WOJEWODA MAZOWIECKI

Warszawa, 15 lutego 2018 r.

WK-I.431.12.2.2017

Pani
Marzena Dębowska
Mazowiecki Wojewódzki Inspektor
Nadzoru Budowlanego

Ul. Czereśniowa 98
02-456 Warszawa

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 6 ust. 4 pkt 3 ustawy o kontroli w administracji rządowej[1] i art. 28 ust. 1 pkt 2 ustawy o wojewodzie i administracji rządowej w województwie[2], a także art. 25 ust. 1 pkt 3 lit. b ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[3], Marta Skrzecz, Katarzyna Możdżyńska – inspektorzy wojewódzcy w Wydziale Kontroli oraz Łukasz Plaskot – starszy inspektor wojewódzki w Biurze Informatyki i Rozwoju Systemów Informatycznych[4], przeprowadzili w dniach od 6 do 21 listopada 2017 r. kontrolę w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Warszawie, z siedzibą przy ul. Czereśniowej 98.

Kontrolą objęto stan realizacji zadań dotyczących działania systemów teleinformatycznych używanych do realizacji zadań publicznych albo realizacji obowiązków wnikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej – w okresie od 1 stycznia 2016 r. do 17 października 2017 r.

Nawiązując do projektu wystąpienia pokontrolnego z 22 stycznia 2018 r., do którego nie wniesiono zastrzeżeń, przekazuję Pani wystąpienie pokontrolne.

---

1 Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092).
2 Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2017 r. poz. 2234).
3 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570).
4 Obecnie w Biurze Obsługi Urzędu.

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 dwa systemy teleinformatyczne używane w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Warszawie (dalej WINB) do realizacji zadań publicznych tj. system Elektronicznego Zarządzania Dokumentacją (dalej EZD) oraz system RESAK-BUD. W jednostce nie prowadzono rejestrów publicznych, o których mowa w art. 14 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

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

Na stronie Biuletynu Informacji Publicznej (dalej BIP) WINB udostępniono Elektroniczną Skrzynkę Podawczą znajdującą się na elektronicznej Platformie Usług Administracji Publicznej (dalej ePUAP), umożliwiającą doręczanie pism w formie dokumentów elektronicznych wraz ze wskazaniem jej adresu w formie identyfikatora URI, czym spełniono wymogi art. 16 ust. 1a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz § 3 ust. 1 pkt 1 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[5]. WINB umożliwił przyjmowanie dokumentów elektronicznych służących do załatwiania spraw w formatach danych określonych w załączniku nr 2 i 3 do rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (dalej rozporządzenie w sprawie KRI).[6]

Na stronie BIP WINB, w zakładce *Skargi i wnioski* zamieszczono informację o możliwości składania do urzędu skarg i wniosków pocztą elektroniczną na adres kancelarii, a także za pośrednictwem platformy ePUAP. W ww. zakładce umieszczono link przekierowujący użytkownika bezpośrednio do usługi *Skargi, wnioski, zapytania do urzędu* na platformie ePUAP.

[5] Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, worów i kopii dokumentów elektronicznych (Dz. U. z 2015 r. poz. 971, z późn. zm.).

[6] 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).

Znajduje się tam między innymi opis świadczonej usługi, co umożliwia skuteczne zapoznanie się z informacją o sposobie dostępu oraz zakresie użytkowym serwisów dla usługi realizowanej przez jednostkę. Informacja o Elektronicznej Skrzynce Podawczej oraz link do usługi *Skargi, wnioski, zapytania do urzędu* został zamieszczony również na stronie BIP jednostki w zakładce *Elektroniczna Skrzynka Podawcza*. Powyższe spełnia wymogi określone w § 5 ust. 2 pkt 1 i 4 rozporządzenia w sprawie KRI oraz wskazuje na zastosowanie modelu usługowego, zdefiniowanego w § 2 pkt 8 rozporządzenia w sprawie KRI.

Ponadto ustalono, że WINB przekazał do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych (dalej CRWDE) wniosek o publikację wzoru dokumentu elektronicznego dla usługi Zażalenie na niezałatwienie sprawy w terminie lub na przewlekłe prowadzenie postępowania przez powiatowego inspektora nadzoru budowlanego, zgodnie z art. 19b ust. 3 ustawy o informatyzacji. Jednakże z uwagi m.in. na nieprecyzyjnie oznaczoną nazwę podmiotu w profilu konta ePUAP ww. wzór nie został opublikowany.

