MINISTER EDUKACJI I NAUKI

Warszawa, 16 listopada 2020 r.

DKO-WEK.0913.1.2019

Pan
Marcin Smolik
Dyrektor
Centralnej Komisji Egzaminacyjnej
ul. Józefa Lewartowskiego 6
00-190 Warszawa

Wystąpienie pokontrolne

Zgodnie z art. 47 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej* (Dz. U. Nr 185, poz. 1092) przedstawiam *Wystąpienie pokontrolne* z kontroli przeprowadzonej w Centralnej Komisji Egzaminacyjnej dotyczącej *działania i bezpieczeństwa wybranych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych.*

Na podstawie art. 6 ust. 3 pkt 1 *ustawy o kontroli w administracji rządowej* oraz art. 25 ust. 1 pkt 3 lit. b ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (j.t. Dz. U. z 2017 r. poz. 570), Ministerstwo Edukacji Narodowej[1] w okresie od 25 listopada 2019 r. do 17 stycznia 2020 r. przeprowadziło kontrolę w Centralnej Komisji Egzaminacyjnej, z siedzibą w Warszawie przy ul. Józefa Lewartowskiego 6.

---

[1] Kontrolę przeprowadzili pracownicy Ministerstwa Edukacji Narodowej:

1. Pan Marian Piotr Romanowski, główny specjalista w Wydziale Efektów Kształcenia Departamentu Kształcenia Ogólnego, na podstawie upoważnienia nr 50/2019 z 25 listopada 2019 r.,
2. Pani Urszula Witkowska, naczelnik wydziału w Wydziale Efektów Kształcenia Departamentu Kształcenia Ogólnego, na podstawie upoważnienia nr 49/2019 z 25 listopada 2019 r.,
3. Pani Magdalena Tomaszewska, kierownik Zakładu Aplikacji i Systemów Informatycznych w Centrum Informatycznym Edukacji Ministerstwa Edukacji Narodowej, na podstawie upoważnienia nr 51/2019 z 25 listopada 2019 r.,
4. Pan Marcin Napiórski, kierownik Zakładu Infrastruktury Teleinformatycznej w Centrum Informatycznym Edukacji Ministerstwa Edukacji Narodowej, na podstawie upoważnienia nr 52/2019 z 25 listopada 2019 r.,
5. Pan Maciej Moraczewski, starszy informatyk w Zakładzie Infrastruktury Teleinformatycznej w Centrum Informatycznym Edukacji Ministerstwa Edukacji Narodowej, na podstawie upoważnienia nr 06/2020 z 30 kwietnia 2020 r.

Kontrola została przeprowadzona w zakresie działania i bezpieczeństwa wybranych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych. Kontrola stanowiła realizację Planu Kontroli Ministra Edukacji Narodowej na rok 2019 oraz priorytetu Szefa Kancelarii Prezesa Rady Ministrów na rok 2019: *Bezpieczeństwo teleinformatyczne w administracji rządowej*.

Celem kontroli było:

1) sprawdzenie, czy procedury i regulacje wewnętrzne dotyczące systemów teleinformatycznych wykorzystywanych przez CKE do realizacji zadań publicznych, spełniają minimalne wymagania w zakresie elektronicznej wymiany informacji (interoperacyjności) oraz bezpieczeństwa i dostępności informacji;
2) ocena funkcjonujących procedur zapewniających:
   - współdziałanie różnych systemów teleinformatycznych poprzez właściwą organizację wymiany informacji w postaci elektronicznej, współpracę z innymi systemami informatycznymi oraz procesy wspomagania świadczenia usług drogą elektroniczną;
   - skuteczne zarządzanie bezpieczeństwem informacji dla badanych systemów teleinformatycznych, w tym zapewnienia dostępności, autentyczności, poufności, niezawodności i integralności danych przetwarzanych przez system;
3) sprawdzenie dostępności treści zawartych na stronach internetowych dla osób z niepełnosprawnościami.

Kontrolą objęto okres od 1 stycznia 2017 r. do 26 listopada 2019 r. (tj. dnia rozpoczęcia kontroli).

