MINISTER EDUKACJI NARODOWEJ

Warszawa, 29 kwietnia 2019 r.

BK-WKI.0915.2.2018.FS

Pani Jadwiga Szczypiń
Dyrektor Ośrodka Rozwoju Edukacji

WYSTĄPIENIE POKONTROLNE

Zgodnie z art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. nr 185, poz. 1092) przekazuję wystąpienie pokontrolne.

Na postawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092) oraz art. 25 ust. 1 pkt 3 lit. b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 j.t.), Ministerstwo Edukacji Narodowej[1] w okresie od 22 października do 14 grudnia 2018 r. przeprowadziło kontrolę w Ośrodku Rozwoju Edukacji (dalej: ORE) z siedzibą w Warszawie przy Alejach Ujazdowskich 28.

Kontrola została przeprowadzona w zakresie realizacji obowiązków związanych z utrzymaniem bezpieczeństwa teleinformatycznego w obszarze zapewnienia ciągłości działania, integralności oraz dostępności systemów i sieci teleinformatycznych. Kontrolą objęto okres od 1 stycznia 2017 r. do 22 października 2018 r., tj. dnia rozpoczęcia kontroli.

Ośrodek Rozwoju Edukacji jest państwową jednostką budżetową utworzoną na mocy Zarządzenia Nr 19 Ministra Edukacji Narodowej z dnia 10 grudnia 2010 r. Zgodnie ze statutem[2], ORE jest publiczną placówką doskonalenia nauczycieli o zasięgu ogólnokrajowym, której celem jest podejmowanie i realizacja działań na rzecz doskonalenia systemu oświaty i podnoszenia jakości edukacji, zgodnie z polityką oświatową państwa w obszarze wychowania oraz kształcenia ogólnego, specjalnego, zawodowego i ustawicznego.

Do kontroli został wybrany, w sposób celowy, jeden z systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych,

---

[1] Kontrolę przeprowadził zespół kontrolujący:
1) Pan Franciszek Szkop – starszy specjalista w Wydziale Kontroli Instytucjonalnej Biura Kontroli Ministerstwa Edukacji Narodowej, kierownik zespołu kontrolnego – upoważnienie nr 45/2018 z dnia 09 października 2018 r.
2) Pani Bożena Koniorczyk – główny specjalista w Wydziale Kształcenia i Doskonalenia Nauczycieli Departamentu Kształcenia Ogólnego w Ministerstwie Edukacji Narodowej – upoważnienie nr 44/2018 z dnia 09 października 2018 r.
3) Pan Tomislav Petrović – p.o. Kierownika Zakładu Administracyjnego w Centrum Informatycznym Edukacji- jednostce podległej MEN – upoważnienie nr 46/2018 z dnia 09 października 2018 r.

[2] Statut ORE nadany został Zarządzeniem nr 39 Ministra Edukacji Narodowej z dnia 29 lipca 2016 r. w sprawie nadania statutu Ośrodkowi Rozwoju Edukacji w Warszawie.

tj. system npseo.pl - platforma systemu ewaluacji oświaty. System ten dostarcza narzędzi do sprawowania nadzoru pedagogicznego w szkołach i placówkach oświatowych. Jest wykorzystywany przez wizytatorów kuratoriów oświaty oraz pracowników: jednostek samorządu terytorialnego, MEN i ORE. System został uruchomiony w 2011 r.

Celem kontroli było zbadanie systemu npseo.pl w obszarze spełniania minimalnych wymagań w zakresie elektronicznej wymiany informacji (interoperacyjności), bezpieczeństwa i dostępności. W szczególności przedmiotem kontroli była ocena zapewnienia:

- współdziałania i współpracy systemu npseo.pl z innymi systemami poprzez właściwą organizację wymiany informacji w postaci elektronicznej oraz proces wspomagania świadczenia usług drogą elektroniczną,
- skutecznego zarządzania bezpieczeństwem informacji dla badanych systemów teleinformatycznych, w tym zapewnienia dostępności, autentyczności, poufności, niezawodności i integralności danych przetwarzanych przez system,
- dostępności treści zawartych na stronach internetowych dla osób z niepełnosprawnościami.

Kontrolowany obszar reguluje ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 j.t.; dalej: Ustawa) oraz rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 j.t.; dalej: rozporządzenie ws. KRI).

Ocena

Na podstawie wyników kontroli pozytywnie oceniono, pomimo stwierdzonych nieprawidłowości, funkcjonowanie systemu npseo.pl pod względem spełniania minimalnych wymagań w zakresie elektronicznej wymiany informacji (interoperacyjności), bezpieczeństwa i dostępności.

1. **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 ws. KRI oraz art. 16 Ustawy.