Stwierdzono, że system teleinformatyczny EZD powiązany jest z platformą ePUAP. Komunikacja pomiędzy systemami jest automatyczna, a do zabezpieczeń wykorzystywany jest certyfikat zapewniany przez podmiot odpowiedzialny za działanie platformy ePUAP. Współpraca pomiędzy systemami jest możliwa dzięki wyposażaniu WINB w odpowiedni sprzęt oraz oprogramowanie umożliwiające wymianę danych między systemami, zgodnie z § 16 ust. 1 rozporządzenia w sprawie KRI. Kodowanie znaków w wysyłanych z systemów lub odbieranych przez te systemy dokumentach odbywa się według standardu Unicode UTF-8, zgodnie z § 17 ust. 1 ww. rozporządzenia.

Zgodnie z zarządzeniem Nr 13/15 Mazowieckiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 29 września 2015 r. *w sprawie wdrożenia elektronicznego systemu zarządzania dokumentacją w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Warszawie* czynności kancelaryjne w jednostce wykonywane są w systemie tradycyjnym, który jest podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw, a EZD służy do realizowania czynności kancelaryjnych. Ponadto załącznik nr 1 do ww. zarządzenia zawiera wykaz klas z jednolitego rzeczowego wykazu akt stanowiących wyjątki od podstawowego sposobu dokumentowania przebiegu załatwiania spraw w WINB, tj. sprawy dokumentowane wyłącznie w systemie EZD.

W wyniku kontroli stwierdzono **nieprawidłowość** polegającą na nieumieszczeniu na stronie BIP pełnej informacji o warunkach organizacyjno-technicznych doręczania dokumentów elektronicznych, czym naruszono wymogi określone w § 3 ust. 1 pkt 2-5 rozporządzenia w sprawie

sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.

Ponadto ustalono, że w WINB nie zadeklarowano poziomu świadczenia usług elektronicznych poprzez określenie wskaźników ich dostępności oraz nie prowadzono monitoringu poziomu ich świadczenia, czym naruszono wymogi § 15 ust. 2 rozporządzenia w sprawie KRI.

Przedstawiając powyższe informuję, że realizację zadań dotyczących wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami oraz wspomaganie usług drogą elektroniczną **ocenia się pozytywnie pomimo stwierdzonej nieprawidłowości.**

Ustalenia kontroli wykazały, że w WINB udostępniono elektroniczną skrzynkę podawczą zintegrowaną z systemem EZD oraz zapewniono jej obsługę, używanym systemom teleinformatycznym zapewniono interoperacyjność na poziomie organizacyjnym, zastosowano model usługowy dla systemów teleinformatycznych oraz prawidłowo zarządzano obiegiem dokumentacji w jednostce. Mając natomiast na uwadze nieumieszczenie na stronie BIP pełnej informacji o warunkach organizacyjno-technicznych doręczania dokumentów elektronicznych oraz powyższe uchybienie uzasadnione jest sformułowanie oceny pozytywnej pomimo stwierdzonej nieprawidłowości.

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

W WINB wprowadzono *Politykę Bezpieczeństwa przetwarzania i ochrony danych osobowych* oraz *Instrukcję zarządzania systemem informatycznym RESAK-BUD (włącznie z modułem ASYSTENT),* stanowiące załączniki do Zarządzenia Nr 17/05 Mazowieckiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 30 grudnia 2005 r. W *Polityce bezpieczeństwa przetwarzania i ochrony danych osobowych* określono zasady regulujące sposób zarządzania, ochrony i dystrybucji informacji zawierających dane osobowe oraz procedury postępowania w sytuacji naruszenia poufności danych. Powyższy dokument zawiera również wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, struktury danych osobowych przetwarzanych w WINB oraz opis środków fizycznej ochrony danych osobowych. Natomiast w *Instrukcji zarządzania systemem informatycznym RESAK-BUD (włącznie z modułem ASYSTENT)* określono sposób zarządzania aplikacją RESAK-BUD oraz zasady użytkowania ww. aplikacji, w szczególności: procedury nadawania uprawnień nowym użytkownikom, zmiany zakresu uprawnień istniejących użytkowników, zasady bezpiecznej pracy z aplikacją, obowiązki użytkowników, sposoby zabezpieczenia danych wprowadzanych

