym repozytorium, rodzaju informatycznych nośników danych, na których może zostać doręczony dokument elektroniczny i zapisane urzędowe

poświadczenie odbioru zgodnie z przepisami rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz. U. z 2018 r. poz. 180).

2. Stworzenie w serwisach internetowych wyodrębnionego katalogu usług świadczonych drogą elektroniczną.
3. Opracowanie i wdrożenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji (Polityka Bezpieczeństwa Informacji), uwzględniającego wszelkie przetwarzane w jednostce informacje.
4. Usunięcie z „PB" uprawnień IOD sprzecznych z zapisami art. 39 ust. 1 lit. b) RODO.
5. Stosowanie przyjętych w „PB" wzorów dokumentów.
6. Ujęcie w tematyce szkoleń z zakresu bezpieczeństwa wszystkich rodzajów informacji przetwarzanych w jednostce.
7. W miarę posiadania środków wyposażyć serwerownie w klimatyzację.
8. Wprowadzenie mechanizmu kontroli korzystania z pamięci zewnętrznych.
9. Zawieranie w umowach serwisowych klauzul o poufności i zachowaniu tajemnicy wszelkich udostępnianych informacji.
10. Objęcie wszystkich incydentów związanych z bezpieczeństwem informacji procedurą ich zgłaszania.
11. Opracowanie procedury ciągłości działania.
12. Umieszczenie prawidłowych opisów dla treści nietekstowych zgodnie z wymogami WCAG 2.1.

Proszę o przekazanie informacji o sposobie wykonania zaleceń, a także o podjętych działaniach lub przyczynach ich niepodjęcia w terminie 30 dni od daty doręczenia niniejszego wystąpienia pokontrolnego.

Wojewoda Wielkopolski
(-) Michał Zieliński

Podpis elektroniczny zweryfikowany w dniu 11.10.22
ważny/~~nieważny/brak możliwości weryfikacji~~
Inspektor ds. oc i p/poz
Adam [illegible]orski