Centralna Komisja Egzaminacyjna (dalej: CKE) została powołana z dniem 1 stycznia 1999 r. na mocy ustawy z dnia 25 lipca 1998 r. o *zmianie ustawy o systemie oświaty* (Dz. U. Nr 117, poz. 759). Zadania CKE zostały określone w art. 9a ust. 2 ustawy z dnia 7 września 1991 r. *o systemie oświaty* (j.t. z dnia 18 czerwca 2020 r. Dz. U. z 2020 r. poz. 1327).

Obszary objęte kontrolą regulowały następujące przepisy:

- art. 9c ust. 2 i 9d ust. 1 ustawy z dnia 7 września 1991 r. *o systemie oświaty* (j.t. Dz. U. z 2019 r. poz. 1481, z późn. zm.) – dalej: *ustawa o systemie oświaty*;
- art. 25 ust. 1 pkt 3 lit. b ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne, dotyczącego przeprowadzania kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych* (j.t. Dz. U. z 2019 r. poz. 700, z późn. zm.) – dalej: *ustawa o informatyzacji*;

- ustawa z dnia 4 kwietnia 2019 r. *o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych* (Dz. U. poz. 848) – dalej: *ustawa o dostępności cyfrowej;*
- 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* (j.t. Dz. U. z 2017 r. poz. 2247, z późn. zm.) – dalej: *rozporządzenie KRI.*

W CKE wykorzystywane są następujące systemy teleinformatyczne:
- System Informatyczny Obsługi Egzaminów Potwierdzających Kwalifikacje w Zawodzie – służący do organizacji i obsługi egzaminu potwierdzającego kwalifikacje w zawodzie;
- Scoris Assessor – służący do przeprowadzania oceniania egzaminu gimnazjalnego z matematyki w trybie zdalnym;
- System Informatyczny Obsługi Banków Zadań;
- Serwis BIP – służący do realizacji przepisów o dostępie do informacji publicznej;
- Elektroniczna skrzynka podawcza (ESP).

Kontrolą objęto System Informatyczny Obsługi Egzaminów Potwierdzających Kwalifikacje w Zawodzie (dalej: SIOEPKZ). System został wyprodukowany przez Polską Wytwórnię Papierów Wartościowych S.A. i uruchomiony produkcyjnie 1 stycznia 2018 r.

Celem stosowania SIOEPKZ jest organizacja i obsługa egzaminu potwierdzającego kwalifikacje w zawodzie. Główne funkcje systemu to:
- zgłaszanie oraz przesyłanie deklaracji przystąpienia do egzaminu zdających,
- planowanie egzaminu,
- przeprowadzanie elektronicznego egzaminu za pomocą wirtualnego serwera egzaminacyjnego,
- zamawianie i wprowadzanie zadań egzaminacyjnych,
- udostępnianie wyników i statystyk szkołom i zdającym.

System przetwarza dane osobowe dyrektorów i pracowników szkół, egzaminatorów, zdających, informacje o wynikach egzaminów zdających. Przetwarzane są również treści zadań i harmonogramy wszystkich egzaminów potwierdzających kwalifikacje w zawodzie. Wewnętrznymi użytkownikami systemu są pracownicy CKE, oke oraz firmy utrzymującej system. Aktualnie w systemie znajduje się około 30000 użytkowników (dyrektorzy i pracownicy szkół, egzaminatorzy, pracownicy CKE i oke).

Ocena działalności kontrolnej.

Na podstawie wyników kontroli, działalność CKE w zakresie objętym kontrolą została oceniona pozytywnie z uchybieniami. Uchybienia stwierdzono w dwóch kontrolowanych obszarach, tj. w obszarze bezpieczeństwa informacji oraz w obszarze dostosowania treści zawartych na stronach internetowych dla osób z niepełnosprawnościami.

Ocenie podlegały niezależnie trzy główne obszary kontroli, tj. interoperacyjność systemów teleinformatycznych, bezpieczeństwo informacji oraz dostosowanie systemów teleinformatycznych dla osób niepełnosprawnych. Ocenę kontrolowanej działalności uzasadniają ustalenia kontroli.