do aplikacji. W powyższym dokumencie wyszczególniono funkcje: Administratora Danych – którym jest Mazowiecki Wojewódzki Inspektor Nadzoru Budowlanego, Administratora systemu – którym jest osoba upoważniona przez Administratora Danych do zarządzania systemem RESAK-BUD, Naczelnika Wydziału – którym jest również pracownik koordynujący pracę zespołu.

Ponadto w WINB obowiązywało Zarządzenie Nr 3/16 Mazowieckiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 18 stycznia 2016 r. w sprawie wdrożenia procedury *Bezpieczne przetwarzanie danych w JAR w systemie EZD funkcjonującym w ramach infrastruktury MUW*[7]. W ww. procedurze określono zasady korzystania oraz zarządzania systemem EZD w jednostkach administracji rządowej. Powyższy dokument ma za zadanie zapewnienie bezpieczeństwa danych przetwarzanych w systemie. Procedura swoim zakresem obejmuje wszystkie jednostki administracji rządowej. Z ww. procedurą pracownicy zostali zapoznani poprzez udostępnienie jej w systemie EZD, dodatkowo nowo zatrudnieni pracownicy zapoznają się z powyższym dokumentem podczas szkoleń z obsługi przedmiotowego systemu.

W toku kontroli potwierdzono zaangażowanie kierownictwa jednostki w proces ustanawiania i funkcjonowania systemu bezpieczeństwa informacji m.in. poprzez dokonanie analizy ryzyka, a także przeznaczanie środków na zakup nowego systemu monitoringu wizyjnego i utworzenie strefy dostępnej wyłącznie dla pracowników WINB.

W 2017 r., w jednostce dokonano identyfikacji i analizy ryzyka w obszarze bezpieczeństwa informacji, stosownie do wymogów określonych w § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI.

W *Instrukcji zarządzania systemem informatycznym RESAK-BUD (włącznie z modułem ASYSTENT) oraz* procedurze *Bezpieczne przetwarzanie danych w JAR w systemie EZD funkcjonującym w ramach infrastruktury MUW* uregulowano proces nadawania uprawnień do pracy w systemach teleinformatycznych, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI.

Stosownie do § 20 ust. 2 pkt 6 ww. rozporządzenia zapewniono szkolenia osób zaangażowanych w proces przetwarzania informacji. Zakres tematyczny szkoleń obejmował m.in. zagadnienia związane z cyberbezpieczeństwem, rodzajami złośliwego oprogramowania i incydentami w obszarze cyberbezpieczeństwa.

W okresie objętym kontrolą nie wystąpiły przypadki projektowania i wdrażania systemów teleinformatycznych.

[7] Procedura ISO Mazowieckiego Urzędu Wojewódzkiego w Warszawie.

W powyższym okresie wystąpił jeden incydent naruszenia bezpieczeństwa informacji[8], który został bezzwłocznie zgłoszony przez pracownika Naczelnikowi Wydziału Administracyjno-Organizacyjnego oraz Administratorowi Sieci Informatycznej. Podjęte działania zapobiegły rozprzestrzenieniu się złośliwego oprogramowania w sieci wewnętrznej jednostki.

Zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji zawarto w *Polityce Bezpieczeństwa przetwarzania i ochrony danych osobowych* oraz *Instrukcji zarządzania systemem informatycznym RESAK-BUD (włącznie z modułem ASYSTENT)* oraz w procedurze *Bezpieczne przetwarzanie danych w JAR w systemie EZD funkcjonującym w ramach infrastruktury MUW,* zgodnie z § 20 ust. 2 pkt 11 rozporządzenia w sprawie KRI.

