Warszawa, dnia ..6... lutego 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

BM-WSKN.0811.4.2016

Egz. Nr ..1..

Minister Nauki i Szkolnictwa Wyższego

WYSTĄPIENIE POKONTROLNE

z kontroli dotyczącej zgodności systemów teleinformatycznych, używanych do realizacji zadań publicznych z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, przeprowadzonej na podstawie art. 25 ust. 1 pkt 3 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[1], w Ministerstwie Nauki i Szkolnictwa Wyższego[2] (dalej: MNiSW).

Zgodnie z art. 47 w związku z art. 46 ust. 2 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[3], przekazuję Panu Ministrowi Wystąpienie pokontrolne.

Kontrolę przeprowadzono w trybie zwykłym, określonym ustawą z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej.* Kontrola została przewidziana w Planie kontroli do realizacji przez Biuro Ministra Ministerstwa Cyfryzacji w 2016 roku, zatwierdzonym przez Ministra Cyfryzacji Annę Streżyńską w dniu 12 kwietnia 2016 r.

Czynności kontrolne prowadzone były w dniach od 2 do 18 listopada 2016 r. przez zespół kontrolny w składzie:

- Bogdan Kowalczyk – główny specjalista w Wydziale Skarg, Kontroli i Nadzoru Biura Ministra Ministerstwa Cyfryzacji – kierownik zespołu — upoważnienie nr 10/2016 z dnia 13 października 2016 r.;
- Magdalena Soszyńska – Zastępca Dyrektora Biura Ministra Ministerstwa Cyfryzacji – członek zespołu— upoważnienie nr 10/2016 z dnia 13 października 2016 r.

Celem kontroli było dokonanie oceny działania systemów teleinformatycznych używanych do realizacji zadań publicznych pod względem zgodności z minimalnymi wymaganiami dla systemów

[1] Dz. U. z 2014 r. poz. 1114 z późn. zm.
[2] Ministerstwo Nauki i Szkolnictwa Wyższego ul. Hoża 20, 00-529 Warszawa.
[3] Dz. U. Nr 185, poz. 1092

teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych oraz przestrzegania wymagań odnoszących się do Krajowych Ram Interoperacyjności.

Kontrolą objęto okres od dnia 1 września 2015 r. do 31 sierpnia 2016 r.

Zespół kontrolny poddał analizie funkcjonujący w MNiSW System Zarządzania Bezpieczeństwem Informacji oraz 2 z 7 systemów teleinformatycznych MNiSW:

1. Strona internetowa MNiSW - www.nauka.gov.pl;
2. Zintegrowany system informacji o nauce i szkolnictwie wyższym POLON – rejestr publiczny.

OCENA

Na podstawie analizy dokumentacji źródłowej oraz otrzymanych pisemnych wyjaśnień zespół kontrolny sformułował następującą ocenę kontrolowanych obszarów:

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną - pozytywnie z uchybieniami;
2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych — pozytywnie z nieprawidłowościami;
3. Dostosowanie systemów informatycznych do standardu WCAG 2.0 — pozytywnie z nieprawidłowościami.

Podsumowując całościowo wyniki analizy dokumentacji źródłowej dotyczącej kontrolowanych zagadnień oraz otrzymanych pisemnych wyjaśnień, działanie systemów teleinformatycznych w MNiSW pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub rejestrów publicznych oraz przestrzegania wymagań odnoszących się do Krajowych Ram Interoperacyjności oceniono pozytywnie z nieprawidłowościami.

SZCZEGÓŁOWE USTALENIA KONTROLI

Słownik:
BIP — Biuletyn Informacji Publicznej;
BI — bezpieczeństwo informacji;
baza konfiguracji CMDB – baza danych zarządzania konfiguracją (Configuration Management DataBase), centralny rejestr zasobów informatycznych ich konfiguracji i relacji pomiędzy elementami konfiguracji;
CRWDE — centralne repozytorium wzorów dokumentów elektronicznych;
ePUAP — Elektroniczna Platforma Usług Administracji Publicznej. System teleinformatyczny udostępniający usługi elektroniczne administracji publicznej dla obywateli i podmiotów prowadzony przez ministra właściwego do spraw informatyzacji;
ESP — elektroniczna skrzynka podawcza;
KRI — Krajowe Ramy Interoperacyjności stanowią zbiór zasad i sposobów postępowania podmiotów w celu zapewnienia systemom informatycznym interoperacyjności działania, rozumianej jako

zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą;

MC — Ministerstwo Cyfryzacji;

MNiSW — Ministerstwo Nauki i Szkolnictwa Wyższego;

RI — Repozytorium Interoperacyjności — część zasobów ePUAP przeznaczona do udostępniania informacji służących osiąganiu interoperacyjności;

rozporządzenie ePUAP — rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. *w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej*[4];

rozporządzenie KRI — 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*[5];

ustawa *o informatyzacji* — ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne;*

XML — (eXtensible Markup Language) — tekstowy format służący do opisywania informacji (danych) w sposób strukturalny; jest to format, przy pomocy którego nadaje się znaczenie poszczególnym fragmentom informacji;

PDF — format plików służący do prezentacji, przenoszenia i drukowania treści tekstowo-graficznych, stworzony i promowany przez firmę Adobe Systems; format PDF powstał jako format wynikowy, mający zachować pełny wygląd dokumentu po wydrukowaniu;

doc — dokument w postaci sformatowanego tekstu, wewnętrzny standard Microsoft Corp.;

dostępność — właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;

integralność — zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;

interoperacyjność — zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych; osiąganie interoperacyjności następuje poprzez ciągłe doskonalenie jednostki w zakresie zarządzania systemami informatycznymi;

model usługowy — model architektury systemu informatycznego, w którym dla użytkowników (klientów/odbiorców) zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji;

polityka bezpieczeństwa informacji, polityka BI, PBI — zestaw praw, reguł i praktycznych doświadczeń, regulujących sposób zarządzania, ochrony i dystrybucji informacji wewnątrz określonej organizacji;

poufność — zapewnienie, że informacja jest dostępna tylko dla osób do tego upoważnionych;

usługa elektroniczna — w myśl art. 2 pkt 4 ustawy z dnia 8 lipca 2002 r. *o świadczeniu usług drogą elektroniczną*[6], jest to usługa świadczona bez jednoczesnej obecności stron (na odległość), poprzez

---

[4] Dz. U. z 2014 r., poz. 584.

[5] Dz. U. z 2012 r., poz. 526 z późn. zm., Dz. U. z 2016 r. poz. 113.

[6] Dz. U. z 2013 r., poz. 1422 z późn. zm., Dz. U. z 2016 r. poz. 615.

przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania;

współdzielenie informacji — wspólne użytkowanie tych samych zasobów przez różne osoby i/lub podmioty, np. zasobów takich jak: pliki, bazy danych, dokumenty itp.

KONTEKST ORGANIZACYJNY

Zgodnie z przepisami ustawy *o informatyzacji* osobą odpowiedzialną za realizację zadań wynikających z rozporządzenia KRI w ministerstwie jest jego kierownik, tj. Minister. W okresie objętym kontrolą stanowisko Ministra Nauki i Szkolnictwa Wyższego piastowali:

- Pani Lena Kolarska-Bobińska – od 3 grudnia 2013 r. do 15 listopada 2015 r.
- Pan Jarosław Gowin – od 16 listopada 2015 r.

Funkcję Dyrektora Generalnego Ministerstwa Nauki i Szkolnictwa Wyższego pełnili:

- do dnia 21 stycznia 2016 r. - Pan Mark Kuciński, którego w czasie nieobecności zastępował Pan Marcin Czaja;
- od dnia 1 lutego 2016 r. - Pani Anna Budzanowska, którą w czasie nieobecności zastępuje Pani Alicja Steć – Dyrektor Biura Dyrektora Generalnego;

W okresie objętym kontrolą stan zatrudnienia w MNiSW przedstawiał się następująco[7]:

- 1 września 2015 r. – 366,45 etatu, tj. 369 osób;
- 31 sierpnia 2016 r. – 364,25 etatu, tj. 367 osób;

MNiSW ma swoją siedzibę w budynku przy ul. Hożej 20 w Warszawie. Ochronę fizyczną budynku zapewnia straż przemysłowa. Budynek jest objęty systemem tv przemysłowej oraz systemem kontroli dostępu z zastosowaniem czytników kart zbliżeniowych przy drzwiach wejściowych oraz w strefach podwyższonej ochrony.

Serwerownia znajduje się w pomieszczeniach zaadaptowanych na ten cel z pomieszczeń biurowych. Jest wyposażona w system kontroli dostępu, dwustronne zasilanie, systemy podtrzymania zasilania i klimatyzacji oraz system gaszenia gazem. Piony dystrybucyjne sieci LAN objęte są systemem kontroli dostępu, posiadają systemy podtrzymanie zasilania i klimatyzacji.