W trakcie kontroli analizą objęto procedury i regulacje wewnętrzne CKE dotyczące badanego obszaru, tj.:

- zarządzenie nr 670 dyrektora CKE *w sprawie wprowadzenia polityki bezpieczeństwa* i *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych*,
- zarządzenie nr 518 dyrektora CKE *w sprawie wprowadzenia w CKE Polityki Bezpieczeństwa SIOEPKZ i SIOBZ* (dalej: *Polityka bezpieczeństwa SIOEPKZ*),
- zarządzenie nr 594 dyrektora CKE z 5.10.2017 r. – *Instrukcja inwentaryzacyjna*,
- zarządzenie nr 521 dyrektora CKE *zmieniające zarządzenie w sprawie wprowadzenia instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt, instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego CKE* (dalej: JRWA),
- dokumentację powykonawczą – warstwa infrastrukturalna SIOEPKZ,
- dokumentację powykonawczą – procedura aktualizacji oprogramowania systemowego SIOEPKZ,
- dokumentację powykonawczą – procedura aktualizacji oprogramowania systemowego SIOEPKZ,
- dokumentacja powykonawczą – procedura odtwarzania serwera fizycznego SIOEPKZ,
- dokumentację powykonawczą – procedura uruchomienia SIOEPKZ,
- dokumentację powykonawczą – procedura wyłączenia SIOEPKZ,
- dokumentację powykonawczą – procedura wymiany taśm SIOEPKZ,
- dokumentację powykonawczą – procedura zmiany retencji kopii bezpieczeństwa na taśmie SIOEPKZ,
- dokumentację powykonawczą – warstwa infrastrukturalna – procedury utrzymaniowe SIOEPKZ,
- dokumentację powykonawczą – warstwa bazy danych SIOEPKZ,
- dokumentację powykonawczą – warstwa aplikacji SIOEPKZ.

Wyniki kontroli w poszczególnych obszarach.

I. **Interoperacyjność – wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.**

Wymogi dotyczące interoperacyjności systemów teleinformatycznych zostały określone w § 5, 15 - 18 i 20 - 21 *rozporządzenia KRI* oraz art. 16 *ustawy o informatyzacji*.

Zgodnie z art. 16 ust. 1a *ustawy o informatyzacji* CKE udostępnia elektroniczną skrzynkę podawczą spełniającą standardy określone przez ministra właściwego do spraw informatyzacji oraz zapewnia jej obsługę. Na głównej stronie Biuletynu Informacji Publicznej (dalej: BIP) CKE zamieszczony jest odnośnik do platformy e-PUAP, jednak ze względu na niepowiązanie go z hiperłączem, kliknięcie odnośnika nie powoduje nawiązania połączenia z e-PUAP.

Adres skrytki odbiorczej platformy e-PUAP jest dostępny na stronie BIP CKE, jednak jest zamieszczony w sposób nieintuicyjny (nie jest zamieszczony w „kontakty" ale w „załatwianie spraw"→ „skargi, wnioski i petycje"). Należy zwrócić uwagę, że zgodnie z § 5 ust. 2 pkt 1 i 4 *rozporządzenia KRI*, na stronie BIP powinny być zamieszczane i aktualizowane opisy procedur obowiązujących przy załatwianiu spraw drogą elektroniczną oraz o sposobie dostępu oraz zakresie użytkowym serwisów CKE.

Zgodnie z § 15 ust. 2 *rozporządzenia KRI* CKE zarządza systemami w taki sposób' aby dostarczać usługi na deklarowanym poziomie dostępności na podstawie udokumentowanej procedury. W celu realizacji tych zobowiązań w umowie utrzymania systemu SIOEPKZ zdefiniowano SLA (*service level agreement*[2]) oraz *Politykę bezpieczeństwa SIOEPKZ*. Zleceniobiorca został zobligowany do działania zgodnie z normami jakości ISO/IEC 9001, bezpieczeństwa ISO/IEC 27001, zarządzania usługami w IT ISO/IEC 20000, zarządzania ciągłością działania ISO 22301 lub równoważnymi, tj. zapewniającymi osiągnięcie wszystkich minimalnych paramentów określonych w ww. normach.

Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie zostało uregulowane w zarządzeniu nr 521 dyrektora CKE *w sprawie wprowadzenia instrukcji kancelaryjnej JRWA, instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego*.