W toku kontroli ustalono, że zgodnie z § 20 ust. 2 pkt 7, 9 i 12 ww. rozporządzenia, WINB zapewnia ochronę przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenie informacji w sposób uniemożliwiający osobom nieuprawnionym jej ujawnienie, modyfikację, usunięcie lub zniszczenie, poprzez:

- stosowanie zabezpieczeń do budynku i pomieszczeń, przy użyciu ochrony fizycznej, monitoringu wizyjnego[9], a także poprzez wydzielenie strefy, do której mają dostęp wyłącznie pracownicy jednostki, w której znajduje się np. serwerownia[10] oraz wydawanie kluczy wyłącznie osobom uprawnionym,
- demontowanie dysków twardych z urządzeń komputerowych przekazywanych do utylizacji,
- wykonywanie kopii zapasowych serwerów,
- nadawanie użytkownikom uprawnień do systemów na podstawie upoważnień i ustnych ustaleń,
- ograniczenie uprawnień użytkowników na stacjach roboczych,
- zabezpieczenie komputerów użytkowników aktualnym oprogramowaniem antywirusowym, automatycznie aktualizującym sygnatury wirusów,
- stosowanie mechanizmów kryptograficznych,

---

[8] Zgodnie z wyjaśnieniami Zastępcy Mazowieckiego Wojewódzkiego Inspektora Nadzoru Budowlanego z 10 listopada 2017 r. cyt.: *„(…)* [redacted] *(…)”*.

[9] Zgodnie z wyjaśnieniami Zastępcy Mazowieckiego Wojewódzkiego Inspektora Nadzoru Budowlanego z 10 listopada 2017 r. cyt.: *„Siedziba WINB mieści się w pomieszczeniach* [redacted] *(…)”*.

[10] Dostęp do pomieszczeń serwerowni [redacted]

- automatyczną aktualizację oprogramowania systemów operacyjnych komputerów,
- wyposażenie serwerów i urządzeń sieciowych w zasilanie awaryjne zabezpieczające system przed przepięciami i chwilowymi zanikami napięcia.

Wykorzystywany w WINB system EZD zapewnia rozliczalność operacji poprzez gromadzenie informacji o wykonanych czynnościach w dziennikach systemowych. W stosunku do ww. systemu przeglądu logów dokonują pracownicy Mazowieckiego Urzędu Wojewódzkiego w Warszawie, natomiast w przypadku systemu RESAK-BUD jednostka nie posiada informacji w ww. zakresie[11].

W wyniku kontroli stwierdzono **następujące nieprawidłowości**:

1. Nieopracowanie kompleksowej dokumentacji systemu zarządzania bezpieczeństwem informacji. W jednostce wprowadzono *Politykę Bezpieczeństwa przetwarzania i ochrony danych osobowych* oraz *Instrukcję zarządzania systemem informatycznym RESAK-BUD (włącznie z modułem ASYSTENT),* a także procedurę *Bezpieczne przetwarzanie danych w JAR w systemie EZD funkcjonującym w ramach infrastruktury MUW*, jednakże w zawężeniu wyłącznie do ochrony danych osobowych oraz dwóch systemów teleinformatycznych. Należy zwrócić uwagę, że system zarządzania bezpieczeństwem informacji odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. Podmiot publiczny, aby zapewnić bezpieczeństwo informacji działania systemów teleinformatycznych winien zastosować podejście systemowe, w ramach którego będzie zarządzał kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji. Kompleksowość podejścia oznacza objęcie systemem zarządzania bezpieczeństwem informacji całej organizacji wraz ze wszystkimi systemami teleinformatycznymi i procesami przetwarzania informacji w niej zachodzącymi.

   Ponadto niezaktualizowano funkcjonujących w jednostce regulacji wewnętrznych, pomimo zmiany otoczenia polegającej na wydzieleniu strefy, do której dostęp mają wyłącznie pracownicy jednostki oraz wejścia w życie przepisów dotyczących spełnienia minimalnych wymagań dla systemów teleinformatycznych[12]

   Powyższym naruszono regulację § 20 ust. 1 rozporządzenia w sprawie KRI, zgodnie z którą cyt.: *„Podmiot realizujący zdania publiczne opracowuje i ustanawia, wdraża*

[11] Umowa o nadzór autorski nad pakietem oprogramowania [redacted]

[12] Rozdział IV rozporządzenia KRI.