Wsparcie informatyczne MNiSW zapewniają Wydziały Biura Dyrektora Generalnego, Wydział Infrastruktury Informatycznej kierowany przez Naczelnika Pana Łukasza Barteckiego. W Wydziale zatrudnionych jest 10 pracowników. Dodatkowo problematyką budowy i organizacji SZBI zajmuje się Wydział Organizacji i Cyfryzacji kierowany przez Pana Naczelnika Wiesława Majosa. Pod opieką administracyjną Wydziału Infrastruktury Informatycznej znajdują się: aplikacje biurowe, poczta elektroniczna, system zarządzania dokumentacją EZD oraz usługi katalogowe. Administrowaniem systemami o nazwach: Zintegrowany System Informacji o Nauce i Szkolnictwie Wyższym POL-on (dalej: POL-on) i System przeznaczonym do rejestrowania i obsługi wniosków o finansowanie nauki (dalej OSF) na rzecz MNiSW zajmuje się Ośrodek Przetwarzania Informacji - Państwowy Instytut Badawczy, będący jednostką nadzorowaną przez MNiSW. Administrowaniem: BIP, główną stroną internetową urzędu oraz bazą ogłoszeń zajmuje się firma Net P.C. na zasadzie powierzenia.

[7] Pismo Dyrektora Biura Kontroli, Pani Alicji Dudy z dnia 14 listopada 2016 r.

W okresie objętym kontrolą doszło do zmian kierownictwa Ministerstwa. Zmiana wpłynęła w sposób pozytywny na proces budowy i wdrażania Polityki Bezpieczeństwa Informacji w ramach SZBI.

(Dowód: akta kontroli str. 41, 43-45)

1. **Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną**

Przepisy dotyczące interoperacyjności mają na celu stworzenie warunków do współdziałania ze sobą systemów informatycznych jednostek realizujących zadania publiczne w celu zapewnienia szybkiej wymiany informacji zarówno wewnątrz urzędu, jak i z innymi urzędami administracji publicznej. Wdrożenie tych przepisów powinno przyczynić się do usprawnienia realizacji zadań urzędów, w tym załatwiania spraw obywateli i przedsiębiorców na odległość i w krótszym czasie, bez żądania informacji będących już w posiadaniu urzędów. Jednocześnie, powinny zostać stworzone warunki korzystania z serwisów internetowych urzędu przez osoby z niepełnosprawnościami.

1.1. Usługi elektroniczne

Jednym z podstawowych celów działania urzędu jest realizacja usług dla obywateli i innych podmiotów w sposób szybki i sprawny oraz maksymalnie przyjazny dla obywatela/podmiotu. Realizację praktyczną ww. postulatów można uzyskać poprzez udostępnienie wszelkich możliwych usług świadczonych przez urząd na platformie elektronicznej dostępnej przez sieć Internet. Tak realizowane usługi pozwolą na załatwianie spraw w urzędzie z domu lub z dowolnego innego miejsca, w którym obywatel/podmiot ma dostęp do sieci Internet. Usługi powinny być świadczone wg jednolitych, standardowych procedur, jasno komunikowanych obywatelowi/podmiotowi. Celem stosowania usług elektronicznych jest ułatwienie w dostępie do usług poprzez wyeliminowanie korespondencji papierowej obywatela/podmiotu z urzędem, zastąpienie druków i formularzy papierowych ich odpowiednikami elektronicznymi dostępnymi do wypełnienia na platformie usług elektronicznych urzędu, a także wyeliminowanie papierowych dokumentów kierowanych do obywatela/podmiotu i zastąpienie ich odpowiednikami elektronicznymi przesyłanymi droga elektroniczną, np. na skrytkę na platformie ePUAP.

MNiSW udostępnia elektroniczną skrzynkę podawczą (dalej: ESP) na platformie ePUAP pozwalającą na przesłanie drogą elektroniczną pism skierowanych do urzędu, w tym: pism ogólnych, skarg, wniosków, zapytań itp. Korespondencja wpływająca przez ESP wprowadzana jest do systemu Elektronicznego Zarządzania Dokumentacją (EZD). Pracownik kancelarii ogólnej MNiSW kieruje korespondencję do sekretariatów departamentów, po czym korespondencja jest dekretowana przez dyrektora departamentu. W MNiSW opracowano łącznie 58 usług elektronicznych, z czego w okresie objętym kontrolą 6 usług. Dla 54 usług opracowano formularze elektroniczne w formacie .doc, a dla 4 w formacie XML. Na stronie głównej Ministerstwa znajdują się informacje o możliwości korzystania z ESP na ePUAP w zakresie przesyłania pism ogólnych. W zakładkach tematycznych dotyczących konkretnych spraw informacje o podstawie prawnej, procedurze merytorycznej oraz wzory dokumentów do wypełnienia. Na stronach BIP Ministerstwa znajdują się procedury obowiązujące przy załatwianiu spraw drogą elektroniczną. Usługi MNiSW realizowane są na 1 i 2 poziomie dojrzałości (poziom informacyjny i interakcyjny).

Podczas kontroli stwierdzono brak aktualizacji informacji statystycznej o e-usługach na stronie głównej Ministerstwa; dane tam publikowane dotyczące liczby świadczonych e-usług oraz liczby odbieranej i wysyłanej e-korespondencji odnoszą się do roku 2013[8].

(Dowód: akta kontroli str. 41, 218-221)

1.2. Centralne repozytorium wzorów dokumentów elektronicznych

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory opracowanych i używanych dokumentów. W przypadku uruchamiania przez dany urząd usługi elektronicznej, która już funkcjonuje w innym urzędzie, dany urząd powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych znajdujące się w CRWDE. W przypadku uruchamiania usługi, dla której nie ma opublikowanych wcześniej wzorów dokumentów w CRWDE, urząd jest zobowiązany opracować i przekazać do CRWDE wzory dokumentów elektronicznych związanych z nową usługą.

MNiSW przekazywało wzory dokumentów elektronicznych do CRWDE oraz publikuje informacje o nich w BIP. Minister Nauki i Szkolnictwa wyższego wydał upoważnienia do podpisywania wniosków o publikację dokumentów elektronicznych w CRWDE Naczelnikowi Wydziału Infrastruktury Informatycznej BDG oraz zastępcy dyrektora BDG.

(Dowód: akta kontroli str. 41, 218-221)

1.3. Model usługowy

Model usługowy został zdefiniowany w § 2 pkt 8 rozporządzenia KRI. Jest to model, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji (inaczej: system zorientowany na usługi). Zarządzanie usługami elektronicznymi w oparciu o model usługowy wymaga posiadania i stosowania wewnętrznych procedur obsługi usługi oraz dostarczania ich na zadeklarowanym poziomie zgodnie z wymaganiami § 15 ust. 2 rozporządzenia KRI.

MNiSW w sposób nieformalny realizowało procedury pozwalające na identyfikację właściciela merytorycznego, ustalenie odpowiedzialności za utrzymanie usług od strony technicznej. Jednak nie zadeklarowano poziomu ich świadczenia oraz nie prowadzono monitoringu dotrzymywaniu poziomu ich świadczenia, co jedynie częściowo wypełnia wymagania § 15 ust. 2 rozporządzenia KRI w tym obszarze.

(Dowód: akta kontroli str. 41, 218-221)

1.4. Współpraca badanych systemów informatycznych z innymi systemami

Wiele rejestrów w urzędach administracji publicznej przechowuje i przetwarza identyczne informacje np. o obywatelu/podmiocie (PESEL, REGON, NIP, dane adresowe). Ułatwieniem w załatwieniu spraw dla obywatela/podmiotu będzie sytuacja, gdy urząd nie będzie żądał od obywatela/podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego postulatu wymaga, aby system informatyczny, w którym prowadzony jest rejestr odwoływał się bezpośrednio do danych

[8] http://www.nauka.gov.pl/e-urzad/statystyki-e-urzad.html

gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.