---

[2] SLA to umowa o gwarantowanym poziomie świadczenia usług poprzez ustalenie między klientem a usługodawcą poziomu jakości usług w stałym cyklu obejmującym: uzgodnienia, monitorowanie usługi, raportowanie i przegląd osiąganych wyników.

Serwery systemu SIOEPKZ połączone są za pomocą dedykowanych urządzeń sprzętowo-szyfrujących mających certyfikaty ABW/SKW.

Systemy teleinformatyczne CKE realizują przesłanki interoperacyjności zawarte w rozporządzeniu KRI. Wymiana uporządkowanych w określonej strukturze danych, między systemami wykazanymi w trakcie kontroli, odbywa się za pomocą sieci teleinformatycznej.

Na podstawie ustaleń dokonanych w trakcie kontroli stwierdzono, że w obszarze interoperacyjności CKE otrzymuje ocenę cząstkową pozytywną.

II. Bezpieczeństwo informacji – system zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

Wymogi dotyczące systemu zarządzania bezpieczeństwem informacji zostały określone w § 20 *rozporządzenia KRI*.

Zgodnie z § 20 ust. 1-2 *rozporządzenia KRI*, w CKE opracowano, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), który zapewnia poufność, dostępność i integralność informacji z uwzględnieniem autentyczności, rozliczalności, niezaprzeczalności i niezawodności.

W ramach SZBI, opracowano:
- *Politykę bezpieczeństwa systemów SIOEPKZ i SIOBZ*, która została wprowadzona zarządzeniem nr 518 dyrektora CKE z 1 grudnia 2016 r.,
- *Politykę bezpieczeństwa i instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych*, która została wprowadzona zarządzeniem nr 670 dyrektora CKE z 26 września 2018 r.

SZBI jest monitorowany i poddawany przeglądom w ramach umowy utrzymaniowej. Raz w tygodniu odbywają się spotkania komitetu do spraw systemu (w skład komitetu wchodzi dyrekcja CKE oraz specjaliści i pracownicy firmy utrzymaniowej). Zgodnie z wyjaśnieniami CKE, do dnia przeprowadzenia kontroli nie zaistniała potrzeba nowelizowania *Polityki bezpieczeństwa*.

Zakres utrzymania aktualności inwentaryzacji sprzętu i oprogramowania Systemu, został uregulowany w umowie utrzymaniowej. Raz w miesiącu przekazywane są aktualne kody źródłowe systemów umożliwiających niezależne uruchomienie systemów. Kody są niezbędne w sytuacjach kryzysowych, np. po całkowitym załamaniu systemu we wszystkich lokalizacjach. Kody źródłowe systemu są przechowywane w kilku lokalizacjach (innych niż lokalizacja elementów systemu). Zgodnie z umową wykonawca dokonuje przeglądu sprzętu infrastruktury z dostatecznym wyprzedzeniem pozwalającym utrzymać ciągłość

działania systemu po wygaśnięciu umowy.

Zasady udzielania dostępu do poszczególnych elementów i danych Systemu określone zostały w *Polityce bezpieczeństwa SIOEPKZ* w pkt. 7.

Zgodnie z § 20 ust. 2 pkt 4 - 5 *rozporządzenia KRI*, zarządzanie bezpieczeństwem informacji realizowane jest przez: podejmowanie 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 (pkt 4); bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4 (pkt 5).

Uprawnienia udzielone użytkownikom Systemu są okresowo przeglądane w kontekście ról wykonywanych w systemie. Z dniem ustania stosunku pracy pracownika, uprawnienia są bezzwłocznie odbierane. Użytkownicy przy każdym logowaniu do systemu potwierdzają znajomości polityki bezpieczeństwa. Dostęp do pracy w systemie udzielany jest po wcześniejszym zapoznaniu się z elementami polityki bezpieczeństwa właściwymi dla danej roli użytkownika w systemie.

Zgodnie z § 20 ust. 2 pkt 14 *rozporządzenia KRI* zarządzanie bezpieczeństwem informacji realizowane jest przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. W trakcie kontroli ustalono, że w CKE nie realizowano audytu wewnętrznego w zakresie bezpieczeństwa informacji co najmniej raz w roku.