i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność" oraz § 20 ust. 2 pkt 1, zgodnie z którą cyt.: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (…) 1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia (…)".*

2. Niezapewnienie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, czym naruszono § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI.
3. Nadanie uprawnień do pracy w systemie EZD, w trzech przypadkach[13], pomimo braku upoważnień do przetwarzania danych osobowych, czym naruszono dyspozycję § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI, zgodnie z którą kierownictwo podmiotu publicznego umożliwia realizację i egzekwowanie działań w zakresie cyt.: „(…) *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*".
4. Zablokowanie dostępu do ośmiu kont[14] w systemie EZD po upływie od 5 dni do 8 miesięcy od dnia rozwiązania stosunku pracy, czym naruszono regulację § 20 ust. 2 pkt. 5 rozporządzenia w sprawie KRI, zgodnie z którą cyt.: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację*

[13] W przypadku [redacted]. Zgodnie z wyjaśnieniami Mazowieckiego Wojewódzkiego Inspektora Nadzoru Budowlanego z 20 listopada 2017 r. cyt.: *„(…) w przypadku* [redacted] *Spowodowane to zostało znacznym spiętrzeniem zadań (…), co skutkowało niedopatrzeniem w tym przypadku*".

[14] Zgodnie z wyjaśnieniami Mazowieckiego Wojewódzkiego Inspektora Nadzoru Budowlanego z 20 listopada 2017 r. cyt.: *„(…) Najprawdopodobniej przyczyną takiego stanu rzeczy było zbyt duże obciążenie pracą wszystkich pracowników odpowiedzialnych za terminowe wykonanie czynności w tym obszarze (…)*".

i egzekwowanie następujących działań: (…) 5) bezzwłoczne zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4 (…)".

5. Nieustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, pomimo wykorzystywania urządzeń mobilnych, takich jak komputery przenośne poza siedzibą jednostki[15] oraz dostępu zdalnego umożliwiającego pracę na odległość jednemu z pracowników jednostki[16]. Powyższym naruszono wymóg § 20 ust. 2 pkt 8 rozporządzenia w sprawie KRI.
6. Niezawarcie w dwóch umowach[17] zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Działaniem takim naruszono wymóg § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI, zgodnie z którym kierownictwo podmiotu publicznego umożliwia realizację i egzekwowanie działań w zakresie cyt.: *„zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji".*
7. Nieprzeprowadzenie w okresie objętym kontrolą okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji. Zaniechaniem takim naruszono dyspozycję § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI, zgodnie z którą kierownictwo podmiotu publicznego umożliwia realizację i egzekwowanie działań w zakresie cyt.: *„zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok".*

Ponadto w wyniku kontroli stwierdzono, że:

- kopie zapasowe serwerów przechowywane są w miejscu ich utworzenia, przez co nie jest możliwe uniknięcie uszkodzeń spowodowanych przez katastrofę, która dotknęłaby ośrodek podstawowy przetwarzania danych, dodatkowo wymagane jest regularne testowanie jakości kopii zapasowych poprzez odtworzenie systemu informatycznego z kopii, zwykle na niezależnym od środowiska produkcyjnego sprzętowym środowisku testowym

[15] Zgodnie z wyjaśnieniami Zastępcy Mazowieckiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 10 listopada 2017 r. cyt.: *„(…)* [redacted]".

[16] Zgodnie z protokołem z rozmowy przeprowadzonej 15 listopada 2017 r. z właścicielem firmy zajmującej się obsługą informatyczną jednostki [redacted]

[17] Dotyczy umowy nr 12/2012 z 17 grudnia 2012 r. o nadzór autorski nad pakietem oprogramowania RESAKBUD wraz z aneksem nr 1 z 7 stycznia 2014 r. oraz aneksem nr 2 z 19 grudnia 2014 r., a także umowy nr 1/15 z 12 stycznia 2015 r. w przedmiocie obsługi informatycznej wraz z aneksem nr z 8 stycznia 2016 r. i aneksem nr 2 z 30 grudnia 2016 r.