Rejestr publiczny o nazwie Zintegrowany System Informacji o Nauce i Szkolnictwie Wyższym POL-on dostępny w sieci Internet na stronie https://polon.nauka.gov.pl prowadzony jest zgodnie z ustawą z dnia 27 lipca 2005 r. *Prawo o szkolnictwie wyższym*[9], ustawą z dnia 30 kwietnia 2010 r. *o zasadach finansowania nauki*[10] oraz ustawą z dnia 14 marca 2003 r. *o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki*[11]. Na rejestr składają się:

- Rejestry uczelni i instytucji naukowych w tym: rejestr uczelni niepublicznych, rejestr instytucji szkolnictwa wyższego, rejestr jednostek naukowych, rejestr związków uczelni, instytucje kościelne, biblioteki naukowe;
- Rejestry osobowe, w tym: ogólnopolski wykaz nauczycieli akademickich i pracowników naukowych, ogólnopolski wykaz profesorów, ogólnopolski wykaz doktorów i doktorów habilitowanych, wykaz pracowników naukowych zatrudnionych w jednostkach naukowych realizujących badania naukowe i projekty rozwojowe;
- Rejestry Działalności badawczo-rozwojowej jednostek naukowych, w tym: nieruchomości, infrastruktura naukowo badawcza, infrastruktura informatyczna, wartości niematerialne i prawne, laboratoria badawcze i aparatura, projekty naukowe, czasopisma naukowe wydawane przez jednostki naukowe, zorganizowane konferencje naukowe, wdrożone systemy jakości, patenty i prawa ochronne, wdrożenia wyników badań naukowych i prac rozwojowych przez inne podmioty;
- Rejestry powiązane w tym: zestawienie prowadzonych studiów na kierunkach, uprawnienia jednostek naukowych do nadawania stopni naukowych, ankieta jednostki, polska bibliografia naukowa, ogólnopolskie repozytorium prac dyplomowych.

System Pol-on współpracuje z rejestrem TERYT - w zakresie danych adresowych, z rejestrem REGON – w zakresie danych jednostek, z systemem GUS w zakresie statystyki nauki i szkolnictwa wyższego. System POL-on w zakresie udostępniania danych nie wchodzi w bezpośrednią interakcję z innymi systemami informatycznymi. System POL-on pozwala administratorom merytorycznym (pracownikom MNiSW) oraz uprawnionym pracownikom instytucji i podmiotów naukowych na ręczne wprowadzanie danych oraz wszystkim użytkownikom, w tym klientom urzędu na przeglądanie rejestrów i ręczne wygenerowanie wydruków i zestawień tabelarycznych.

(Dowód: akta kontroli str. 41, 146-178)

1.5. Obieg dokumentów

Stosowanie systemu elektronicznego zarządzania obiegiem dokumentów wpływa na uporządkowanie i usprawnienie ich obiegu, znacząco ułatwia i przyspiesza prowadzenie archiwizacji oraz zapewnia bezpośredni dostęp do dokumentów archiwalnych, co wpływa na przyspieszenie załatwianych spraw (realizowanych przez urzędy usług) oraz minimalizowanie nakładu pracy. Celem wdrożenia

[9] Dz. U. z 2005 r., poz. 1365 z późn. zm.
[10] Dz. U. 2010 r., poz. 615.
[11] Dz. U. 2003 r., poz. 595.

elektronicznego obiegu dokumentów jest wyeliminowanie z obiegu wewnętrznego urzędu dokumentów papierowych.

W MNiSW funkcjonuje System Elektronicznego Zarządzania Dokumentacją (dalej EZD). Zarządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 2 stycznia 2013 r. *zmieniające zarządzenie w sprawie wprowadzenia w Ministra Nauki i Szkolnictwa Wyższego instrukcji kancelaryjnej, rzeczowego wykazu akt i instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego* reguluje kompleksowo zakres i sposób stosowania elektronicznego zarządzania obiegiem dokumentów zapewniając właściwy poziom bezpieczeństwa.

(Dowód: akta kontroli str. 41)

1.6. Format danych udostępniany przez badane systemy informatyczne

Istotą współdzielenia informacji w urzędach jest stworzenie możliwości wymiany danych pomiędzy różnymi systemami informatycznymi oraz umożliwienie odbiorcom swobodnego dostępu do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików.

Dla badanych systemów MNiSW kodowanie znaków w wysyłanych z systemów dokumentach odbywa się według standardu Unicode UTF-8, zgodnie z § 17 ust. 1 rozporządzenia KRI. Systemy udostępniają zasoby informatyczne w jednym z formatów danych określonych w załączniku 2 do rozporządzenia tj. w doc i xls, zgodnie z § 18 ust. 1 rozporządzenia KRI.

Ustalenia:

1. MNiSW w badanym okresie świadczyło usługi w formie elektronicznej na 1 i 2 poziomie dojrzałości (poziom informacyjny i interakcyjny) przy wykorzystaniu opracowanych formularzy w formatach .doc lub .xml przesyłanych na elektroniczną skrzynkę podawczą ministerstwa na ePuap.
2. MNiSW przekazywało wzory dokumentów elektronicznych do CRWDE i udostępniało na stronie BIP wzory dokumentów elektronicznych dla realizowanych usług.
3. MNiSW w sposób nieformalny realizowało procedury pozwalające na identyfikację właściciela merytorycznego, ustalenie odpowiedzialności za utrzymanie usług od strony technicznej. Jednak nie zadeklarowano poziomu ich świadczenia oraz nie prowadzono monitoringu dotrzymywania poziomu ich świadczenia, co jedynie częściowo wypełnia wymagania § 15 ust. 2 rozporządzenia KRI w tym obszarze.
4. Systemy objęte badaniem nie wchodzą w bezpośrednią interakcję z innymi systemami informatycznymi, gdyż pełnią rolę informacyjną. System Pol-on współpracuje z rejestrem TERYT - w zakresie danych adresowych, z rejestrem REGON – w zakresie danych jednostek, z systemem GUS w zakresie statystyki nauki i szkolnictwa wyższego.
5. W MNiSW funkcjonuje System Elektronicznego Zarządzania Dokumentacją, a regulacje wewnętrzne kompleksowo opisują zakres i sposób stosowania elektronicznego obiegu dokumentów i ich archiwizacji, zapewniając odpowiedni poziom bezpieczeństwa.
6. Dla kontrolowanych systemów kodowanie znaków w wysyłanych z systemów dokumentach odbywa się według standardu Unicode UTF-8, zgodnie z § 17 ust. 1 rozporządzenia KRI, a ich udostępnianie w jednym z formatów danych określonych w załączniku 2 do rozporządzenia tj. w doc i xls, zgodnie z § 18 ust. 1 rozporządzenia KRI.

2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

Wraz z rozwojem elektronicznej formy komunikacji znaczenia nabiera zapewnienie dostępności, integralności i poufności danych posiadanych i przetwarzanych przez urzędy. Dlatego też, szczególnie istotne jest zapewnienie bezpieczeństwa informacji przetwarzanych w użytkowanych przez podmioty publiczne systemach informatycznych. W przeciwnym razie powstaje ryzyko utraty ww. właściwości gwarantujących bezpieczeństwo informacji, a w konsekwencji utrata stabilności pracy urzędów. Podważyć to może zaufanie obywateli do organów administracji publicznej. Jednostka, aby zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji.

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia (§ 20 ust. 2 pkt 1 rozporządzenia KRI). Dokumentacja ta jest warunkiem niezbędnym dla możliwości skutecznego zarządzania bezpieczeństwem informacji.

W zakresie bezpieczeństwa teleinformatycznego w badanym okresie w MNiSW obowiązywały:

1. Zarządzenie Nr 48/2009 Ministra Nauki i Szkolnictwa Wyższego z dnia 7 października 2009 r. w sprawie zasad ochrony danych osobowych przetwarzanych w Ministerstwie Nauki i Szkolnictwa Wyższego.
2. Zarządzenie nr 5/2011 Dyrektora Generalnego z dnia 3 marca 2011 r. w sprawie sieci komputerowej Ministerstwa Nauki i Szkolnictwa Wyższego.
3. Zarządzenie Nr 58/2011 Ministra Nauki i Szkolnictwa Wyższego z dnia 6 lipca 2011 r. w sprawie kontroli zarządczej w Ministerstwie Nauki i Szkolnictwa Wyższego.
4. Zarządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 3 sierpnia 2016 r. w sprawie kontroli zarządczej w Ministerstwie Nauki i Szkolnictwa Wyższego.
5. Zarządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 kwietnia 2013 r. w sprawie powołania Zespołu do spraw Zarządzania Ryzykiem.

Obowiązujące regulacje ograniczają zakres ochrony informacji do ochrony danych osobowych. W badanym okresie MNiSW nie wprowadzono Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), co oznacza, że w badanym okresie w MNiSW ww. system nie został wdrożony i nie funkcjonował, zatem nie mógł być monitorowany, poddawany przeglądom i doskonalony. Wobec powyższego nie zostały spełnione wymagania § 20 ust. 1 rozporządzenia KRI.

Świadomość takiego stanu znalazła odzwierciedlenie w oświadczeniu o stanie kontroli zarządczej Ministra Nauki i Szkolnictwa Wyższego za rok 2015 z dnia 29 kwietnia 2016 r., gdzie w zastrzeżeniach dotyczących kontroli zarządczej w MNiSW znalazł się zapis mówiący że: „Obowiązujące regulacje nie wypełniają w całości zakresu objętego rozporządzeniem Rady Ministrów z dn. 12.04.2012 r.

w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".[12]

Aktualnie (w terminie przeprowadzania kontroli) w MNiSW obowiązuje Polityka Bezpieczeństwa Informacji MNiSW podpisana przez Ministra Nauki i Szkolnictwa Wyższego w dniu 19 października 2016 r., w której zawarto deklarację Kierownictwa co do zapobiegania i reagowania na zagrożenia prowadzące do utraty poufności, integralności i dostępności informacji. Ponadto, zdefiniowane zostały cele Polityki oraz wskazano na potrzebę jej aktualizacji i komunikowania. Polityka opisuje: organizację SZBI w MNiSW, w tym role, kompetencje i odpowiedzialności personelu, produkty zarządcze SZBI, zasady dotyczące komunikacji, kształcenia, zasady metodyczne oraz dotyczące harmonogramu wdrożenia. Polityka wprowadza hierarchiczną trójpoziomowa strukturę dokumentacji składającej się na SZBI. Na ww. strukturę składają się: Polityka Bezpieczeństwa Informacji, polityki tematyczne/zarządzenia, procesy (listy kontrolne: procedur, instrukcji, standardów i szablony dokumentów). Załącznikiem do Polityki jest deklaracja stosowania celów i zabezpieczeń szczegółowo opisująca poszczególne zagrożenia oraz deklarowane przez MNiSW sposoby zabezpieczenia.

Obecnie w MNiSW prowadzone są prace mające na celu stworzenie i zatwierdzenie szczegółowego programu wdrożenia SZBI, a także prace związane z opracowaniem dokumentacji SZBI poziomu drugiego i trzeciego (dokumenty podrzędne Polityce Bezpieczeństwa Informacji).

Krytycznie należy ocenić podejmowane przed 2016 rokiem działania kierownictwa w celu stworzenia warunków aktualizacji regulacji wewnętrznych dotyczących SZBI w zakresie dotyczącym zmieniającego się otoczenia (wymagania § 20 ust. 2 pkt 1 rozporządzenia KRI). Działania w tym zakresie prowadzone były nieefektywnie, gdyż pomimo funkcjonowania ustawy *o informatyzacji* i rozporządzenia KRI w MNISW nie wdrożono SZBI.

Obecnie w MNiSW stworzone są warunki do aktualizacji regulacji wewnętrznych dotyczących SZBI w zakresie dotyczącym zmieniającego się otoczenia, a informacje zawarte w Raporcie z audytu systemu zarządzania bezpieczeństwem informacji w MNiSW[13] z grudnia 2015 r. spowodowały rozpoczęcie prac nad SZBI, których pierwszym efektem jest wcześniej wspomniana Polityka Bezpieczeństwa Informacji (z 19 października 2016 r.), co potwierdza zgodność z § 20 ust. 2 pkt 1 rozporządzenia KRI.

(Dowód: akta kontroli str. 41, 46-141, 142-144, 281-326)

2.2. Dokonywanie analizy zagrożeń związanych z przetwarzaniem informacji

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Na analizę ryzyka składają się: identyfikacja, szacowanie, a następnie określenie sposobu postępowania z ryzykiem oraz deklaracja stosowania zabezpieczeń będąca podstawą podejmowania wszelkich działań minimalizujących ryzyko stosownie do

[12] Oświadczenie o stanie kontroli zarządczej Ministra Nauki i Szkolnictwa Wyższego za rok 2015 z dnia 29 kwietnia 2016r. - http://www.bip.nauka.gov.pl/kontrola-zarzadcza/oswiadczenie-ministra-nauki-i-szkolnictwa-wyzszego-o-stanie-kontroli-zarzadczej-za-2015-r.html

[13] Raport z audytu systemu zarządzania bezpieczeństwem informacji w MNiSW względem wymogów normy PN-ISO/IEC 27001:2014 – grudzień 2015 r. NASK IB ul. Wąwozowa 18, 02-796 Warszawa.

przeprowadzonej analizy. Analiza ryzyka pozwala na proaktywne zarządzanie BI, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk. Analiza ryzyka pozwala na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka.

W oparciu o wewnętrzne regulacje, tj. Zarządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 kwietnia 2013 r. w sprawie powołania Zespołu do spraw Zarządzania Ryzykiem oraz Zarządzenie Nr 58/2011 Ministra Nauki i Szkolnictwa Wyższego z dnia 6 lipca 2011 r. w sprawie kontroli zarządczej w Ministerstwie Nauki i Szkolnictwa Wyższego w II kw. 2015 roku przeprowadzono analizę ryzyka.

Analiza ryzyka dotyczyła ryzyk związanych z realizacją celów strategicznych na potrzeby kontroli zarządczej MNiSW[14]. Przedstawiony zespołowi kontrolnemu rejestr ryzyk kluczowych zawiera między innymi ryzyka związane z realizacją celu ogólnego jakim jest „optymalizacja bezpieczeństwa informacji"[15]. W tym obszarze zidentyfikowano 5 ryzyk kluczowych, przeprowadzono ich szacowanie oraz zaproponowano działania zaradcze.

Stwierdzono, że w badanym okresie MNiSW nie posiadało odrębnych wewnętrznych regulacji dotyczących szacowania ryzyka utraty integralności, dostępności lub poufności informacji na potrzeby SZBI. Istniejące regulacje i tworzone na ich podstawie analizy ryzyka wykonywane były na potrzeby kontroli zarządczej i w niewystarczający sposób obejmowały problematykę bezpieczeństwa informacji. W związku z powyższym jedynie częściowo spełnione zostały wymagania określone w § 20 ust. 2 pkt 3 rozporządzenia KRI.

(Dowód: akta kontroli str. 41, 222-227)

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Baza inwentaryzacyjna powinna zawierać wszystkie zidentyfikowane aktywa informatyczne, przez co możliwe będzie ich odtworzenie w przypadku np.: katastrofy. Baza inwentaryzacyjna jest niezbędna przy wprowadzaniu wszelkich zmian w środowisku teleinformatycznym urzędu ograniczając możliwość zaistnienia zakłóceń w pracy, które wynikałyby z błędnych decyzji i podejmowanych działań, będących skutkiem braku aktualnej i kompleksowej wiedzy o stanie infrastruktury teleinformatycznej.

W badanym okresie w zakresie zarządzania majątkiem trwałym w MNiSW obowiązywały następujące regulacje: Zarządzenie nr 50/2009 Dyrektora Generalnego z dnia 15 października 2009 r. w sprawie szczegółowych zasad dokumentowania przemieszczeń środków trwałych oraz zmiany ich użytkowników w Ministerstwie Nauki i Szkolnictwa Wyższego oraz Zarządzenie Nr 48/2009 Ministra Nauki i Szkolnictwa Wyższego z dnia 7 października 2009 r. w sprawie zasad ochrony danych osobowych przetwarzanych w Ministerstwie Nauki i Szkolnictwa Wyższego.

[14] Notatka służbowa Dyrektora Biura Ministra do Dyrektora Generalnego MNiSW dotycząca analizy ryzyk kluczowych w MNiSW po III kw. 2016 r. z 26 października 2016r.
[15] Załącznik do Notatki służbowej z 26 października 2016r. - Rejestr ryzyk kluczowych II kw. 2016 r.

Na postawie powyższych regulacji w MNiSW prowadzony jest rejestr środków trwałych. Jego funkcjonowanie wynika z ustawy z dnia 29 września 1994 r. *o rachunkowości*[16], a nie z ustawy *o informatyzacji*.

Z wyjaśnień uzyskanych w trakcie kontroli wynika, że Wydział Infrastruktury Informatycznej BDG w celu zarządzania konfiguracją sprzętu oraz oprogramowania prowadzi własne rejestry zasobów IT, w tym rejestry o następujących nazwach:

- Systemy, Usługi, Konta,
- Urządzenia aktywne sieci szkieletowej,
- Licencje,
- Domeny,
- Wydzielone strefy sieci wewnętrznej,
- Urządzenia WiFi,
- Konfiguracje, a w nim: Konfiguracja zasobów dyskowych, depozytor kluczy, Kamery IP,
- Rejestr i konfiguracja systemu kopii bezpieczeństwa.

Stwierdzić zatem należy, że pomimo braku pisemnych procedur dotyczących i inwentaryzacji aktywów IT na potrzeby SZBI prowadzony jest rejestr zasobów teleinformatycznych zawierający informacje o zidentyfikowanych aktywach informatycznych, w tym sprzętu i oprogramowania służącego do przetwarzania informacji obejmującego ich rodzaj i konfigurację, zgodnie z wymaganiami § 20 ust. 2 pkt 2 rozporządzenia KRI.