Zgodnie z wyjaśnieniem CKE: *Audytor wewnętrzny zatrudniony jest obecnie w CKE na 0,5 etatu. W związku z liczną tematyką działań audytowych przeprowadzanie audytu raz w roku nie było możliwe.*

W 2019 r. w CKE przeprowadzony został audyt zewnętrzny w zakresie bezpieczeństwa informacji SIOEPKZ przez podmiot zewnętrzny. W raporcie z audytu zawarto informacje o podatnościach w zakresie aplikacji. W opinii kontrolerów podatności te mogą stwarzać ryzyko wystąpienia zdarzeń związanych z naruszeniem bezpieczeństwa informacji.

CKE poinformowało również, że: (...) *audyty wewnętrzne odnoszące się do KRI będą od 2020 roku przeprowadzane pod koniec każdego roku kalendarzowego.*
Audyt wewnętrzny w zakresie bezpieczeństwa informacji, na 2020 rok został zaplanowany na IV kwartał.

We wrześniu 2020 r. CKE powołała zespół ds. obsługi informatycznej (ZOI). CKE poinformowała, że: *w zakres kompetencji kierownika ZOI wchodzi*

bezpośrednio nadzorowanie działań odnoszących się do bezpieczeństwa informacji zgodnie z KRI. Umiejscowienie działań odnoszących się do KRI w dedykowanym zespole, w którym zostali zatrudnieni specjaliści ds. systemów informatycznych, pozwoli na pełniejsze ustrukturyzowanie działań CKE w zakresie KRI.

CKE poinformowała, że funkcjonalności w systemie SIOEPKZ obciążone podatnością na dane zagrożenie są dostępne tylko dla konkretnych typów użytkowników i ich priorytet jest nieproporcjonalny do liczby osób, które mają do nich dostęp. 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 z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Rozporządzenie KRI nie różnicuje więc zabezpieczenia systemów zależnie od liczby użytkowników. Wobec powyższego, mniejsza liczba użytkowników systemu nie może być wskazaniem do ograniczenia zabezpieczeń systemowych. Mając na uwadze przepisy rozporządzenia KRI stwierdzone w ww. raporcie z audytu zewnętrznego podatności powinny zostać usunięte.

Konstrukcja Systemu zapewnia odpowiedni poziom bezpieczeństwa polegający w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii (zgodnie z § 20 ust. 2 pkt 12 lit. b *rozporządzenia KRI*). Celem zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami określone zostały procedury bezpieczeństwa w *Polityce bezpieczeństwa SIOEPKZ* w pkt. 8 „Bezpieczeństwo fizyczne i środowiskowe" (zgodnie z § 20 ust. 2 pkt 7 *rozporządzenia KRI*).

W ocenie kontrolujących niektóre zapisy *Polityki bezpieczeństwa SIOEPKZ* są zbyt szczegółowe. Ujawnienie niektórych informacji zawartych w dokumencie może mieć wpływ na zapewnienie bezpieczeństwa informacji. W związku z powyższym, zasadne jest przeprowadzenie analizy dokumentu w zakresie obecnego stopnia szczegółowości informacji w nim zawartych, a wrażliwych dla środowiska systemu.

Zgodnie z § 20 ust. 2 pkt 3 *rozporządzenia KRI* zarządzanie bezpieczeństwem informacji realizowane jest również przez przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

CKE na bieżąco monitoruje ryzyka związane z utrzymaniem, środowiskiem utrzymania i zmianami w Systemie SIOEPKZ, w postaci przeprowadzanej analizy ryzyka. Analiza ryzyka skupia się jednak głównie na ryzykach związanych z danymi przetwarzanymi w systemie, a w małym stopniu na aspektach związanych z analizą bezpieczeństwa, ciągłością działania i obciążeniem systemu. Nie określane są ryzyka związane ze środowiskiem technicznym, niezbędnym do przetwarzania danych systemu SIOEPKZ.

Podczas kontroli ustalono przewidywany czas utrzymania Systemu (50 lat), liczbę lokalizacji Sytemu (tj. 9 lokalizacji).

Biorąc powyższe pod uwagę w ocenie kontrolerów zasadne jest zatem objęcie analizą ryzyka również ww. spraw związanych z utrzymaniem systemu SIOEPKZ, w tym liczbę lokalizacji.