oraz testowaniu pracy użytkowej odtworzonego systemu[18], natomiast kontrolowana jednostka nie wykonuje okresowych testów odtworzeniowych. Powyższym naruszono wymóg § 20 ust. 2 pkt 12 lit. b rozporządzenia w sprawie KRI, tj. cyt.: *„(…) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: (…) b) minimalizowaniu ryzyka utraty informacji w wyniku awarii (…)”*,

- w jednostce nie uregulowano sposobu zgłaszania i postępowania w przypadku zaistnienia incydentów naruszenia bezpieczeństwa informacji[19], czym naruszono wymóg § 20 ust. 2 pkt 13 ww. rozporządzenia,
- w umowie o nadzór autorski[20], zawartej pomiędzy WINB a podmiotem zewnętrznym, nie określono poziomu niezawodności, w tym parametrów SLA na usługi serwisowe, takich jak wymagany poziom dostępności oraz sposób jego monitorowania i raportowania, czym naruszono dyspozycję § 15 ust. 1 rozporządzenia w sprawie KRI, zgodnie z którym cyt.: „*Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich (…) niezawodności (…) przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk*”.

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

Ustalenia kontroli wykazały, że w WINB przeprowadzono analizę ryzyka utraty integralności, dostępności lub poufności informacji, zapewniono szkolenie osób zaangażowanych w proces przetwarzania informacji, zgłoszono incydent naruszenia bezpieczeństwa informacji oraz zastosowano odpowiednie zabezpieczenia techniczno-organizacyjne systemów teleinformatycznych.

Mając natomiast na uwadze, że w wyniku kontroli stwierdzono, że:

- opracowana w jednostce dokumentacja dotycząca polityki bezpieczeństwa nie regulowała w wystarczający sposób zagadnień związanych z bezpieczeństwem informacji oraz nie była aktualizowana w zakresie zmieniającego się otoczenia,

[18] Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, opracowane przez Ministerstwo Cyfryzacji. Warszawa, 15 grudnia 2015 r.

[19] Zagadnienie dotyczące postępowania z incydentami naruszenia bezpieczeństwa informacji zostało uregulowane jedynie w stosunku do systemu EZD, w procedurze „*Bezpieczne przetwarzanie danych w JAR w systemie EZD funkcjonującym w ramach infrastruktury MUW*”.

[20] Dotyczy umowy Nr 12/2012 z 17 grudnia 2012 r. o nadzór nad pakietem oprogramowania RESAK-BUD, wraz z aneksami nr 1 z 7 stycznia 2014 r. oraz aneksem nr 2 z 19 grudnia 2014 r.

- nie zapewniono aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
- nadano uprawnienia do pracy w systemie EZD pracownikom nieposiadającym upoważnień do przetwarzania danych osobowych oraz nie odebrano, w sposób bezzwłoczny, uprawnień pracownikom, z którymi rozwiązano stosunek pracy,
- nie ujęto w umowach zapisów gwarantujących odpowiedni poziom bezpieczeństwa,
- nie przeprowadzono audytu wewnętrznego w zakresie bezpieczeństwa informacji,
- nie podjęto odpowiednich działań związanych z przechowywaniem oraz testowaniem kopii zapasowych, minimalizujących ryzyko utraty informacji w wyniku awarii,

oraz powyższe uchybienia uzasadnione jest sformułowanie oceny negatywnej.

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

Stronę internetową oraz stronę BIP WINB działające pod adresami www.maz.winb.gov.pl[21] oraz www.bip.maz.winb.gov.pl poddano weryfikacji zgodności ze standardem WCAG 2.0 za pomocą walidatorów http://validator.w3.org oraz http://jigsaw.w3.org/css-validator/. Wskazane, w wyniku weryfikacji ww. stron internetowych, błędy i ostrzeżenia, nie miały wpływu na prezentowane treści.

W wyniku kontroli stwierdzono, że ww. strony internetowe jednostki są częściowo dostosowane do odbioru ich treści przez osoby z niepełnosprawnościami, tj. zawierały rozwiązania techniczne umożliwiające osobom niedowidzącym zapoznanie się z treścią informacji poprzez zmianę kontrastu oraz wielkości liter, czym naruszono wymogi określone w § 19 rozporządzenia w sprawie KRI.

Przedstawiając powyższe informuję, że realizację zadań w zakresie zapewnienia dostępności informacji zawartych na stronach internetowych jednostki dla osób niepełnosprawnych **ocenia się pozytywnie pomimo stwierdzonego uchybienia.**

[21] W dniu 2 stycznia 2018 r. Naczelnik Wydziału Administracyjno-Organizacyjnego przesłał do Wydziału Kontroli e-mail z informacją o umieszczeniu w sieci nowej strony internetowej WINB, która została dostosowana do potrzeb osób niepełnosprawnych, w związku z powyższym odstępuje się od sformułowania nieprawidłowości w przedmiotowym zakresie.

Przedstawiając powyższe ustalenia zobowiązuję Panią do podjęcia działań w celu wyeliminowania stwierdzonych w trakcie kontroli nieprawidłowości, a w szczególności do:

- umieszczenia na stronie BIP jednostki pełnej informacji o warunkach organizacyjno-technicznych doręczania dokumentów elektronicznych, określonych w § 3 ust. 1 pkt 2-5 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych,
- opracowania kompleksowej polityki bezpieczeństwa informacji obejmującej system zarządzania bezpieczeństwem informacji całej organizacji wraz ze wszystkimi systemami teleinformatycznymi i procesami przetwarzania informacji w niej zachodzącymi oraz zapewnienia jej aktualizacji w zakresie dotyczącym zmieniającego się otoczenia, w myśl § 20 ust. 1 i ust. 2 rozporządzenia w sprawie KRI,
- zapewnienia aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, zgodnie z § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI,
- nadawania uprawnień do pracy w systemie EZD, zgodnie z posiadanymi upoważnieniami do przetwarzania danych osobowych, stosownie do § 20 ust. 2 pkt 4 ww. rozporządzenia,
- bezzwłocznej zmiany uprawnień w systemie EZD w przypadku zmiany zadań lub rozwiązania stosunku pracy, zgodnie z § 20 ust. 2 pkt. 5 rozporządzenia w sprawie KRI,
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 8 ww. rozporządzenia,
- zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI,
- przeprowadzania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, zgodnie z dyspozycją § 20 ust. 2 pkt 14 rozporządzenia w sprawie KRI.

Ponadto wskazuję na konieczność:

- deklarowania poziomu świadczenia usług elektronicznych poprzez określenie wskaźników ich dostępności oraz prowadzenia monitoringu poziomu ich świadczenia, zgodnie z wymogami § 15 ust. 2 rozporządzenia w sprawie KRI,

- przechowywania kopii zapasowych serwerów w lokalizacji innej niż miejsce ich utworzenia oraz regularnego testowania ich jakości poprzez odtworzenie systemu informatycznego z kopii, na niezależnym od środowiska produkcyjnego sprzętowym środowisku testowym oraz testowania pracy użytkowej odtworzonego systemu w celu minimalizowania ryzyka utraty informacji w wyniku awarii, zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia w sprawie KRI,
- uregulowania sposobu zgłaszania i postępowania w przypadku zaistnienia incydentów naruszenia bezpieczeństwa informacji, stosownie do § 20 ust. 2 pkt 13 ww. rozporządzenia,
- określania w umowach zawartych pomiędzy jednostką a podmiotami zewnętrznymi poziomu niezawodności, w tym parametrów SLA na usługi serwisowe, takich jak wymagany poziom dostępności oraz sposób jego monitorowania i raportowania, w celu eksploatowania systemów z uwzględnieniem ich niezawodności przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk, zgodnie z dyspozycją § 15 ust. 1 rozporządzenia w sprawie KRI,
- dostosowania stron internetowych jednostki do odbioru ich treści przez osoby z niepełnosprawnościami poprzez spełnienie wymagań WCAG 2.0, zgodnie z wymogami określonymi w § 19 rozporządzenia w sprawie KRI.

Przedstawiając powyższe informuję, że zgodnie z art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze. Zobowiązuję Panią na podstawie art. 49 ww. ustawy do przekazania, w terminie 14 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, pisemnej informacji o sposobie wykonania zaleceń pokontrolnych albo innym sposobie usunięcia stwierdzonych nieprawidłowości.

z up. WOJEWODY MAZOWICKIEGO
Bogusław Krupa
Zastępca Dyrektora
Wydziału Kontroli