(Dowód: akta kontroli str. 41, 179-184)

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

W badanym okresie zarządzanie uprawnieniami dostępu do przetwarzania danych osobowych w MNiSW regulowały: Zarządzenie Nr 48/2009 Ministra Nauki i Szkolnictwa Wyższego z dnia 7 października 2009 r. w sprawie zasad ochrony danych osobowych przetwarzanych w Ministerstwie Nauki i Szkolnictwa Wyższego oraz Zarządzenie nr 5/2011 Dyrektora Generalnego z dnia 3 marca 2011 r. w sprawie sieci komputerowej Ministerstwa Nauki i Szkolnictwa Wyższego oraz Zarządzenie nr 5/2011 Dyrektora Generalnego z dnia 3 marca 2011 r. w sprawie sieci komputerowej Ministerstwa Nauki i Szkolnictwa Wyższego. Pracownicy MNiSW uzyskiwali dostęp do zasobów informatycznych po podaniu unikalnego loginu i hasła. Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie działań zastrzeżonych dla administratorów systemów. W MNiSW na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 20 ust. 2 pkt 4 rozporządzenia KRI. Konta byłych pracowników w systemach informatycznych MNiSW w okresie objętym badaniem były sukcesywnie blokowane, zgodnie z § 20 ust. 2 pkt 5 rozporządzenia KRI. Rejestr uprawnień dostępu do zasobów informatycznych miał (i ma) postać

[16] Dz. U. z 2013 r., poz. 330 z późn. zm., Dz. U. z 2016 r. poz. 1047.

papierową i stanowi go zbór pisemnych wniosków o nadanie, zmianę lub cofnięcie uprawnień, przechowywany w komórce ds. informatyki. Nadawaniem uprawnień dla użytkowników systemu POL-on (w tym użytkowników w instytucjach nauki i szkolnictwa wyższego) zajmuje się Ośrodek Przetwarzania Informacji Państwowy Instytut Badawczy (będący administratorem technicznym systemu). MNiSW nie posiadało wewnętrznych regulacji dotyczących procedur kontrolnych stopnia adekwatności zakresu uprawnień do realizowanych przez użytkowników zadań.

(Dowód: akta kontroli str. 41)

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Świadomość współodpowiedzialności za BI oraz świadomość zagrożeń i konsekwencji zaistnienia incydentów związanych z naruszeniem BI wśród pracowników urzędu jest istotnym elementem SZBI. Szkolenia z zakresu BI powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów związanych z BI.

W badanym okresie w zakresie szkoleń w MNiSW obowiązywało Zarządzenie nr 33/2010 Dyrektora Generalnego MNiSW z dnia 31 sierpnia 2010 r. w sprawie określenia zasad podnoszenia kwalifikacji zawodowych pracowników MNiSW.

W roku 2015 w ramach projektu pod nazwą *Podstawy bezpieczeństwa informacji* zorganizowanych zostało dwanaście sesji szkoleniowych dla pracowników Ministerstwa trwających 3,5 godz. każda. Przeprowadzenie szkolenia było wynikiem realizacji zaleceń pokontrolnych audytu dot. oceny zgodności proceduralnej z normą ISO 27001. W szkoleniu uczestniczyli wszyscy pracownicy MNiSW[17]. Ponadto w MNiSW opracowano szkolenie z podstawy bezpieczeństwa informacji w trybie e- learningu. W tym trybie realizowane są na bieżąco szkolenia dla pracowników nowozatrudniony przed dopuszczeniem ich do pracy w systemach teleinformatycznych urzędu.

Powyższe wskazuje, że pomimo braku wewnętrznych regulacji precyzujących prowadzenie szkoleń użytkowników zaangażowanych w proces przetwarzania informacji w systemach informatycznych w ramach SZBI, podejmowane są działania w tym zakresie zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI. Niemniej jednak należy wskazać na brak cykliczności szkoleń w kolejnych latach.

(Dowód: akta kontroli str. 41, 277-280)

2.6. Praca na odległość i mobilne przetwarzanie danych

Wobec możliwości technicznych związanych z telepracą (pracą poza siedzibą urzędu) z wykorzystaniem urządzeń mobilnych takich jak laptopy, tablety, smartfony pojawiają się nowe zagrożenia BI. Konieczne jest opisanie zasad określających sposoby zabezpieczenia urządzeń mobilnych i danych w nich zawartych przed kradzieżą i nieuprawnionym dostępem poza siedzibą jednostki, a także zasad korzystania z ogólnodostępnych sieci.

W okresie objętym kontrolą w MNiSW nie ustanowiono wewnętrznych procedur w zakresie bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, a obowiązujące regulacje dotyczące bezpieczeństwa nie precyzują szczegółowych zasad dających

[17] Sprawozdanie z przebiegu zrealizowanego szkolenia zamkniętego pn.: *Podstawy bezpieczeństwa informacji* z dnia 3 listopada 2015 r.

gwarancję bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, w związku z czym nie wypełniają one obowiązku wynikającego z § 20 ust. 2 pkt 8 rozporządzenia KRI.

(Dowód: akta kontroli str. 41, 46-141)

2.7. Serwis sprzętu informatycznego i oprogramowania

W przypadku systemów informatycznych o znaczeniu krytycznym dla urzędu niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego, systemowego, sprzętu i rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii. Umowy powinny posiadać klauzule prawne zabezpieczające BI w przypadku wejścia w ich posiadania przez firmy serwisujące.

W okresie objętym kontrolą w zakresie serwisu sprzętu i oprogramowania w MNiSW obowiązywało Zarządzenie Nr 48/2009 Ministra Nauki i Szkolnictwa Wyższego z dnia 7 października 2009 r. w sprawie zasad ochrony danych osobowych przetwarzanych w Ministerstwie Nauki i Szkolnictwa Wyższego. Poza wymaganą ww. przepisem ochroną dotyczącą ochrony danych osobowych nie funkcjonowały regulacje wewnętrzne dotyczące zasad współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów teleinformatycznych, w tym zawierających wymagane klauzule prawne w zakresie BI. Niemniej jednak, pomimo stwierdzonego braku wewnętrznych procedur i regulacji ww. zakresie na potrzeby SZBI, umowy zawarte przez MNiSW dotyczące badanych systemów, tj. strony internetowej oraz systemu POL-on zawierały zapisy zapewniające odpowiedni poziom bezpieczeństwa informacji, co przy braku stosowych regulacji wewnętrznych w tym zakresie jedynie częściowo wypełnia wymagania § 20 ust. 2 pkt 10 rozporządzenia KRI.

(Dowód: akta kontroli str. 41, 146-178)

2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Pomimo stosowania zabezpieczeń pozwalających na ograniczanie ryzyka związanego z przetwarzaniem informacji w urzędzie istnieje ryzyko szczątkowe, świadomie akceptowane przez Kierownictwo. W ramach ryzyka szczątkowego, a także ryzyka nieobjętego analizą ryzyka mogą pojawić się incydenty naruszenia BI. Incydenty te powinny być bezzwłocznie zgłaszane w określony i z góry ustalony sposób, a także powinien być opisany sposób reakcji na te incydenty przez wyznaczone osoby w celu szybkiego podjęcia działań korygujących.

W okresie objętym kontrolą w zakresie serwisu sprzętu i oprogramowania w MNiSW obowiązywało Zarządzenie Nr 48/2009 Ministra Nauki i Szkolnictwa Wyższego z dnia 7 października 2009 r. w sprawie zasad ochrony danych osobowych przetwarzanych w Ministerstwie Nauki i Szkolnictwa Wyższego. Procedura reagowania na incydenty opisana w powyższej regulacji dotyczyła naruszenia zasad ochrony danych jedynie w przypadku naruszenia ochrony danych osobowych.

Pomimo braku regulacji wewnętrznych dotyczących zarządzania incydentami naruszenia bezpieczeństwa informacji w ramach SZBI w trakcie czynności kontrolnych, przedłożono zespołowi kontrolnemu rejestr incydentów[18] zawierający wszystkie zgłoszenia IT (nie tylko dotyczące bezpieczeństwa danych osobowych) oraz poinformowano, że pracownicy pionu informatyki zajmują

[18] Raport zgłoszeń dotyczących bezpieczeństwa za okres od 15.03.2016 r. do 07.11.2016 r.

się każdym zgłoszonym problemem. Rejestr zawierał 99 zgłoszeń. Przy każdym zgłoszeniu odnotowano informacje o zgłaszającym, przedmiocie zgłoszenia, kategoryzacji zgłoszenia, osobie rozwiązującej problem oraz sposobie rozwiązania problemu. Każde zgłoszenie posiadało unikalny nr ID. Rejestracja i procedowanie wszystkich incydentów związanych z bezpieczeństwem informacji przy jednoczesnym braku pisemnych procedur w tym obszarze, oznacza jedynie częściowe spełnione wymagania § 20 ust. 2 pkt 13 rozporządzenia KRI.

(Dowód: akta kontroli str. 41, 46-145)

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Wymogiem SZBI jest regularne (nie rzadziej niż raz na rok) przeprowadzanie audytów wewnętrznych w zakresie BI w systemach informatycznych, co pozwoli na ewentualne ujawnienie słabości SZBI i jego doskonalenie.

W okresie objętym kontrolą w MNiSW nie funkcjonowały regulacje określające zasady wykonywania audytów wewnętrznych systemów informatycznych na potrzeby SZBI.

W okresie objętym kontrolą w MNiSW przeprowadzony zostały „Audyt systemu zarządzania bezpieczeństwem informacji MNISW względem wymogów normy PN-ISO/IEC 27001:2014". Wyniki audytu zawarte są w Raporcie z audytu[19]. Audyt wykazał liczne niezgodności sposobu zarzadzania bezpieczeństwem informacji z wymaganiami normy PN-ISO/IEC 27001:2014 KRI. Zespół audytowy wskazał mi.in., że „obowiązująca Polityka Bezpieczeństwa Informacji zawarta w Zarządzeniu Nr 48/2009 Ministra Nauki i Szkolnictwa Wyższego z dnia 7 października 2009 r. W sprawie zasad ochrony danych osobowych przetwarzanych w Ministerstwie Nauki i Szkolnictwa Wyższego nie spełnia części wymagań wskazanych w § 20 rozporządzenia KRI". Ponadto, Raport z Audytu wykazał, że poza regulacjami związanymi z ochroną danych osobowych „w wielu obszarach stosowane są niesformalizowane procedury funkcjonujące w MNiSW. Proces organizacji zarządzania bezpieczeństwem informacji jak również przypisanie ról i odpowiedzialności za bezpieczeństwo informacji ogranicza się do wąskiej grupy osób co w praktyce sprowadza się do proponowania rozwiązań, ich wdrażania a następnie weryfikowania przez osoby odpowiedzialne za obszar IT organizacji".

Należy zaznaczyć, że niektóre z zaleceń poaudytowych dotyczące opracowania i wdrożenia Polityki Bezpieczeństwa Informacji w ramach SZBI uwzględniono w planach Biura Dyrektora Generalnego w celach i zadaniach do wykonania w ramach kontroli zarządczej[20]. Realizacja audytu, o którym mowa wyżej, oznacza zgodność z wymaganiem § 20 ust. 2 pkt 14 rozporządzenia KRI.

(Dowód: akta kontroli str. 41, 46-141)

2.10. Kopie zapasowe

Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Kopie powinny być właściwie tworzone, przechowywane i testowane. Celem

[19] Raport z audytu systemu zarządzania bezpieczeństwem informacji MNISW względem wymogów normy PN-ISO/IEC 27001:2014. Wykonany przez Naukową i Akademicką Sieć Komputerową instytut badawczy. Datowany na: listopad- grudzień 2015 r.

[20] Załącznik do Notatki służbowej z 26 października 2016 r. - Rejestr ryzyk kluczowych II kw. 2016 r

tworzenia kopii zapasowych danych jest możliwość ich odzyskania, tj. przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system np. w bazie danych. Wymóg ten można osiągnąć robiąc regularnie kopie całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych oraz poprzez regularne odtwarzanie systemu z kopii na niezależnym środowisku sprzętowym oraz testowaniu pracy użytkowej tak odtworzonego systemu.

W okresie objętym kontrolą w zakresie wykonywania kopii zapasowych w MNiSW obowiązywało Zarządzenie Nr 48/2009 Ministra Nauki i Szkolnictwa Wyższego z dnia 7 października 2009 r. w sprawie zasad ochrony danych osobowych przetwarzanych w Ministerstwie Nauki i Szkolnictwa Wyższego. Powyższa regulacja dotyczy jedynie ochrony danych osobowych.

Pomimo braku regulacji wewnętrznych dotyczących zarządzania kopiami bezpieczeństwa w ramach SZBI w trakcie czynności kontrolnych przedłożono zespołowi kontrolnemu dokumentację powdrożeniową systemu wykonywania kopii zapasowych[21], w której dostawca rozwiązania opisał szczegółowo procedurę wykonywania kopii zapasowych oraz procedurę odtwarzania systemów z kopii. Stwierdzono, że wyżej wymienione procedury były na bieżąco stosowane w MNiSW. Poddany analizie przykładowy raport dzienny z wykonywania kopii bezpieczeństwa[22] wygenerowany z systemu wykonywania kopii zapasowych potwierdza skuteczne, automatyczne wykonanie kopii zapasowych 29 obiektów systemowych w tym serwerów, plików i logów zgodnie z wymaganiem § 20 ust. 2 pkt 12 lit b rozporządzenia KRI w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii. Zastrzeżenie dotyczy zapewnienia przechowywania utworzonych kopii zapasowych w lokalizacji innej, niż lokalizacja serwerowni w której przetwarzane są zabezpieczane systemy.

(Dowód: akta kontroli str. 41, 46-141, 180-217)

2.11. Projektowanie, wdrażanie i eksploatacja systemów telekomunikacyjnych

Bezpieczeństwo systemu teleinformatycznego w dużym stopniu zależy od jego budowy. Stąd wymagania, aby system teleinformatyczny został zaprojektowany i zbudowany zgodnie z zasadami BI opisanymi w obowiązujących normach i standardach przemysłowych. Procedury odbioru danego systemu teleinformatycznego muszą zagwarantować kompleksowe przetestowanie wbudowanych zabezpieczeń pod względem uzyskania założonego poziomu BI. Podczas użytkowania systemu teleinformatycznego konieczne jest monitorowanie jego pracy m.in. w celu dostrzeżenia wszelkich nieprawidłowości i podejmowania bezpośrednich działań korygujących.

W MNiSW, pomimo braku odrębnych regulacji wewnętrznych w tym zakresie, zapewniono warunki dla uzyskania odpowiedniej funkcjonalności, niezawodności, używalności, wydajności, przenaszalności i pielęgnowalności systemów informatycznych w fazie ich projektowania, wdrażania i eksploatacji, co częściowo spełnia wymagania § 15 ust. 1 rozporządzenia KRI. Wymagania związane

[21] Dokumentacja Powdrożeniowa Symantec Netbacup 7.6.01 f-my BizTech Konsulting SA. (bez daty wytworzenia).
[22] Raport dzienny z wykonania kopii bezpieczeństwa Symantek NetBackup OpsCenter z dnia 6 listopada 2016 r.

z ww. atrybutami w stosunku do systemów przetwarzających dane osobowe zawarte były w Zarządzeniu Nr 48/2009 Ministra Nauki i Szkolnictwa Wyższego z dnia 7 października 2009 r. w sprawie zasad ochrony danych osobowych przetwarzanych w Ministerstwie Nauki i Szkolnictwa Wyższego oraz Zarządzeniu nr 5/2011 Dyrektora Generalnego z dnia 3 marca 2011 r. w sprawie sieci komputerowej Ministerstwa Nauki i Szkolnictwa Wyższego.

Jednakże, w badanym okresie MNiSW nie posiadało regulacji wewnętrznych określających szczegółowe wymagania techniczne i eksploatacyjne w zakresie projektowania, wdrażania i odbioru systemów informatycznych planowanych do wdrożenia, takich jak: wymagana architektura systemu, sposób licencjonowania i wykorzystania praw autorskich, zgodność z obowiązującym prawem, m.in. z ustawą z dnia 16 lipca 2014 r. *Prawo telekomunikacyjne*[23] i ustawą *o informatyzacji*, sposób i poziom zabezpieczeń, zastosowanie norm i standardów przemysłowych, zastosowanie rozwiązań funkcjonalnych odpowiednich dla osiągnięcia założonych celów, prezentacji treści dla osób z niepełnosprawnościami, wydajności, poziomu niezawodności SLA, mechanizmów kontroli i audytu, sposobu dostarczenia i instalacji systemu informatycznego oraz wymagania sprzętowe i środowiskowe dla systemu, sposób i zakres testów oraz dokumentacji oraz warunki i kryteria odbioru. Wymagania na nowe systemy informatyczne lub modyfikacje istniejących systemów formułowane są w MNiSW w sposób doraźny w oparciu o wzory umów wykonawców oraz bieżące potrzeby zamawiającego.

Nie potwierdzono funkcjonowania formalnych regulacji dotyczących procesu zarządzania zmianami w systemach MNiSW, w tym analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany.

W MNiSW realizowany jest ciągły proces zarządzania i monitorowania systemów informatycznych i środowiska ich pracy pod kątem bezpieczeństwa wydajności i pojemności, co pozwala na przewidywanie i zapobieganie ewentualnym problemom z tym związanym, a także zarządzanie, monitorowanie i diagnostykę systemów informatycznych w MNiSW, w tym: serwerów, stacji roboczych i infrastruktury sieciowej.

(Dowód: akta kontroli str. 41, 46-141, 222-227)

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

W celu uzyskania odpowiedniego poziomu BI przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników, stosowanych jest szereg zabezpieczeń informatycznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji. Zastosowane zabezpieczenia powinny być adekwatne do poziomu ryzyka wynikającego z analizy ryzyka BI.

Zgodnie z § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI w MNiSW zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami oraz ustalono zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie poprzez:

[23] Dz. U. 2014 r. poz. 243 z późn. zm.

a) zabezpieczenie dostępu do informacji poprzez wymuszone logowanie użytkowników z podaniem unikalnego hasła do systemów MNiSW;

b) kontrolę i monitorowanie ruchu osobowego, zabezpieczenia fizycznego dostępu do pomieszczeń;

c) podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez monitorowanie infrastruktury teleinformatycznej, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę zgłoszeń serwisowych, analizę incydentów naruszenia BI;

d) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowania zabezpieczeń kryptograficznych, stosowania systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall.

W MNiSW stosowano ogólne zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, zgodne z § 20 ust. 2 pkt 11 rozporządzenia KRI. Ogólne zasady postępowania zawarto w istniejącej PBI w MNiSW dotyczącej bezpieczeństwa danych osobowych jednak zastosowane zabezpieczenia nie wynikają z analizy ryzyka i planu postępowania z ryzykiem.

(Dowód: akta kontroli str. 41, 46-141, 222-227)

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Aby zapewnić bezpieczeństwo informacji przetwarzanych przez systemy teleinformatyczne niezbędne jest stosowanie szeregu zabezpieczeń techniczno-organizacyjnych dotyczących środowiska teleinformatycznego. Stosowanie zabezpieczeń powinno wynikać z analizy ryzyka i powstałej w jej wyniku planu postępowania z ryzykiem i deklaracji stosowania zabezpieczeń.

Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia KRI w MNiSW zapewniono odpowiedni poziom bezpieczeństwa systemów teleinformatycznych poprzez:

a) aktualizację oprogramowania oraz redukcję ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych (poprzez wdrażanie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących ich bezpieczeństwo, aktualizację oprogramowania antywirusowego i antyspamowego, aktualizację oprogramowania zabezpieczającego ruch sieciowy);

b) minimalizowanie ryzyka utraty informacji w wyniku awarii oraz ochronę przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnienie bezpieczeństwa plików systemowych (poprzez zastosowanie redundantnych rozwiązań sprzętowych w tym: dwustronnego zasilania, redundancji klimatyzacji, zastosowanie klastra serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, równoważenie obciążenia (ang. load balancing), monitorowanie parametrów środowiskowych w serwerowni (temperatura, wilgotność, zadymienie), zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci);

c) zastosowanie mechanizmów kryptograficznych dla transmisji danych i poczty elektronicznej.

Stwierdzono, że serwerownia MNiSW umiejscowiona jest w pomieszczeniu wydzielonym z pokoju biurowego, co powoduje m in. nadmierne zagęszczenie instalacji teleinformatycznych.

Zastosowane w tym obszarze zabezpieczenia nie wynikają z analizy ryzyka i planu postępowania z ryzykiem.

(Dowód: akta kontroli str. 41, 46-141, 222-227)

2.14. Rozliczalność działań w systemach informatycznych

Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby w ustalonym zakresie. Dokumentowaniu w postaci zapisów w dziennikach systemów (logi) podlegają wszelkie działania związane z przetwarzaniem informacji, a także działania administracyjne, co zapewnia rozliczalność tych operacji, tj. informację kto, kiedy i co wykonał w systemie teleinformatycznym. Świadomość użytkowników, że żadne ich działanie nie zostanie anonimowe podnosi poziom BI. Informacje zawarte w logach powinny być regularnie przeglądane w celu wykrycia działań niepożądanych i powinny być przechowywane w bezpieczny sposób co najmniej 2 lata.

W badanym okresie MNiSW nie dysponowało regulacjami wewnętrznymi, w których zostałyby określone zasady prowadzenia logów systemowych, w tym sposobu ich gromadzenia, miejsca i okres ich przechowywania, a także ich systematycznego przeglądania i analizy w celu wykrycia działań niepożądanych. Pomimo braku odpowiednich regulacji wewnętrznych w systemach MNiSW będących przedmiotem kontroli rozliczalność działań użytkowników i administratorów podlegała dokumentowaniu w postaci zapisów w dziennikach systemów (logach). Zapisywanie logów na zewnętrznych nośnikach informacji dokonywane było w automatycznym procesie wykonywania kopi zapasowych. Jednakże z ustaleń wynika, że nie jest prowadzona systematyczna kontrola logów pod względem ich zawartości i okresu przechowywania, co jest niezgodne z § 21 ust. 1 i 2 rozporządzenia KRI.

(Dowód: akta kontroli str. 41, 46-141, 180-217)

USTALENIA:

1. Obowiązujące w MNiSW regulacje ograniczają zakres ochrony informacji do ochrony danych osobowych. W badanym okresie w MNiSW nie wprowadzono Systemu Zarządzania Bezpieczeństwem Informacji, co oznacza, że w ww. okresie w MNiSW ww. system nie został wdrożony i nie funkcjonował, zatem nie mógł być monitorowany, poddawany przeglądom i doskonalony. Wobec powyższego nie zostały spełnione wymagania § 20 ust. 1 rozporządzenia KRI. W chwili obecnej w MNiSW stworzone są warunki aktualizacji regulacji wewnętrznych dotyczących SZBI (opracowana i zatwierdzona Polityka Bezpieczeństwa Informacji z 19 października 2016 r.) w zakresie dotyczącym zmieniającego się otoczenia zgodnie z § 20 ust. 2 pkt 1 rozporządzenia KRI.
2. Stwierdzono, że w badanym okresie MNiSW nie posiadało odrębnych wewnętrznych regulacji dotyczących szacowania ryzyka utraty integralności, dostępności lub poufności informacji na potrzeby SZBI. Istniejące regulacje i tworzone na ich podstawie analizy ryzyka wykonywane

były na potrzeby kontroli zarządczej i w niewystarczający sposób obejmowały problematykę bezpieczeństwa informacji, przez co jedynie częściowo zostały spełnione wymagania określonego w § 20 ust. 2 pkt 3 rozporządzenia KRI.

3. Stwierdzono, że pomimo braku pisemnych procedur dotyczących i inwentaryzacji aktywów IT na potrzeby SZBI prowadzony jest rejestr zasobów teleinformatycznych zawierający informacje o zidentyfikowanych aktywach informatycznych, w tym sprzętu i oprogramowania służącego do przetwarzania informacji obejmującego ich rodzaj i konfigurację, zgodnie z wymaganiami § 20 ust. 2 pkt 2 rozporządzenia KRI.
4. W MNiSW w skuteczny sposób zarządzano uprawnieniami do pracy w systemach informatycznych, na bieżąco monitorowano dostęp do zasobów informatycznych, co jest zgodne z wymaganiami § 20 ust. 2 pkt 4 rozporządzenia KRI. Konta byłych pracowników w systemach informatycznych MNiSW były w okresie objętym badaniem sukcesywnie blokowane, zgodnie z § 20 ust. 2 pkt 5 rozporządzenia KRI.
5. Pomimo braku wewnętrznych regulacji dotyczących szkoleń użytkowników zaangażowanych w proces przetwarzania informacji w systemach informatycznych w ramach SZBI, podejmowane są skuteczne działania w tym zakresie, zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI. Niemniej jednak należy wskazać na brak cykliczności szkoleń.
6. W okresie objętym kontrolą w MNiSW nie ustanowiono wewnętrznych procedur w zakresie bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, a obowiązujące regulacje są w tym zakresie niewystarczające, co jest niezgodne z wymaganiem § 20 ust. 2 pkt 8 rozporządzenia KRI.
7. Umowy serwisowe zawarte przez MNiSW ze stronami trzecimi dotyczące badanych systemów, zawierały zapisy zapewniające odpowiedni poziom bezpieczeństwa informacji, co przy braku w okresie kontrolowanym stosowych regulacji wewnętrznych w tym zakresie, jedynie częściowo wypełnia wymagania § 20 ust. 2 pkt 10.
8. W okresie objętym kontrolą w MNiSW podlegały rejestracji i były procedowanie zgłoszenia dotyczące różnych zdarzeń w obszarze informatyki w tym incydenty naruszenia bezpieczeństwem informacji. Jednak nie ustanowiono wewnętrznych regulacji w zakresie obsługi incydentów związanych z naruszeniem bezpieczeństwa informacji w ramach SZBI. Oznacza to jedynie częściowe spełnione wymagania § 20 ust. 2 pkt 13 rozporządzenia KRI.
9. W okresie objętym kontrolą w MNiSW nie funkcjonowały regulacje określające zasady wykonywania audytów wewnętrznych systemów informatycznych na potrzeby SZBI. Przeprowadzony w tym czasie audyt był zlecony firmie zewnętrznej (nie był realizowany przez komórki audytu wewnętrznego), co oznacza jedynie częściową zgodność z § 20 ust. 2 pkt 14 rozporządzenia KRI.
10. W MNiSW zapewniono odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych polegający w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii zgodnie z wymaganiami § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI tworząc kopie zapasowe systemów i danych, realizując odpowiednie procedury wykonywania kopii zapasowych. Zastrzeżenie dotyczy zapewnienia przechowywania utworzonych kopii zapasowych w lokalizacji innej, niż lokalizacja serwerowni w której przetwarzane są zabezpieczane systemy.

11. Wymagania zawarte w § 15 ust. 1 rozporządzenia KRI zostały spełnione częściowo, ponieważ w MNiSW w badanym okresie nie funkcjonowały regulacje wewnętrzne określające szczegółowe wymagania techniczne, bezpieczeństwa i eksploatacyjne w zakresie projektowania, wdrażania i odbioru systemów informatycznych, a także ich użytkowania i serwisowania, a podejmowane działania w tym obszarze miały charakter doraźny. Jednocześnie realizowany jest ciągły proces zarządzania i monitorowania systemów informatycznych i środowiska ich pracy pod kątem bezpieczeństwa wydajności i pojemności, co pozwala na przewidywanie i zapobieganie ewentualnym problemom z tym związanym, a także zarządzanie, monitorowanie i diagnostyka systemów informatycznych w MNiSW, w tym: serwerów, stacji roboczych i infrastruktury sieciowej.
12. Zgodnie z § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI w MNiSW zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami oraz ustalono zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. Podkreślić jednak należy, że stosowane zabezpieczenia nie wynikają z analizy ryzyka i planu postępowania z ryzykiem.
13. Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia KRI w MNiSW zapewniono odpowiedni poziom bezpieczeństwa systemów teleinformatycznych pomimo, iż stosowane zabezpieczenia nie wynikają z analizy ryzyka i planu postępowania z ryzykiem.
14. W badanym okresie MNiSW nie dysponowało regulacjami wewnętrznymi, w których zostałyby określone zasady prowadzenia logów systemowych, w tym sposobu ich gromadzenia, miejsca i okresu ich przechowywania, a także ich systematycznego przeglądania i analizy w celu wykrycia działań niepożądanych. Pomimo, iż niektóre logi systemowe był archiwizowane, to nie jest prowadzona ich systematyczna kontrola pod względem zawartości i okresu przechowywania co powoduje jedynie częściową zgodność z wymaganiami § 21 ust. 1 i 2 rozporządzenia KRI.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób z niepełnosprawnościami

W eksploatowanych systemach teleinformatycznych powinny zostać zastosowane rozwiązania techniczne umożliwiające osobom niedosłyszącym lub niedowidzącym zapoznanie się z treścią informacji m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu, czy też odsłuchanie wyświetlanej treści - zgodnie ze standardem WCAG 2.0. Termin dostosowania systemów teleinformatycznych do prezentacji zasobów informacyjnych wg. powyższego standardu upłynął 30 maja 2015 r.

Strony internetowe badanych systemów MNiSW nie zostały w pełni dostosowane do odbioru ich treści przez osoby z niepełnosprawnościami. Zastosowane rozwiązania techniczne umożliwiające osobom niedowidzącym zapoznanie się z treścią informacji poprzez powiększenie czcionki dotyczyły głównie podstawowych informacji ogólnych umieszczonych na głównej stronie urzędu. Pozostałe treści, w tym np. załączone dokumenty w formatach PDF i doc nie były dostosowane do potrzeb osób niedowidzących. System POL-on nie został dostosowany do odbioru treści przez osoby z niepełnosprawnościami, co oznacza niespełnienie wymagań określonych w § 19 rozporządzenia KRI.

(Dowód: akta kontroli str. 41)

Ustalenie:

1. Z systemów MNiSW będących przedmiotem badania, strona internetowa urzędu jest częściowo dostosowana do odbioru prezentowanych treści przez osoby niepełnosprawne natomiast system Pol-on nie wypełnia wymogów określony w WCAG 2.0., co oznacza niespełnienie wymagań określonych w § 19 rozporządzenia KRI.

* * *

Po zbadaniu *działania systemów teleinformatycznych, używanych do realizacji zadań publicznych oraz realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji 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,*

zalecam

1. Określenie i zakomunikowanie, a następnie monitorowanie poziomu jakościowego świadczenia usług elektronicznych w oparciu o model usługowy, zgodnie z wymaganiem określonym w § 15 ust. 2 rozporządzenia KRI.
2. Przeprowadzenie analizy rejestrów MNiSW pod kątem identyfikacji danych, które zostały pierwotnie wprowadzone do innego rejestru publicznego uznanego za referencyjny oraz przeprowadzenie analizy możliwości techniczno-organizacyjnych wymiany danych poprzez bezpośrednie odwołanie się do danych referencyjnych przez rejestr MNiSW inicjujący wymianę, zgodnie z wymaganiem określonym w § 5 ust. 3 pkt 3 rozporządzenia KRI.
3. Wdrożenie SZBI (zgodnie z przyjętymi w MNiSW założeniami i planami oraz zatwierdzona Polityką Bezpieczeństwa Informacji) zgodnie z wymaganiem określonym w § 20 ust. 2 pkt 1 rozporządzenia KRI, a następnie sukcesywne monitorowanie, poddawanie przeglądom i doskonalenie SZBI zgodnie z wymaganiem określonym w § 20 ust. 1 rozporządzenia KRI.
4. Zarządzanie ryzykiem utraty integralności, dostępności lub poufności informacji w oparciu o wewnętrzne regulacje w ramach SZBI, w tym przeprowadzane cyklicznych analizy ryzyka BI, tworzenie planów postępowania z ryzykiem zgodnie z wymaganiem określonym w § 20 ust. 2 pkt 3 rozporządzenia KRI.
5. Organizowanie cyklicznych szkoleń osób zaangażowanych w proces przetwarzania informacji, w związku ze zmieniającymi się zagrożeniami bezpieczeństwa informacji i stosowanymi zabezpieczeniami, zgodnie z wymaganiem określonym w § 20 ust. 2 pkt 6 rozporządzenia KRI.
6. Ustanowienie w ramach SZBI podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, zgodnie z wymaganiem określonym w § 20 ust. 2 pkt 8 rozporządzenia KRI.
7. Ustanowienie w ramach SZBI wewnętrznych przepisów regulujących tematykę zawierania ze stronami trzecimi umów serwisowych gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z wymaganiem określonym § 20 ust. 2 pkt 10 rozporządzenia KRI.
8. Rozszerzenie zakresu istniejącej procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji (dotyczącej naruszenia ochrony danych osobowych) na wszystkie incydenty dotyczące

naruszenia bezpieczeństwa informacji, zgodnie z wymaganiem określonym w § 20 ust. 2 pkt 13 rozporządzenia KRI.

9. Zapewnienia przechowywania utworzonych kopii zapasowych w lokalizacji innej, niż lokalizacja serwerowni w której przetwarzane są zabezpieczane systemy.
10. Ustanowienie w ramach SZBI wewnętrznych przepisów określających szczegółowe wymagania techniczne, bezpieczeństwa i eksploatacyjne w zakresie projektowania wdrażania i odbioru systemów informatycznych, a także ich użytkowania i serwisowania zgodnie z wymaganiem określonym w § 15 ust. 1 rozporządzenia KRI.
11. Ustanowienie w ramach SZBI i stosowanie wewnętrznych przepisów, w których zostałyby określone zasady prowadzenia logów systemowych, w tym sposób ich gromadzenia, miejsce i okres ich przechowywania, a także ich systematycznego przeglądania i analizy w celu wykrycia działań niepożądanych, zgodnie z wymaganiem określonym w § 21 ust. 1 i 2 rozporządzenia KRI.
12. Dostosowanie systemów MNiSW dla obsługi przez osoby z niepełnosprawnościami w oparciu o wymagania określone w dokumencie WCAG 2.0, zgodnie z § 19 rozporządzenia KRI.

Mając na uwadze powyższe uprzejmie informuję, że zgodnie z art. 46 ust. 3 pkt 3 ustawy *o kontroli w administracji rządowej* oczekuję od Pana Ministra, w terminie 60 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, informacji o sposobie wykorzystania wyżej wymienionych uwag i wniosków; a także o podjętych działaniach lub przyczynach niepodjęcia działań.

* * *

Niniejsze Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach.

2 up.
DYREKTOR
Biura Ministra
Ministerstwa Cyfryzacji
Dominika WALIGÓRSKA

Wykonano w 2 egz.:
Egz. Nr 1 – Ministerstwo Nauki i Szkolnictwa Wyższego
ul. Hoża 20, 00-529 Warszawa,
Egz. Nr 2 – aa.

Sporządził: Zespół kontrolny