CKE nie prowadzi planów postępowania ze zidentyfikowanymi ryzykami. Plany te wspomagałyby proces monitorowania ryzyk, w przypadkach gdyby proces ich minimalizacji był długotrwały lub ich minimalizacja nie była możliwa.

CKE nie przeprowadzało testów ciągłości działania w przypadku awarii jednej bądź wielu lokalizacji serwerowni oraz przeprowadzenia testów odtworzeniowych w przypadku awarii systemu. W rozdziale 12.1. *Polityki bezpieczeństwa CKE* zawarto, że:

- *Plany ciągłości działania muszą być aktualizowane i testowane w regularnych odstępach czasu co najmniej raz w roku. Po wykonaniu każdego testu sporządzany jest pisemny raport do Kierownictwa CKE, zawierający szczegółowe rezultaty testu i opis środków zaradczych, jakie powinny być powzięte w przyszłości.*
- *Personel teleinformatyczno-techniczny, zajmujący się eksploatacją SIOEPKZ we współpracy z innymi jednostkami organizacyjnymi, musi przygotowywać, okresowo uaktualniać i regularnie testować plany reagowania na wypadek awarii lub katastrofy.*

Przedstawiony przez CKE miesięczny raport z działania systemu, nie zawierał informacji dotyczących przeprowadzania ww. testów.

System został przekazany do utrzymania podmiotowi zewnętrznemu. Utrzymanie systemu, zgodnie z dokumentacją, przewidziane jest na 50 lat. CKE nie posiada pełnej dokumentacji systemu SIOEPKZ. W opinii kontrolerów brak pełnej dokumentacji technicznej w CKE może mieć wpływ na działanie systemu, w przypadku potrzeby zmiany dostawcy usług utrzymania, rozszerzenia systemu lub integracji z innymi systemami.

W wyniku kontroli stwierdzono, że nie zostały opracowane niżej wymienione polityki wskazane w *Polityce bezpieczeństwa*, tj.:

- polityka zarządzania ciągłością działania,
- polityka przetwarzania mobilnego.

Zgodnie z § 20 ust. 2 pkt 6 *rozporządzenia KRI*, zarządzanie bezpieczeństwem informacji realizowane jest w również przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenia bezpieczeństwa informacji,
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

W okresie objętym kontrolą odbyły się następujące szkolenia grupowe, w których brali udział pracownicy oraz kierownictwo CKE:

- „Ochrona danych osobowych w praktyce – warsztaty kompetencyjne dla pracowników CKE" (10-11 maja 2018 r.),
- „Katalog właściwych zachowań wobec zagrożeń informacyjnych" (5-7 listopada 2019 r.).

CKE poinformowało również, że przedstawiciele CKE (tj. Pełnomocnik ds. ochrony informacji niejawnych i kierownik WAG koordynujący ochronę danych osobowych) wzięli udział w V Konferencji Naukowej – Ochrona Danych Osobowych, Informacji Niejawnych i Prawnie Chronionych w Systemie Bezpieczeństwa Państwa (w dniu 26 września 2019 r.), a doświadczenie i wiedza nabyte podczas tej konferencji są wykorzystywane w bieżących działaniach związanych z bezpieczeństwem informacji.

W zakresie szkoleń indywidulanych dla pracowników CKE odnoszących się do spraw bezpieczeństwa informacji poinformowano, że nowo zatrudnieni pracownicy CKE są zapoznawani z zasadami ochrony informacji. Przeszkolenie w ww. zakresie pracownik potwierdza podpisem na oświadczeniu o zachowaniu danych w poufności, którego wzór stanowi załącznik do ogólnej polityki bezpieczeństwa CKE.

CKE przekazało również nw. informacje, że użytkownik systemu potwierdza znajomości polityki bezpieczeństwa i skutków jej naruszania przy każdym logowaniu do systemu w zależności od roli jaką pełni. Użytkownik ma dostęp do pracy w systemie po wcześniejszym zapoznaniu się z elementami polityki bezpieczeństwa.

Na podstawie ustaleń dokonanych w trakcie kontroli stwierdzono, że w obszarze bezpieczeństwa informacji CKE otrzymuje ocenę cząstkową pozytywną z uchybieniami.