System npseo.pl powstał w ramach projektu „Program wzmocnienia efektywności nadzoru pedagogicznego i oceny jakości pracy szkoły etap III" realizowanego przez ORE w partnerstwie z Uniwersytetem Jagiellońskim i Erą Ewaluacji Sp. z o.o. Projekt był realizowany w latach 2011–2015 i współfinansowany ze środków UE.

W ramach systemu funkcjonuje ogólnodostępna strona internetowa www.npseo.pl oraz platforma systemu ewaluacji oświaty, dostępna po zalogowaniu się. Możliwość logowania i korzystania z zasobów platformy mają użytkownicy określeni w § 27 rozporządzenia Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie nadzoru pedagogicznego (Dz. U. poz. 1658).

System npseo.pl został zaprojektowany, wdrożony i jest eksploatowany z uwzględnieniem jego funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych standardów i metodyk. Procedura wdrażania systemów teleinformatycznych opisana jest w Polityce Bezpieczeństwa Informacji (PBI) ORE. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa oraz zgodności z PBI oraz Ustawą, w ORE opracowano procedurę, w ramach której Administrator Bezpieczeństwa Informacji (ABI) nadzoruje wdrażanie nowych systemów teleinformatycznych.

Zgodnie z § 16 ust. 1 rozporządzenia ws. KRI, system npseo.pl jest wyposażony w oprogramowanie umożliwiające wymianę danych z innymi systemami. Komunikacja odbywa się poprzez web service - powtarzalne wykonywanie przez system z góry określonych funkcji po otrzymaniu, za pomocą sieci teleinformatycznej, danych uporządkowanych w określonej strukturze. Zgodnie z zaleceniami W3C (World Wide Web Consortium), dane przekazywane są za pomocą protokołu HTTP i z wykorzystaniem XML.

Zgodnie z § 17 i 18 rozporządzenia ws. KRI, kodowanie znaków w dokumentach wysyłanych z systemu, także w odniesieniu do informacji wymienianej przez ten system z innymi systemami, odbywa się według standardu Unicode UTF-8. Połączenia z platformą są szyfrowane (Certyfikat SSL).

Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia ws. KRI ORE zapewnił odpowiedni poziom bezpieczeństwa w systemie npseo.pl poprzez stosowanie wprowadzonych w PBI zapisów o sposobie wdrażania systemów informatycznych. Dostawca usługi dzierżawy serwerów i hostingu zapewnia dzierżawę serwerów dedykowanych wraz z obsługą techniczną w ilościach i parametrach technicznych określonych przez ORE. Zapewniony jest monitoring poprawności działania wskazanych usług sieciowych i zdalna pomoc techniczna oraz monitoring obciążenia serwera - CPU, RAM, NIC, HDD. Dane aktualizowane są co 10 minut. Wykonawca zapewnia bezwarunkowe bezpieczeństwo danych Zamawiającego przechowywanych na serwerach Wykonawcy. Co dwadzieścia cztery godziny wykonywany jest automatyczny backup danych z wszystkich serwerów i baz danych MySQL i PostgreSQL, w sposób nie utrudniający korzystanie z serwisu. Prawidłowy przebieg procesu jest monitorowany przez Administratora Wykonawcy.

Usługi w ramach systemu npseo.pl dostarczane są na deklarowanym poziomie dostępności i odbywają się w oparciu o udokumentowane procedury, zgodnie z § 15 ust. 2 rozporządzenia ws. KRI.

Regulamin organizacyjny ORE zapewnia zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

Stwierdzone nieprawidłowości:

W ORE nie odnotowywano i nie przechowywano w dziennikach systemu części działań użytkowników. Zgodnie z § 21 ust. 2-4 rozporządzenia ws. KRI wymagane jest odnotowywanie i przechowywanie w dziennikach systemu działań użytkowników lub obiektów systemowych polegających na dostępie do systemu z uprawnieniami administracyjnymi, konfiguracji systemu, w tym konfiguracji zabezpieczeń oraz przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Ocena cząstkowa badanego obszaru: pozytywna z nieprawidłowościami.

2. Bezpieczeństwo informacji - system zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

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

, W ORE opracowano, ustanowiono i wdrożono, zgodnie z § 20 ust. 1 i 2 rozporządzenia ws. KRI, System Zarządzania Bezpieczeństwem Informacji (SZBI). SZBI został wprowadzony Zarządzeniem nr 4 Dyrektora ORE z dnia 01.09.2016 r. *w sprawie wprowadzenia w Ośrodku Rozwoju Edukacji w Warszawie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.*

Na wprowadzoną dokumentację SZBI składają się następujące dokumenty:

1) Polityka Bezpieczeństwa Informacji (PBI);
2) Instrukcja Zarządzania Systemami Informatycznymi,
3) Instrukcja Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych.

Funkcjonujący w ORE SZBI jest monitorowany, poddawany przeglądom i doskonalony. Regulacje SZBI są analizowane i aktualizowane. W kontrolowanym okresie czterokrotnie dokonano następujących aktualizacji ww. Zarządzenia nr 4:

- nr 7/2018 z dnia 30.05.2018 r. - aktualizacja dotyczyła wprowadzenia zmian w *Zasadach przetwarzania danych osobowych i korzystania z systemów teleinformatycznych* polegających na doprecyzowaniu zasad niszczenia i likwidacji zbędnej dokumentacji oraz wprowadzeniu zakazu korzystania ze służbowej poczty elektronicznej za pośrednictwem urządzeń prywatnych;
- nr 11/2018 z dnia 18.06.2018 r. - aktualizacja dotyczyła wprowadzenia zasad minimalnych wymagań zabezpieczenia komputerów dla pracowników wykonujących swoje obowiązki poza siedzibą ORE;

- nr 13/2018 z dnia 7.08.2018 r. - aktualizacja dotyczyła wprowadzenia wzoru oświadczenia o wyrażeniu zgody na używanie prywatnego sprzętu teleinformatycznego do celów służbowych oraz o obowiązku zachowania poufności danych osobowych w ORE;
- nr 14/2018 z dnia 6.09.2018 r. – aktualizacja wprowadziła wzór skierowania na szkolenie wstępne dotyczące bezpieczeństwa przetwarzania i ochrony danych osobowych nowych pracowników ORE.

W dniu 15 maja 2018 r. przygotowano sprawozdanie z przeglądu systemów informatycznych pod względem zgodności przetwarzania danych osobowych z przepisami RODO[3]. Sprawozdanie wykazało, że sposób przetwarzania danych w ORE, zarówno w systemach teleinformatycznych, jak i w innych obszarach, nie jest w pełni zgodny z RODO. W związku z powyższym rozpoczęto prace mające na celu wprowadzenie nowej dokumentacji SZBI, która byłaby zgodna z obowiązującymi przepisami. ORE wyjaśnił, że do dnia zakończenia kontroli MEN dokumentacja była przygotowywana do wdrożenia.

ORE przeprowadza okresową analizę ryzyka utraty integralności, dostępności lub poufności oraz podejmuje działania minimalizujące to ryzyko. Analiza została przedstawiona w dokumencie „Raport: Podsumowanie wyników identyfikacji i analizy ryzyk zagrażających realizacji celów i zadań ORE w 2017 r." z dnia 7 marca 2017 r. Raport został przygotowany na podstawie dokumentu pn. „Instrukcja zarządzania ryzykiem w ORE" wprowadzonego zarządzeniem nr 2/2015 (§ 2 ust. 6) Dyrektora ORE z dnia 30 stycznia 2015 r. W roku 2018 przygotowano „Rejestr celów i ryzyka na rok 2018".

W ORE systematycznie dokonuje się inwentaryzacji sprzętu służącego do przetwarzania informacji. Coroczna inwentaryzacja przeprowadzana jest na podstawie Zarządzenie nr 18/2018 Dyrektora ORE w Warszawie z dnia 4 października 2018 r. w sprawie wprowadzenia instrukcji inwentaryzacyjnej w ORE. Wykaz sprzętu zawiera modele urządzeń, jednakże bez ich szczegółowej konfiguracji, co jest wymagane przepisami § 20 ust. 2 pkt 2 rozporządzenia ws. KRI.

Osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w nim w stopniu adekwatnym do realizowanych zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji (§ 20 ust. 2 pkt 4 rozporządzenia ws. KRI). Sposób nadawania i odbierania uprawnień oraz upoważnień do przetwarzania danych osobowych został wprowadzony Zarządzeniem nr 7/2018 Dyrektora ORE z dnia 30.05.2018 r. Zarówno dostęp do systemów teleinformatycznych, jak i upoważnienia do przetwarzania danych są nadawane i odbierane na podstawie pisemnych wniosków bezpośrednich przełożonych pracowników. Wnioski są sprawdzane i akceptowane przez inspektora ochrony danych osobowych (IOD) a następnie

---

[3] Rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE.L Nr 119, str. 1).

przekazywane właściwemu administratorowi systemu, który nadaje uprawnienia i archiwizuje wnioski. Nowo wydane upoważnienia są na bieżąco wpisywane do ewidencji upoważnień. W ORE stosowana jest zasada minimalizacji uprawnień użytkowników w systemach informatycznych, a co najmniej raz w roku przeprowadzana jest weryfikacja kont domenowych i pocztowych pod kątem aktualności upoważnień.

Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia ws. KRI dotyczącym zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, szkolenia z tego zakresu zrealizowano w 2018 r. (w dniach 18-24 maja oraz 13 września). Zgodnie z wyjaśnieniami ORE, w roku 2017 szkolenia takie nie były przeprowadzane. W PBI zawarto również zapis o obowiązku zapoznania się z PBI przez pracowników ORE.

W Zarządzeniu nr 13/2018 Dyrektora ORE w Warszawie z dnia 7.08.2018 r. ustanowiono podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

Zasady współpracy z podmiotami zewnętrznymi zostały opisane w PBI. Treść klauzul informacyjnych zamieszczanych w umowach i innych dokumentach jest każdorazowo weryfikowana przez IOD. Umowy serwisowe podpisane ze stronami trzecimi zawierają zapisy gwarantujące bezpieczeństwo informacji, zgodnie ze stanem prawnym obowiązującym w dniu podpisania umów.

PBI określa sposób postępowania z incydentami naruszenia bezpieczeństwa. Incydenty są zgłaszane zarówno do IOD, jak i do Zespołu Technologii Informacyjno-Komunikacyjnych. W przypadku stwierdzenia naruszenia, prowadzone jest sprawdzenie doraźne mające na celu ustalenie przyczyn zdarzenia. Następnie, w sprawozdaniu ze sprawdzenia, zamieszcza się ustalenia i zalecenia oraz harmonogram działań naprawczych.

W ORE zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Informacje są zabezpieczone w sposób uniemożliwiający osobom nieuprawnionym ich ujawnienie, modyfikacje, usunięcie lub zniszczenie.

W ORE funkcjonuje system kontroli dostępu oraz monitoring. Kamery obejmują korytarze wewnętrzne oraz teren wokół budynków. Obraz z kamer monitorowany jest na bieżąco przez strażników ochrony mienia. Pomieszczenia wyposażono w zamykane szafy, klucze do pomieszczeń przechowywane są pod kontrolą portiera i wydawane wyłącznie pracownikom właściwych komórek organizacyjnych lub osobom upoważnionym zgodnie z zakresem obowiązków.

Załącznik nr 2 do Zarządzenia nr 4 Dyrektora ORE z dnia 01.09.2016 r. reguluje działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji.

Ocena cząstkowa badanego obszaru: pozytywna.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych.

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 niepełnosprawne. Obecna wersja dokumentu WCAG (2.0) została opublikowana w roku 2008. Wymogi określone w ww. dokumencie zostały wprowadzone do obowiązującego prawa i zapisane w § 19 i załączniku 4 do rozporządzenia ws. KRI.

Strona internetowa npseo.pl udostępnia oprogramowanie asystujące odczytujące zawartość strony, strona zapewnia również wersję kontrastową i możliwość powiększenia czcionki.

W odniesieniu do platformy ewaluacji systemu oświaty, takie możliwości dostępne są jedynie w sekcji logowania. Zasadnicza zawartość platformy: arkusze kontroli, ewaluacji i monitorowania nie spełniają wymagań WCAG 2.0.

ORE wyjaśnił, że założenia budowy platformy powstały przed wejściem w życie ww. rozporządzenia ws. KRI.

Stwierdzone nieprawidłowości:

Zalecenia dotyczące tworzenia dostępnych serwisów internetowych, tj. web content accessability guidelines (WCAG 2.0), nie funkcjonują w pełnym wymiarze w systemie npseo.pl.

Ocena cząstkowa badanego obszaru: pozytywna z nieprawidłowościami.

Na podstawie art. 46 ust. 3 pkt 1 ustawy o kontroli w administracji rządowej, w związku ze stwierdzonymi w toku kontroli nieprawidłowościami, przedstawiam następujące zalecenia:

1. W dziennikach systemu npseo.pl, zgodnie z § 21 ust. 2-4 rozporządzenia ws. KRI należy odnotowywać i przechowywać działania użytkowników lub obiektów systemowych polegających na dostępie do systemu z uprawnieniami administracyjnymi, konfiguracji systemu, w tym konfiguracji zabezpieczeń oraz przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
2. Należy doprowadzić do pełnego wprowadzenia i stosowania zaleceń dotyczących tworzenia dostępnych serwisów internetowych (WCAG 2.0) w systemie npseo.pl.

Na podstawie art. 49 ustawy o kontroli w administracji rządowej, proszę o przekazanie w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, informacji o sposobie wykonania zaleceń.

Od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach.

Z upoważnienia Ministra Edukacji Narodowej

Sławomir Adamiec
Dyrektor Generalny