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

WCAG (*web content accessability guidelines*) to zbiór rekomendacji, których należy przestrzegać, aby zapewnić dostęp do treści internetowych możliwie szerokiej grupie użytkowników, włączając w to osoby z niepełnosprawnościami. Wymogi określone w ww. dokumencie zostały wprowadzone do obowiązującego prawa i zapisane w § 19 i załączniku 4 do *rozporządzenia KRI*.

Ustawa o *dostępności cyfrowej* zobowiązuje w art. 10 ust. 1 podmioty publiczne do sporządzenia *Deklaracji dostępności w sposób dostępny cyfrowo*. Deklaracja dostępności na stronie BIP podmiotu powinna zostać opublikowana od 23 września 2019 r.

W górnym pasku strony internetowej CKE jest odnośnik „Deklaracja dostępności" dodatkowo oznaczony symbolem osoby na wózku inwalidzkim, jednak po kliknięciu użytkownik jest informowany, że strona jest w trakcie przygotowania. Na stronie BIP CKE jest zamieszczony dokument pn. „Oświadczenie o dostępności cyfrowej 2019". Dokument ten jest jednak zamieszczony w nieoczywistym miejscu, tj. działalność CKE→dostępność cyfrowa. Zgodnie z ww. dokumentem „CKE oświadcza, że jej strony internetowe są w pełni zgodne z przepisami ustawy[3]". Nie stwierdzono dowodów przeprowadzenia testów potwierdzających spełnienie wymogów dostępności WCAG.

Na podstawie ustaleń dokonanych w trakcie kontroli stwierdzono, że w obszarze dostosowania dla osób z niepełnosprawnościami CKE otrzymuje ocenę cząstkową pozytywną z uchybieniami.

Zalecenia i wnioski

Na podstawie art. 46 ust. 3 pkt 1 *ustawy o kontroli w administracji rządowej*, w związku z wyżej przedstawionymi ustaleniami, poniżej przedstawiam zalecenia oraz wnioski:

Zalecenia:

1. Doprowadzić do pełnego stosowania przepisów § 5 ust. 2 pkt 1 i 4 *rozporządzenia KRI*, zgodnie z którymi na stronie BIP powinny być zamieszczane i aktualizowane opisy procedur obowiązujących przy załatwianiu spraw drogą elektroniczną oraz o sposobie dostępu oraz zakresie użytkowym serwisów CKE.

[3] *Ustawa o dostępności cyfrowej.*

2. Przeprowadzać okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok, zgodnie z § 20 ust. 2 pkt 14 *rozporządzenia KRI*.
3. Usunąć podatności w zakresie aplikacji stwierdzone w raporcie z audytu zewnętrznego z 2019 r.
4. Przeprowadzać testy ciągłości działania w przypadku awarii jednej bądź wielu lokalizacji serwerowni oraz przeprowadzać testy odtworzeniowe w przypadku awarii systemu.
5. Opracować, zgodnie z *Polityką bezpieczeństwa*, nie opracowane dotychczas polityki: politykę zarządzania ciągłością działania i politykę przetwarzania mobilnego.

Wnioski:

1. Przeprowadzić analizę polityki bezpieczeństwa SIOEPZK w zakresie stopnia szczegółowości informacji w niej zawartych celem możliwości ich ograniczenia.
2. W analizie ryzyka związanej z utrzymaniem, środowiskiem utrzymania i zmianami w Systemie SIOEPKZ, uwzględniać ryzyka związane ze środowiskiem technicznym, tj. utrzymaniem systemów oraz przewidywanym czasem ich funkcjonowania, jak również rozważyć stworzenie planów postępowania ze wszystkimi zidentyfikowanymi ryzykami.
3. Zapewnić w siedzibie CKE dostęp do pełnej dokumentacji systemu SIOEPKZ.
4. Zamieszczać deklarację dostępności w taki sposób, aby użytkownik strony internetowej mógł mieć do niej dostęp podczas nawigacji po stronie oraz podjąć działania celem udokumentowania spełniania wymogów dostępności WCAG.

Na podstawie art. 49 *ustawy o kontroli w administracji rządowej*, przedstawiając powyższe wystąpienie pokontrolne, proszę o przekazanie, w terminie 21 dni od daty otrzymania niniejszego wystąpienia, informacji o sposobie wykonania zaleceń i wniosków.

Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach.