Minister
Edukacji i Nauki

Przemysław Czarnek

DKO-WKiDN.0915.1.2022
Warszawa, 21 grudnia 2022 r.

Pan
p.o. Dyrektor Tomasz Madej
Ośrodek Rozwoju Edukacji
Al. Ujazdowskie 28
00-478 Warszawa

WYSTĄPIENIE POKONTROLNE

Zgodnie z art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224), przekazuję niniejsze Wystąpienie pokontrolne.

Na podstawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224), 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 2021 r. poz. 2070 j.t.), Ministerstwo Edukacji i Nauki[1] (dalej: MEiN) w terminie od 31 maja 2022 r. do 16 września 2022 r. przeprowadziło w Ośrodku Rozwoju Edukacji (dalej: ORE), z siedzibą w Warszawie w Alejach Ujazdowskich 28[2], kontrolę pn. *Działanie i bezpieczeństwo wybranych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych*.

Celem kontroli było dokonanie oceny zapewnienia bezpieczeństwa teleinformatycznego systemów teleinformatycznych działających w ORE, w szczególności:

1) współdziałania systemów teleinformatycznych – poprzez właściwą organizację wymiany informacji w postaci elektronicznej, współpracę z innymi systemami informatycznymi - oraz procesów wspomagania świadczenia usług drogą elektroniczną;
2) skutecznego zarządzania bezpieczeństwem informacji dla badanych systemów teleinformatycznych, w tym zapewnienia dostępności, autentyczności, poufności, niezawodności i integralności danych przetwarzanych przez system;

[1] Kontrolę przeprowadzili pracownicy Ministerstwa Edukacji i Nauki:
1) Bożena Koniorczyk, radca w Wydziale Kształcenia i Doskonalenia Nauczycieli w Departamencie Kształcenia Ogólnego i Podstaw Programowych, na podstawie upoważnień nr 10/2022 z dnia 30 maja 2022 r. i nr 22/2022 z dnia 22 sierpnia 2022 r.;
2) Alicja Jakubiak-Kępińska, główny specjalista w Wydziale Kontroli dla Działu Oświata i Wychowanie w Departamencie Kontroli i Audytu, na podstawie upoważnienia nr 11/2022 z dnia 30 maja 2022 r. i r 23/2022 z dnia 1 sierpnia 2022 r.;
3) Natalia Piętak, główny specjalista w Wydziale Bezpieczeństwa w Biurze Dyrektora Generalnego, na podstawie upoważnienia nr 12/2022 z dnia 30 maja 2022 r. i nr 24/2022 z dnia 1 sierpnia 2022 r.

[2] ORE prowadzi działalność pod następującymi adresami:
- Al. Ujazdowskie 28, 00-478 Warszawa,
- ul. Polna 46A, 00-644 Warszawa,
- ul. Paderewskiego 77, 05-070 Sulejówek.

3) dostępności treści zawartych na stronach internetowych dla osób z niepełnosprawnościami

oraz sprawdzenie czy regulacje wewnętrzne dotyczące badanych systemów teleinformatycznych wykorzystywanych przez ORE do realizacji zadań publicznych zawierają odpowiednie uregulowania, dzięki którym systemy teleinformatyczne spełniają minimalne wymagania w zakresie elektronicznej wymiany informacji (interoperacyjności) oraz bezpieczeństwa i dostępności informacji.

Kontrolą objęto okres od 1 stycznia 2021 r. do 31 maja 2022 r., tj. do dnia rozpoczęcia kontroli.

ORE jest publiczną placówką doskonalenia nauczycieli o zasięgu ogólnokrajowym, prowadzoną przez Ministra Edukacji i Nauki na podstawie art. 8 ust. 5 pkt 1 lit. b ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe. Zasady działania placówki określają przepisy ww. ustawy oraz rozporządzenia Ministra Edukacji Narodowej z dnia 28 maja 2019 r. w sprawie placówek doskonalenia nauczycieli (Dz.U. z 2019 r. poz. 1045) i rozporządzenia z dnia 27 sierpnia 2021 r. zmieniającego rozporządzenie w sprawie placówek doskonalenia nauczycieli (Dz.U. z 2021 r. poz. 1601 j.t.).

W myśl przepisów § 2 ust. 2 i 3 pkt 1 ww. rozporządzenia w sprawie placówek doskonalenia nauczycieli Ośrodek Rozwoju Edukacji działa na podstawie statutu, który jest nadawany placówce przez organ prowadzący, tj. ministra właściwego do spraw oświaty i wychowania. ORE funkcjonuje na podstawie statutu nadanego przez Ministra Edukacji Narodowej zarządzeniem Nr 39 z dnia 29 lipca 2016 r. w sprawie nadania statutu Ośrodkowi Rozwoju Edukacji w Warszawie (Dz. Urz. MEN poz. 37).

W statucie Ośrodka Rozwoju Edukacji określono zadania obowiązkowe, wynikające z § 13 ust. 1 ww. rozporządzenia w sprawie placówek doskonalenia nauczycieli oraz z:

- art. 60 ust. 5 ustawy – Prawo oświatowe, zgodnie z którym minister właściwy do spraw oświaty i wychowania może powierzyć prowadzonej przez siebie placówce doskonalenia nauczycieli o zasięgu ogólnokrajowym wykonywanie zadań, o których mowa w art. 60 ust. 1 pkt 3 i ust. 2 ww. ustawy, tj. zadań związanych z zapewnieniem sprawności i efektywności nadzoru pedagogicznego oraz prowadzeniem elektronicznej platformy nadzoru pedagogicznego;
- art. 183 ust. 2 ustawy – Prawo oświatowe, w myśl którego do zadań placówki doskonalenia, o której mowa w art. 8 ust. 5 pkt 1 lit. b, należy podejmowanie działań na rzecz doskonalenia systemu oświaty, zgodnie z polityką oświatową państwa, w zakresie określonym w statucie tej placówki;
- art. 183 ust. 3 ustawy – Prawo oświatowe, w myśl którego minister prowadzący placówkę doskonalenia, o której mowa w art. 8 ust. 5 pkt 1 lit. b, może powierzać tej placówce wykonywanie zadań związanych z podnoszeniem jakości edukacji, zapewniając środki na ich realizację;
- art. 9g ust. 11a pkt 3 ustawy z dnia 26 stycznia 1982 r. Karta Nauczyciela (Dz.U. z 2021 r. poz. 1762 j.t.), zgodnie z którym publiczna placówka doskonalenia nauczycieli, o której mowa w art. 8 ust. 5 pkt 1 lit. b ustawy - Prawo oświatowe (tj. prowadzona przez Ministra Edukacji i Nauki) organizuje szkolenie dla kandydatów na ekspertów komisji egzaminacyjnej lub kwalifikacyjnej dla nauczycieli ubiegających się o awans na stopień nauczyciela mianowanego lub dyplomowanego.

Kontrolowany obszar reguluje:

- ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[3] (dalej: ustawa o informatyzacji);
- 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[4] (dalej: rozporządzenie KRI);
- rozporządzenie z dnia 14 września 2011 r. Prezesa Rady Ministrów w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[5] (dalej: rozporządzenie w sprawie sporządzania i doręczania dokumentów elektronicznych);
- ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych[6] (dalej: ustawa o dostępności cyfrowej).

Zgodnie ze statutem Informatycznego Centrum Edukacji i Nauki[7] (dalej: ICEiN) przedmiotem działalności Centrum jest m.in. obsługa informatyczna Ośrodka Rozwoju Edukacji.

Do kontroli zostały wybrane nw. systemy, za pomocą których realizowane są powyższe zadania wynikające z przepisów ustawowych:

1) Platforma systemu ewaluacji oświaty dostępna pod adresami: np.gov.pl (https://seo2.npseo.pl/) i badania.np.gov.pl (https://badania.np.gov.pl/);
2) Szkolenie kandydatów na ekspertów, strona: ekspert.ore.edu.pl (https://ekspert.ore.edu.pl/);
3) Biuletyn Informacji Publicznej ORE, działający pod adresem: bip.ore.edu.pl (https://bip.ore.edu.pl/).

Ocena ogólna kontrolowanej działalności.

Na podstawie wyników kontroli pozytywnie, pomimo stwierdzonych nieprawidłowości, oceniono obszar objęty kontrolą. Nieprawidłowości dotyczyły niespełniania wybranych wymogów dotyczących: interoperacyjności systemów teleinformatycznych, zarządzania bezpieczeństwem informacji oraz publikacji deklaracji dostępności stron internetowych określonej w ustawie o dostępności cyfrowej.

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:

1) art. 16 ust. 1a i art. 19b ust. 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne;
2) § 3 ust. 1 pkt 1, 2, 4, 5 rozporządzenia z dnia 14 września 2011 r. Prezesa Rady Ministrów w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych w związku z art. 3 oraz art. 19b ust. 3 ustawy o informatyzacji;
3) § 5, §15-18, §20-21 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów

[3] Dz.U. z 2021 r. poz. 670 z późn. zm.;

[4] t.j. Dz.U. z 2017 r. poz. 2247;
[5] Dz.U z 2018 r. poz. 180;
[6] Dz.U. z 2019 r. poz. 848;
[7] Statut ICEiN został wprowadzony zarządzeniem Ministra Edukacji i Nauki z dnia 31 stycznia 2022 r. w sprawie zmiany nazwy Centrum Informatycznego Edukacji i nadania statutu Informatycznemu Centrum Edukacji i Nauki (Dz. Urz. MEiN z 2022 r. poz. 10).

publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Interoperacyjność realizowana na podstawie ustawy o informatyzacji oraz rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych.

- Zgodnie z art. 16 ust. 1a ustawy o informatyzacji - *podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę*.

  Ośrodek Rozwoju Edukacji udostępnia elektroniczną skrzynkę podawczą (dalej: ESP), spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji oraz zapewnia jej obsługę. Informacja o udostępnieniu skrzynki ePUAP oraz jej adres znajdują się na stronie: https://www.ore.edu.pl/2017/12/kontakt-ore/ oraz https://bip.ore.edu.pl/265-2/.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 3 ust. 1 pkt 1 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych - *podmioty publiczne informują na swoich stronach podmiotowych Biuletynu Informacji Publicznej, zwanego dalej „BIP", o udostępnionym adresie elektronicznej skrzynki podawczej, podanym w formie identyfikatora URI.*

  Zgodnie z ww. przepisem adres ESP (/ORE_epuap/SkrytkaESP) w Biuletynie Informacji Publicznej Ośrodka Rozwoju Edukacji (dalej: BIP ORE) jest podany w formie identyfikatora URI (Uniform Resource Identifier, tłum. Ujednolicony Identyfikator Zasobów).

  Zdaniem kontrolujących podanie adresu elektronicznej skrzynki podawczej w formie identyfikatora URI, także na stronie internetowej ORE mogłoby spowodować, że strona będzie bardziej intuicyjna w użytkowaniu.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 3 ust. 1 pkt 2 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych - *podmioty publiczne informują na swoich stronach podmiotowych Biuletynu Informacji Publicznej, zwanego dalej „BIP" o maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż 5 megabajtów*.

  W Biuletynie Informacji Publicznej Ośrodka Rozwoju Edukacji pod adresem: https://bip.ore.edu.pl/177/ ORE zamieściło informacje o maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w MB, możliwym do doręczenia za pomocą ESP, nie mniejszym niż 5 MB.

  W trakcie kontroli ustalono, że na stronie BIP ORE pierwotnie znajdował się zapis określający maksymalny rozmiar dokumentu elektronicznego wraz z załącznikami możliwy do doręczenia za pomocą elektronicznej skrzynki podawczej, nieprzekraczający 5 MB. Informacja w tym zakresie została przez ORE poprawiona i zastąpiona brzmieniem: „*maksymalny rozmiar dokumentu elektronicznego wraz z załącznikami możliwy do doręczenia za pomocą elektronicznej skrzynki podawczej nie może przekraczać 500 MB*". Zgodnie z wyjaśnieniami Wicedyrektora ORE, wcześniejszy zapis wynikał z *poprzednich regulacji dot. skrzynki ePUAP. Obecnie wpis na stronie BIP w zakładce Elektroniczna Skrzynka Podawcza został zaktualizowany zgodnie z informacją udostępnioną na stronie*: https://epuap.gov.pl/wps/wcm/connecVepuap2lpllaktualnosciIduze%o2}pliki%2\nowa%2OfunkcjonaInosco/o20nao/oZ}epuap2?Idmy%A4t=true.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z art. 19b ust. 3 ustawy o informatyzacji - *organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich kwalifikowanym podpisem elektronicznym*.

  Ośrodek Rozwoju Edukacji udostępnia w BIP wzór pisma ogólnego do podmiotu publicznego pod adresem: https://epuap.gov.pl/wps/portal/strefa-klienta/katalog-spraw/opis-uslugi/pismo-ogolne-do-podmiotu-publicznego/ORE_epuap oraz zamieszcza na stronie BIP ORE w zakładce „Elektroniczna skrzynka podawcza" link zewnętrzny pn. „Formularz pisma ogólnego" odsyłający do powyższej strony.

  W badanym zakresie nie stwierdzono nieprawidłowości.

Interoperacyjność realizowana na podstawie rozporządzenia KRI.

- Zgodnie z § 5 ust. 2 pkt 1 rozporządzenia KRI – *interoperacyjność na poziomie organizacyjnym osiągana jest przez informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty*.

  Na stronie internetowej ORE pod adresem https://www.ore.edu.pl/, znajduje się *Platforma Systemu Ewaluacji Oświaty* (w zakładce „ORE" → „Wydziały" → „Wydział Nadzoru Pedagogicznego"). Na stronie nie zamieszczono informacji o sposobie dostępu oraz zakresie użytkowym tego serwisu (np.: cel stosowania systemu, wskazanie jego głównych funkcji, zakresu przedmiotowego i podmiotowego stosowania, instrukcje, materiały informacyjne).
  W złożonych wyjaśnieniach wicedyrektor ORE potwierdził brak informacji na temat *Platformy Systemu Ewaluacji Oświaty* na stronie internetowej ORE. Poinformował, że *podstawowe informacje na temat platformy i zakresu gromadzonych danych oraz zasady uzyskiwania dostępu do platformy określa rozporządzenie Ministra Edukacji i Nauki z dnia 1 września 2021 r. zmieniające rozporządzenie w sprawie nadzoru pedagogicznego*[8].

  Wobec przepisu § 5 ust. 2 pkt 1 rozporządzenia KRI stwierdzono, że sposób dostępu oraz zakres użytkowy *Platformy Systemu Ewaluacji Oświaty* nie został przedstawiony w sposób umożliwiający skuteczne zapoznanie się z systemem.

  Na stronie ORE zamieszczony jest także dostęp do systemu *Szkolenie kandydatów na ekspertów* (w zakładce „Nasze serwisy"), gdzie znajdują się informacje umożliwiające skuteczne zapoznanie się z usługami realizowanymi na tym portalu, m.in. takie informacje jak: informacje ogólne nt. szkolenia, organizacja szkolenia, zasady rekrutacji, aktualności gdzie znajdują się szczegółowe informacje dotyczące kolejnych edycji szkolenia, baza osób oczekujących na szkolenie, instrukcja w zakresie logowania się w bazie osób oczekujących na szkolenie, akty prawne, materiały do pobrania.

  W zakładce BIP są udostępnione aktualne informacje publiczne ORE m.in.: status prawny, informacje o zamówieniach publicznych, kontroli zarządczej, aktualnie realizowanych i zakończonych projektach unijnych.

- Zgodnie z § 5 ust. 2 pkt 4 rozporządzenia KRI - *interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną*.

[8] Dz.U. 2021 poz. 1618.

Na podstawie § 3 ust. 1 pkt. 4-5 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych, *podmioty publiczne informują na swoich stronach podmiotowych BIP, o:*
- *rodzajach informatycznych nośników danych, na których może zostać im doręczony dokument elektroniczny;*
- *rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru.*

Na stronie BIP ORE w opublikowanych opisach procedur obowiązujących przy załatwianiu spraw drogą elektroniczną, z zakresu właściwości ORE, nie zamieszczono ww. informacji o rodzajach informatycznych nośników danych, na których może zostać:
- doręczony ORE dokument elektroniczny,
- zapisane urzędowe poświadczenie odbioru.

Wicedyrektor ORE w złożonych wyjaśnieniach poinformował, że ww. informacja zostanie uzupełniona w BIP ORE w zakładce Elektroniczna Skrzynka Podawcza.

- Zgodnie z § 5 ust. 3 pkt 3 rozporządzenia KRI - *interoperacyjność na poziomie semantycznym osiągana jest przez stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.*
  Zgodnie z § 16 ust. 1 rozporządzenia KRI - *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*

  Wicedyrektor ORE poinformował, że s*ystemy: Platforma SEO, Szkolenie kandydatów na ekspertów, BIP ORE nie współpracują z innymi systemami zewnętrznymi, które pozwalają na wymianę informacji.*

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 15 rozporządzenia KRI:
  ust. 1 - systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk;
  ust. 2 - zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczenie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

  Platforma Systemu Ewaluacji Oświaty to system, który powstał w ramach *Programu Operacyjnego Kapitał Ludzki na lata 2007-2013, Działania 3.1.2 Modernizacja systemu nadzoru pedagogicznego*. Platforma *Systemu Ewaluacji Oświaty* została uruchomiana w 2011 r. w celu prowadzenia czynności nadzoru pedagogicznego, przetwarzania i analizy zebranych danych. W rozporządzeniu Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. *w sprawie nadzoru pedagogicznego*[9] określono:

[9] Dz.U. z 2020 r. poz. 1551;

- zakres danych gromadzonych na elektronicznej platformie nadzoru pedagogicznego (§ 27[10]),
- sposób i zakres dostępu do elektronicznej platformy nadzoru pedagogicznego osób realizujących zadania w zakresie nadzoru pedagogicznego, nauczycieli, uczniów, rodziców i przedstawicieli organów prowadzących szkoły lub placówki (§ 28[11]).

Zgodnie z wyjaśnieniami ORE *Platforma Systemu Ewaluacji Oświaty udostępnia narzędzia nadzoru pedagogicznego wizytatorom i dyrektorom szkół/placówek. Pozwala na prowadzenie kontroli planowych, badanie kształcenia u uczniów kompetencji kluczowych oraz przetwarzanie zebranych danych*.

Do platformy mają dostęp (zarejestrowani w systemie) pracownicy organów nadzoru pedagogicznego, przedstawiciele organów prowadzących szkoły/placówki oraz dyrektorzy szkół/placówek. Według stanu na dzień 12.09.2022 r. w systemie zarejestrowanych jest 46 368 użytkowników.

ORE poinformowało, że w okresie objętym kontrolą w ORE obowiązywały umowy[12] na świadczenie usługi pn.: „*Wsparcie techniczne i administrowanie platformą internetową Systemu Ewaluacji Oświaty*". Objęta kontrolą umowa nr ICEiN-8/2022 na świadczenie usługi wsparcia technicznego i administrowania platformą internetową *Systemu Ewaluacji Oświaty,* zawierała zapisy spełniające wymogi określone w §15 ust. 2 KRI. W umowie

[10] § 27 1. Użytkownikami platformy mogą być osoby, o których mowa w § 26 ust. 1 pkt 1, 4 i 5 .
2. Osobiste konto użytkownika jest tworzone przez ministra właściwego do spraw oświaty i wychowania po otrzymaniu od podmiotów, o których mowa w § 26 ust. 1 pkt 1, 4 i 5, następujących informacji dotyczących osoby, która ma być użytkownikiem platformy:
   1) imię i nazwisko;
   2) zajmowane stanowisko;
   3) zakres zadań realizowanych z wykorzystaniem platformy;
   4) służbowy adres poczty elektronicznej.
3. Użytkownik otrzymuje identyfikator (login) i hasło dostępu do platformy. Identyfikator (login) i hasło dostępu mogą być używane wyłącznie przez użytkownika, któremu zostały nadane.
4. Użytkownik może w każdym czasie dokonać zmiany hasła dostępu.
5. Użytkownik uzyskuje dostęp do platformy przez zalogowanie się z użyciem identyfikatora (loginu) oraz hasła dostępu.
6. Identyfikacja użytkownika jest dokonywana automatycznie przez mechanizmy platformy podczas logowania z użyciem identyfikatora (loginu) oraz hasła dostępu.
7. Osobiste konto użytkownika jest likwidowane przez ministra właściwego do spraw oświaty i wychowania, po przekazaniu przez podmioty, o których mowa w § 26 ust. 1 pkt 1, 4 i 5, wniosku o likwidację osobistego konta użytkownika zawierającego informacje, o których mowa w ust. 2 pkt 1, 2 i 4.

[11] § 28 1. Osobom, o których mowa w § 26 ust. 1 pkt 2, umożliwia się dostęp do platformy:
   1) na terenie szkoły lub placówki - przez odblokowanie dostępu do narzędzi nadzoru pedagogicznego przypisanych do danej kontroli;
   2) poza terenem szkoły lub placówki - przez udostępnienie kodu PIN, za pomocą którego osoby te uzyskują dostęp do narzędzi nadzoru pedagogicznego przypisanych do danej kontroli; kod PIN składa się z co najmniej 4 znaków i jest udostępniany na czas prowadzenia danej kontroli.
2. Odblokowania dostępu, o którym mowa w ust. 1 pkt 1, oraz udostępnienia kodu PIN, o którym mowa w ust. 1 pkt 2, dokonuje pracownik, o którym mowa w § 26 ust. 1 pkt 1, wykonujący zadania w zakresie nadzoru pedagogicznego.

[12] Umowa nr 703/WNP/2020 z 30 grudnia 2020 r., umowa nr 14/ZUZP/2021 z 1 lutego 2021 r., umowa nr 972/WNP/2021 z 22 grudnia 2021 r., umowa nr 14/WNP/2022 z 26 stycznia 2022 r., umowa nr ICEiN-8/2022 z 1 marca 2022 r.

określono m.in. wymagania SLA[13] w zakresie rozwiązywania problemów technicznych związanych z prawidłowym działaniem Platformy, w tym w określonych w umowie terminach do usunięcia błędów krytycznych i niekrytycznych oraz sposobu liczenia tych terminów a w przypadku zwłoki z usunięciem wskazanego błędu określono prawo do naliczenia kar umownych. Administratorem technicznym systemu jest firma zewnętrzna, która dokonuje aktualizacji danych.

Zgodnie z informacjami przedstawionymi przez ORE, planowane jest wprowadzenie nowego systemu: *Nowa Platforma Nadzoru Pedagogicznego* (dalej: NPNP). W tym celu zlecono przeprowadzeniu analizy biznesowej oraz przygotowanie dokumentacji opisującej założenia *Nowej Platformy*. Dokument ten powstał w celu opisania koncepcji systemu oraz zebrania wymagań biznesowych. Został skierowany do programistów, testerów oraz zespołu powołanego do prac nad określaniem wymagań dla NPNP, biorących udział w procesie wytwarzania oprogramowania. Zgodnie z założeniami, nowy system ma spełniać wymogi określone w:

- rozporządzeniu MEN z dnia 25 sierpnia 2017 r. *w sprawie nadzoru pedagogicznego*,
- ustawie z dnia 15 kwietnia 2011 r. *o systemie informacji oświatowej*,
- ustawie z dnia 14 grudnia 2016 r. *Prawo oświatowe*,
- rozporządzenia MEN z dnia 11 sierpnia 2017 r. *w sprawie wymagań wobec szkół i placówek*,
- ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych*,
- rozporządzeniu KRI (w zakresie rozdziału III – Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz rozdziału IV – Minimalne wymagania dla systemów teleinformatycznych),
- ustawie z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (w zakresie określonym w art. 173 ustawy).

Szkolenie kandydatów na ekspertów jest systemem o zasięgu krajowym, który został uruchomiony w 2012 r. w celu wspomagania rekrutacji i szkolenia kandydatów na ekspertów do spraw awansu zawodowego nauczycieli. W systemie tym gromadzone są informacje o kandydatach na ekspertów, takie jak imię i nazwisko, adres zamieszkania, adres email, telefon oraz informacje o specjalizacji zawodowej. Szkolenie kandydatów na ekspertów to szkolenie organizowane rokrocznie przez Wydział Innowacji i Rozwoju ORE w ramach Programu Ekspert. Od 2020 r. organizowane są dwie edycje szkolenia rocznie. Szkolenie składa się z dwóch części. Każda zakończona jest egzaminem testowym. Pierwsza część to kształcenie na odległość (e-learning), druga część to zajęcia w formie bezpośredniej. Szkolenia realizowane są zgodnie z *Ramowym programem szkolenia kandydatów na ekspertów*, stanowiącym załącznik do rozporządzenia Ministra Edukacji Narodowej[14] i obejmują następujące treści programowe:

- Rola eksperta,
- Prawo w pracy eksperta,

[13] Service Level Agreement (SLA) – to umowa pomiędzy dostawcą usług informatycznych a odbiorcą. Umowa SLA opisuje usługę informatyczną, dokumentuje docelowy poziom świadczenia usługi, określa obowiązki dostawcy usług informatycznych i odbiorcy. Pojedyncza umowa SLA może dotyczyć wielu usług informatycznych lub wielu klientów – na podstawie definicji zawartej w Polskim Glosariuszu ITIL wraz ze skrótami – wersja 1.0 z dnia 15 grudnia 2011 r., opartym na angielskim glosariuszu, wersja 1.0 z dnia 29 lipca 2011 r., pobranym ze strony internetowej: www.itil-officialsite.com/internationalActivities/TranslatedGlossaries.aspxService

[14] Rozporządzenie Ministra Edukacji Narodowej z dnia 1 marca 2013 r. w sprawie ramowego programu szkolenia kandydatów na ekspertów wchodzących w skład komisji egzaminacyjnych i kwalifikacyjnych dla nauczycieli ubiegających się o awans na stopień zawodowy, sposobu prowadzenia listy ekspertów oraz trybu wpisywania i skreślania ekspertów z listy (Dz.U. z 2020 r. poz. 1453).

- Zespołowy charakter pracy eksperta,
- Egzamin i rozmowa przeprowadzone przez komisję egzaminacyjną i kwalifikacyjną,
- Ocenianie dorobku zawodowego nauczyciela,
- Warsztat pracy eksperta,
- Etyczne aspekty pracy eksperta.

Z systemu korzystają użytkownicy wewnętrzni (administratorzy i osoby szkolące) oraz użytkownicy zewnętrzni (kandydaci na ekspertów) – łącznie 5 063 osoby (stan na dzień 14.09.2022 r.). W okresie objętym kontrolą zostały zorganizowane cztery 60-godzinne szkolenia. Zgodnie z informacjami otrzymanymi z ORE, w części e-learningowej w kontrolowanym okresie uczestniczyło i ukończyło ją 326 osób (tj. zdało egzamin). Do drugiej części szkolenia przystąpiło i ukończyło ją 290 osób, (na podstawie udostępnionych list osób, które ukończyły szkolenie dla kandydatów na ekspertów ds. awansu w latach 2021-2022, tj.142 osoby w roku 2021 i 148 osób w roku 2022). Konta osób, które ukończyły szkolenie są usuwane. Zgodnie z wyjaśnieniami przedstawionymi przez ORE, baza ta jest systematycznie aktualizowana, pod względem liczby użytkowników.

Biuletyn Informacji Publicznej ORE to system, w którym są udostępniane aktualne informacje publiczne ORE, takie jak np. status prawny, dane kontaktowe, informacje o zamówieniach publicznych. Obowiązek utworzenia urzędowego publikatora teleinformatycznego, jakim jest Biuletyn Informacji Publicznej ORE, wynika z przepisów art. 8 ust. 1 i 2[15] ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej* (Dz.U. z 2022 r. poz. 902). ORE jako podmiot, o którym mowa w art. 4 ust. 1 pkt 5[16] tej ustawy, wykonujący zadania publiczne zobowiązany jest do publikowania informacji w Biuletynie Informacji Publicznej. Publikator ten tworzony jest w formie elektronicznej i udostępniany pod adresami witryn internetowych poszczególnych podmiotów. System ten został utworzony w 2007 r. i służy użytkownikom wewnętrznym – administratorom i redaktorom (łącznie: 14 osób) i użytkownikom zewnętrznym – strona jest dostępna publicznie bez logowania.

W umowie nr CIE-36/2019 zawartej 20 grudnia 2019 r. na usługi zapewnienia prywatnej chmury na potrzeby hostingu serwisów internetowych wraz z usługami konfiguracyjnymi i administracyjnymi, dla systemów – *Szkolenie kandydatów na ekspertów* oraz BIP ORE określono m.in. nw. wymagania dotyczące usług hostingowych:

- Wykonawca zagwarantuje dostępność usługi na poziomie nie mniejszym niż 99,9% w okresie 365 dni w roku kalendarzowym. Dopuszczalny czas niedostępności [w godzinach] wynosi 8 godz. 46 min. w roku kalendarzowym;
- w przypadku stwierdzenia obniżenia dostępności hostingu poniżej wymaganego parametru dostępności w skali miesiąca rozliczeniowego wykonawca udzieli zamawiającemu bonifikaty opisanej w umowie dot. usług hostingowych.

Działania związane z monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności, a także działania zapobiegawcze będące

[15] Art. 8 ust. 1. Tworzy się urzędowy publikator teleinformatyczny - Biuletyn Informacji Publicznej – w celu powszechnego udostępniania informacji publicznej, w postaci ujednoliconego systemu stron w sieci teleinformatycznej, zwany dalej „Biuletynem Informacji Publicznej".
2. Informacje publiczne są udostępniane w Biuletynie Informacji Publicznej przez podmioty, o których mowa w art. 4 ust. 1 i 2.

[16] Art. 4 ust. 1 pkt 5. Obowiązane do udostępniania informacji publicznej są władze publiczne oraz inne podmioty wykonujące zadania publiczne, w szczególności podmioty reprezentujące inne osoby lub jednostki organizacyjne, które wykonują zadania publiczne lub dysponują majątkiem publicznym, oraz osoby prawne, w których Skarb Państwa, jednostki samorządu terytorialnego lub samorządu gospodarczego albo zawodowego mają pozycję dominującą w rozumieniu przepisów o ochronie konkurencji i konsumentów.

wynikiem dostrzeżonych problemów podczas monitorowania ich pracy, odbywa się za pomocą narzędzi Zabbix i Vmware, które monitorują środowiska serwerowych w ORE (wyjaśnienia Informatycznego Centrum Edukacji i Nauki).

W ORE ustalone zostały procedury, które określają właściciela merytorycznego usług (komórka organizacyjna podmiotu), odpowiedzialność za utrzymanie usług od strony technicznej, poziom świadczenia usług, monitorowanie poziomu świadczenia usług na zadeklarowanym poziomie.

Zgodnie z *Regulaminem Organizacyjnym* ORE zatwierdzonym 1 grudnia 2016 r.:
- za prowadzenie elektronicznej platformy nadzoru pedagogicznego i administrowania tą platformą odpowiada Wydział Nadzoru Pedagogicznego (dalej: WNP),
- organizowanie szkoleń dla kandydatów na ekspertów komisji kwalifikacyjnych i egzaminacyjnych awansu zawodowego nauczycieli, sposób prowadzenie listy ekspertów oraz tryb wpisywania i skreślania ekspertów z listy należy do zadań Wydziału Innowacji i Rozwoju (dalej: WIR),
- za realizację działań informacyjnych poprzez prowadzenie stron internetowych, intranetu, Biuletynu Informacji Publicznej i obsługę kanałów komunikacji z odbiorcami odpowiada Wydział Upowszechniania Zasobów (dalej: WUZ); do zadań WUZ należy wsparcie informatyczne innych komórek Ośrodka w utrzymaniu platform i portali edukacyjnych.

Zgodnie ze schematem organizacyjnym ORE w skład WUZ wchodzą dwa zespoły:
- Zespół Komunikacji Społecznej (dalej: ZKS) odpowiadający m.in. za prowadzenie serwisów internetowych, intranetu i Biuletynu Informacji Publicznej Ośrodka we współpracy z komórkami organizacyjnymi Ośrodka oraz obsługę innych kanałów promocji i informacji, jak również za redakcję i koordynację informacji zamieszczanych w serwisach internetowych, w BIP i w intranecie.
- Zespół Technologii Informacyjno-Komunikacyjnych (dalej: ZTIK) odpowiadający m.in. za zapewnienie optymalnego funkcjonowania platform oraz za administrowanie i rozbudowę stron internetowych, intranetu i BIP.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 17 ust. 1 rozporządzenia KRI - *kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą*.

  Na podstawie wyjaśnień przekazanych przez ORE ustalono, że kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych objętych kontrolą, odbywa się według standardu Unicode UTF-8.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 18 ust. 1 rozporządzenia KRI - *systemy teleinformatyczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia KRI*.

  Na podstawie przekazanych przez ORE wyjaśnień ustalono, że zasoby informacyjne systemów objętych kontrolą udostępniane są w nw. formatach:
  - *Platforma Systemu Ewaluacji Oświaty* – .pdf (w zakresie przekazywania zbiorczych wyników badania kształcenia u uczniów kompetencji kluczowych), .css (w zakresie interfejsu użytkownika), .html (w zakresie interfejsu użytkownika oraz wersji protokołów kontroli planowych oraz informacji dotyczących kontroli doraźnych

przeznaczonych do przygotowania dokumentacji papierowej w jednostkach odpowiedzialnych za nadzór pedagogiczny), .xlsx (w zakresie raportów);
- *Szkolenie kandydatów na ekspertów* – platforma ta służy do prowadzenia kursów e-learningowych i nie są na niej udostępnianie repozytoria;
- *Biuletyn Informacji Publicznej* ORE – udostępnia dane w formatach: .pdf, .xls, .xlsx, .doc, .docx.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 18 ust 2 rozporządzenia KRI - *jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia*.

  W Biuletynie Informacji Publicznej Ośrodka Rozwoju Edukacji (w zakładce „*Elektroniczna skrzynka podawcza*") ORE zamieściło informację o obowiązujących formatach danych załączników dodawanych do pism (zgodnych z załącznikiem do rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych).

  Zgodnie z wyjaśnieniami uzyskanymi z ORE: „*Platforma systemu ewaluacji oświaty nie pozwala na przesyłanie gotowych dokumentów. Dokumenty zawierające zbiorcze dane generowane są na podstawie informacji wprowadzonych w odpowiednie pola arkuszy zatwierdzonych przez ministra właściwego do spraw oświaty i wychowania. System Szkolenia kandydatów na ekspertów także nie posiada funkcji przyjmowania gotowych dokumentów.*"

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie*.

  W ORE zapewniono zabezpieczenie informacji w sposób uniemożliwiający osobie nieuprawnionej jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. Zarządzeniem nr 4 Dyrektora Ośrodka Rozwoju Edukacji z dnia 1 września 2016 r. wprowadzono w ORE *Politykę Bezpieczeństwa Informacji* (dalej: PBI), zgodnie z którą za poprawne i bezpieczne przetwarzanie danych osobowych odpowiada każda upoważniona do przetwarzania danych osobowych osoba. Administrator Systemów Informatycznych (dalej: ASI) zakłada i usuwa konta użytkowników, nadaje/usuwa/modyfikuje uprawnienia w systemach informatycznych na pisemny wniosek Administratora Bezpieczeństwa Informacji (dalej: ABI), Administratora Danych Osobowych (dalej: ADO) lub kierowników komórek organizacyjnych ORE. Zgodnie z zapisami PBI: *uwierzytelnianie* (pozwalające potwierdzić tożsamość użytkownika) *i kontrola dostępu* (przydzielenie użytkownikowi odpowiednich uprawnień) *są podstawowym środkiem ochrony systemów informatycznych i danych osobowych przetwarzanych w ORE w formie elektronicznej przed dostępem osób lub procesem nieupoważnionym*.

  W ORE prowadzona jest ewidencja wydanych upoważnień do ochrony danych osobowych oraz rejestr kategorii czynności przetwarzania.

  W ORE funkcjonuje system EZD PUW, w ramach którego realizowane jest Elektroniczne Zarządzanie Dokumentacją. System ten został wdrożony 1 maja 2021 r. i służy do wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci elektronicznej. Realizowany jest

w ramach systemu teleinformatycznego, o którym mowa w przepisach wydanych na podstawie art. 5 ust. 2b ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[17].

Postępowanie z dokumentacją, w tym określenie szczegółowych zasad i trybu wykonywania czynności kancelaryjnych zostały opisane w *Instrukcji kancelaryjnej Ośrodka Rozwoju Edukacji w Warszawie* będącej załącznikiem nr 1 do zarządzenia Nr 8/2021 Dyrektora Ośrodka Rozwoju Edukacji w Warszawie z dnia 23 marca 2021 r. W § 9 tego dokumentu wskazano – *"Użytkownicy systemu EZD posiadają upoważnienie do przetwarzania danych osobowych nadane przez administratora danych. Użytkownicy systemu EZD przetwarzają dane osobowe zgodnie z indywidualnym zakresem obowiązków."*

W *Regulaminie Organizacyjnym Ośrodka Rozwoju Edukacji* wskazano, że do zadań Wydziału Administracyjnego należy m.in. zapewnienie sprawnego obiegu dokumentów. W ORE prowadzone są prace nad opracowaniem szczegółowych procedur obiegu dokumentów.

W badanym zakresie nie stwierdzono nieprawidłowości.

Stwierdzone nieprawidłowości w obszarze pierwszym:

1) Na stronie internetowej ORE nie zamieszczono informacji o sposobie dostępu oraz zakresie użytkowym serwisu: *Platforma Systemu Ewaluacji Oświaty*, co uniemożliwia skuteczne zapoznanie się serwisem.
   Wymaganie informowania przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty wynika z § 5 ust. 2 pkt 1 rozporządzenia KRI.
2) Na stronie BIP ORE w opublikowanych opisach procedur obowiązujących przy załatwianiu spraw drogą elektroniczną nie zamieszczono informacji o rodzajach informatycznych nośników danych, na których może zostać doręczony Ośrodkowi dokument elektroniczny oraz zapisane urzędowe poświadczenie odbioru.
   Obowiązek taki wynika z § 3 ust. 1 pkt. 4-5 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz § 5 ust. 2 pkt 4 rozporządzenia KRI.

Ocena cząstkowa badanego obszaru: pozytywna pomimo stwierdzonych nieprawidłowości.

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 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.*

  Zgodnie z § 20 ust. 2 pkt 1 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:*

[17] Dz.U. z 2020 r. poz. 164 j.t.

zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

W ORE obowiązują następujące nw. regulacje.

Regulacje dotyczące ochrony danych osobowych:

1) Zarządzenie nr 4 z dnia 1 września 2016 r. w sprawie wprowadzenia w ORE dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, do którego załączniki stanowią:
   - Zał. nr 1 *Polityka Bezpieczeństwa Informacji* (dalej: PBI), która określa minimalne zabezpieczenia danych osobowych i systemów informatycznych ORE, w których wymagane jest stosowanie zapewniające co najmniej taki poziom bezpieczeństwa danych osobowych, jaki został określony w PBI, przy zastosowaniu odpowiednich środków technicznych i organizacyjnych.
   - Zał. nr 2 *Instrukcja Zarządzania Systemami Informatycznymi* opisująca zasady utrzymania i zarządzania systemami utrzymywanymi przez ORE, w których przetwarzane są dane osobowe, w tym m.in. procedury nadawania i rejestrowania uprawnień do przetwarzania danych w SI, wydawania upoważnień, stosowania metod i środków uwierzytelniania oraz procedur związanych z zarządzaniem upoważnieniami i ich użytkowaniem, procedur tworzenia kopii zapasowych, a także zapisy regulujące sposób zabezpieczania systemu informatycznego.
   - Zał. nr 3 *Instrukcja Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych* opisująca zasady poprawnego i bezpiecznego przetwarzania danych osobowych oraz korzystania z SI będąca uszczegółowieniem zapisów zawartych w PBI.
2) Zarządzenie nr 7/2018 z dnia 30 maja 2018 r. zmieniające ww. zarządzenie nr 4 w sprawie wprowadzenia zmian zapisów w:
   - *Polityce Bezpieczeństwa Informacji* w zakresie:
     - zastąpienia określenia Administrator Bezpieczeństwa Informacji (ABI) określeniem Inspektor Ochrony Danych (IOD);
     - zmiany brzmienia rozdziału 8 w części dotyczącej zasad przetwarzania danych osobowych i korzystania z systemów informatycznych;
     - dodania: załącznika nr 11 – oświadczenie o obowiązku zachowania poufności danych osobowych, załącznika nr 12 – oświadczenie na temat przetwarzania danych osobowych przez pracowników i załącznika nr 13 – oświadczenie na temat przetwarzania danych osobowych przez pracowników uzyskujących dostęp do pomieszczeń, w których przetwarzane są dane osobowe – personel sprzątający;
     - zmiany numeracji załącznika nr 5 – wzór upoważnienia do przetwarzania danych osobowych i załącznika nr 8 – wzór wniosku o upoważnienie pracownika oraz nadanie uprawnień w systemach teleinformatycznych;
   - *Instrukcji Zarządzania Systemami Informatycznymi* w zakresie:
     - zastąpienia określenia Administrator Bezpieczeństwa Informacji (ABI) określeniem Inspektor Ochrony Danych (IOD);
     - zmiany brzmienia rozdziału 3.1 – upoważnienie do przetwarzania danych osobowych i rozdziału 3.2 – nadawanie identyfikatorów i uprawnień;
   - *Instrukcji Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych* w zakresie:
     - zastąpienia określenia Administrator Bezpieczeństwa Informacji (ABI) określeniem Inspektor Ochrony Danych (IOD).
3) Zarządzenie nr 11/2018 z dnia 18 czerwca 2018 r. zmieniające zarządzenie nr 4 w sprawie wprowadzenia zmian zapisów w *Polityce Bezpieczeństwa Informacji* w zakresie dodania punktu 11 w rozdziale 8 w części dotyczącej zasad bezpiecznego

przetwarzania danych osobowych przez pracowników wykonujących swoje obowiązki poza siedzibą ORE przy zastosowaniu minimalnych wymagań dotyczących zabezpieczenia komputerów;

4) Zarządzenie nr 13/2018 z dnia 7 sierpnia 2018 r. zmieniające zarządzenie nr 4 w sprawie wprowadzenia zmian zapisów w *Polityce Bezpieczeństwa Informacji* w zakresie dodania załącznika nr 14 – oświadczenie o wyrażeniu zgody na używanie prywatnego sprzętu teleinformatycznego do celów służbowych oraz o obowiązku zachowania poufności danych osobowych w ORE;
5) Zarządzenie nr 14/2018 z dnia 6 września 2018 r. w sprawie wprowadzenia formularza skierowania na szkolenie wstępne dotyczące bezpieczeństwa przetwarzania i ochrony danych osobowych osób przyjmowanych do pracy w ORE;
6) Zarządzenie nr 34/2018 z dnia 17 grudnia 2018 r. aktualizujące podstawę prawną dotyczącą ochrony danych osobowych w obowiązujących zarządzeniach Dyrektora ORE;
7) Zarządzenie nr 15/2019 z dnia 5 kwietnia 2019 r. zmieniające nazwę zarządzenia nr 4 oraz 11/2018 i 13/2018, które otrzymało brzmienie „w sprawie wprowadzenia w Ośrodku Rozwoju Edukacji w Warszawie zasad przetwarzania danych osobowych";
8) Zarządzenie nr 16/2019 z dnia 8 kwietnia 2019 r. uchylające zarządzenie nr 7/2018 i zmieniające zarządzenie nr 4;
9) Zarządzenie nr 8/2020 z dnia 13 marca 2020 r. zmieniające zarządzenie nr 7/2018 w sprawie zmiany zarządzenia nr 4 w sprawie wprowadzenia w ORE dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych. Należy zauważyć, że wraz z wejściem w życie zarządzenia nr 16/2019 z dnia 8 kwietnia 2019 r., zarządzenie nr 7/2018 straciło moc;
10) Zarządzenie nr 31/2020 z dnia 2 grudnia 2020 r. zmieniające zarządzenie nr 4 w sprawie wprowadzenia zmian zapisów w *Instrukcji Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych* w zakresie dodania w rozdziale 6 „Korzystanie z systemów informatycznych" zasad dotyczących pracy z dokumentami elektronicznymi, przechowywanymi na dysku twardym lokalnej stacji roboczej a zawierającymi robocze kopie danych osobowych, przetwarzanych w systemach informatycznych w ORE.

<u>Regulacje dotyczące ochrony i bezpiecznego korzystania ze sprzętu:</u>

1) Zarządzenie nr 4 z dnia 1 września 2016 r. w sprawie wprowadzenia w ORE dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, do którego załącznik stanowi *Polityka Bezpieczeństwa Informacji*, w części dotyczącej rozdziału „*Wdrożenie systemów Informatycznych w ORE*".
2) Zarządzenie nr 24/2022 z dnia 24 sierpnia 2022 r. w sprawie zasad korzystania przez pracowników Ośrodka Rozwoju Edukacji w Warszawie ze służbowych telefonów komórkowych, kart SIM, Internetu mobilnego, laptopów oraz tabletów.

<u>Regulacje dotyczące inwentaryzacji:</u>

1) Zarządzenie nr 7 z dnia 4 sierpnia 2010 r. w sprawie wprowadzenia Regulaminu Inwentaryzacji;
2) Zarządzenie nr 18/2018 z dnia 4 października 2018 r. w sprawie wprowadzenia instrukcji inwentaryzacyjnej w Ośrodku Rozwoju Edukacji w Warszawie wraz z załącznikami;
3) Decyzja Dyrektora ORE Nr 3 z dnia 16 listopada 2020 r. o zarządzeniu inwentaryzacji na rok 2020 wraz z harmonogramem i planem inwentaryzacji stanowiącymi załączniki do decyzji;

4) Decyzja Dyrektora ORE Nr 3 z dnia 4 listopada 2021 r. o zarządzeniu inwentaryzacji na rok 2021 wraz z harmonogramem i planem inwentaryzacji stanowiącymi załączniki do decyzji;
5) Zarządzenie Nr 46/2019 z dnia 20 grudnia 2019 r. o wyznaczeniu Zespołów Spisowych do przeprowadzenia inwentaryzacji;
6) Zarządzenie Nr 47/2019 z dnia 20 grudnia 2019 r. w sprawie zmiany Zarządzenia Nr 20/2018 z dnia 11 października 2018 r. w sprawie powołania stałej komisji inwentaryzacyjnej celem przeprowadzenia inwentaryzacji;
7) Zarządzenie Nr 34/2020 z dnia 11 grudnia 2020 r. o wyznaczeniu Zespołów Spisowych do przeprowadzenia inwentaryzacji;
8) Zarządzenie Nr 33/2021 z dnia 4 listopada 2021 r. o wyznaczeniu Zespołów Spisowych do przeprowadzenia inwentaryzacji.

Regulacje dotyczące ochrony fizycznej:

1) Zarządzenie nr 4 z dnia 1 września 2016 r. w sprawie wprowadzenia w ORE dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. W załączniku - *Polityka Bezpieczeństwa Informacji*, w rozdziale „*Dostęp fizyczny i zabezpieczenia środowiskowe*", zawarto przepis, że fizyczna ochrona zapewniona jest poprzez system kontroli dostępu do budynków oraz system monitoringu wizyjnego;
2) Zarządzenie nr 24/2019 z dnia 20 maja 2019 r. w sprawie wprowadzenia instrukcji postępowania z kluczami w Ośrodku Rozwoju Edukacji;
3) Zarządzenie nr 13/2020 z dnia 22 czerwca 2020 r. w sprawie wprowadzenia *Regulaminu Pracy Ośrodka Rozwoju Edukacji w Warszawie* (dalej: Regulamin pracy).

   Zgodnie z *Regulaminem pracy*, w celu zapewnienia bezpieczeństwa pracowników, ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, prowadzi się całodobowy monitoring wizyjny we wszystkich miejscach prowadzenia działalności. *Regulamin pracy* określa sposób rejestracji czasu pracy w elektronicznym systemie ewidencji przy użyciu karty magnetycznej.
   W wyjaśnieniach przedstawionych przez ORE wskazano m.in., że „*w budynku przy Al. Ujazdowskich 28 w Warszawie funkcjonuje System Kontroli Dostępu (SKD). Bramki rejestrują godzinę wejścia i wyjścia wszystkich osób wchodzących lub wychodzących z budynku. (...) System Kontroli Dostępu (SKD) umożliwia kontrolę dostępu do budynku przy Al. Ujazdowskich 28 oraz elektroniczną ewidencję czasu pracy pracowników zatrudnionych w budynkach przy Al. Ujazdowskich 28 i przy ul. Polnej 46a w Warszawie*."

4) *Regulamin Organizacyjny* Ośrodka Rozwoju Edukacji w Warszawie zatwierdzony 1 grudnia 2016 r., zgodnie z którym gospodarowanie mieniem należy do zadań Zespołu Gospodarczego Wydziału Administracyjnego ORE.

ORE wskazał, że bezpośrednia ochrona fizyczna budynku w Al. Ujazdowskich 28 w Warszawie *jest realizowana przez pracowników etatowych ORE zatrudnionych na stanowiskach dozorców lub strażników mienia, posiadających analogiczny zakres zadań jak w przypadku firmy zewnętrznej*. Bezpośrednia ochrona fizyczna w budynku przy ul. Polnej 46a w Warszawie i w Centrum Szkoleniowym ORE w Sulejówku przy ul. Paderewskiego 77, jest realizowana przez pracowników firmy zewnętrznej na podstawie umów zawartych z firmą zewnętrzną.

Podczas kontroli stwierdzono, że obowiązująca w ORE *Polityka Bezpieczeństwa Informacji* była wielokrotnie aktualizowana zarządzeniami Dyrektora ORE. W przypadkach wielości wprowadzonych zmian, dla zwiększenia czytelności tekstu, dobrą praktyką jest np. opracowanie tekstu ujednoliconego uwzględniającego wprowadzone zmiany.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

  Zgodnie z zapisami zawartymi w *Instrukcji inwentaryzacyjnej ORE* środki trwałe własne znajdujące się w użytkowaniu ORE inwentaryzuje się drogą spisu z natury natomiast wartości niematerialne i prawne drogą porównania stanów wynikających z ksiąg rachunkowych z danymi wynikającymi z odpowiednich dokumentów, ich analizy oraz weryfikacji. Sprzęt i oprogramowanie służące do przetwarzania informacji w ORE inwentaryzuje się w jednostce na ostatni dzień każdego roku budżetowego. Ośrodek Rozwoju Edukacji inwentaryzuje sprzęt i oprogramowanie służące do przetwarzania informacji.
  W okresie 23.11-15.12.2021 r. została przeprowadzona przez firmę zewnętrzną niezależna ocena bezpieczeństwa sieci informatycznej Ośrodka Rozwoju Edukacji, na podstawie której powstał *Raport audytu bezpieczeństwa sieci informatycznej* (dalej: Raport) z dnia 3 grudnia 2021 r. Zakres tego audytu obejmował m.in. takie obszary jak:
  – inwentaryzacja posiadanych przez ORE zasobów: softwarowych (aplikacje, bazy danych, systemy operacyjne), sprzętowych (serwery, stacje robocze, urządzenia peryferyjne), sieci komputerowych (urządzeń sieciowych), inwentaryzacja dokumentacji (dot. dokumentacji sieci, polityki bezpieczeństwa, umowy usług zewnętrznych) oraz inwentaryzacja usług zewnętrznych;
  – sprawdzenie aktualizacji wersji oprogramowania na serwerach, stacjach roboczych, urządzeniach sieciowych, urządzeniach bezpieczeństwa.

  W trakcie kontroli ORE poinformował o podjętych i wdrożonych działaniach naprawczych.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*

  Zarządzeniem nr 2 Dyrektora ORE z dnia 30 stycznia 2015 r. w sprawie zarządzania ryzykiem wprowadzono *Instrukcję zarządzania ryzykiem w Ośrodku Rozwoju Edukacji w Warszawie*. Zarządzanie ryzykiem jest dokonywane poprzez sporządzanie *Rejestru celów i ryzyka* w danym roku kalendarzowym, który następnie jest aktualizowany co najmniej raz w roku. W okresie objętym kontrolą oraz w następstwie dokonanej identyfikacji ryzyka zostały sporządzone *Rejestry celów i ryzyka na rok 2021 i 2022*, w których opisano ryzyka prawdopodobne do wystąpienia wraz z możliwymi ich skutkami oraz wskazano jakie obowiązują mechanizmy kontrolne w poszczególnym zakresie określające niezbędne rozwiązania organizacyjne i techniczne zabezpieczające proces przetwarzania danych.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj.:*

- *podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;*
- *bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

W obowiązującej w ORE *Polityce Bezpieczeństwa Informacji* został przedstawiony zakres obowiązków dla poszczególnych grup pracowników w procesie przetwarzania danych osobowych. Administrator Systemów Informatycznych na pisemny wniosek Zespołu kadr, kierowników komórek organizacyjnych ORE, Administratora Bezpieczeństwa Informacji lub Administratora Danych Osobowych zakłada identyfikatory oraz nadaje/odbiera/zmienia uprawnienia w systemach informatycznych.

PBI określa zasady przydzielania uprawnień i upoważnień zgodnie z zasadą ich minimalizacji oznaczającej, że nie jest dopuszczalne nadawanie uprawnień wyższych niż wymagane do realizacji obowiązków na danych stanowisku. Okresowo, nie rzadziej niż raz na 3 miesiące, ASI, Administrator Techniczny lub inna osoba uprawniona przeprowadza przeglądy identyfikatorów i uprawnień. Szczegółowa procedura nadawania uprawnień została określona w *Instrukcji Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych*.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. zapewnienia 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*.

  Wprowadzona w ORE *Polityka Bezpieczeństwa Informacji* opisuje procedury kształcenia pracowników ORE z zakresu ochrony danych osobowych. Wszyscy pracownicy ORE przechodzą obowiązkowe szkolenia wstępne (przed rozpoczęciem przetwarzania danych osobowych) oraz okresowe (dla wybranej grupy lub konkretnych osób, w razie uzasadnionej potrzeby) z zakresu ochrony danych osobowych. Pracownicy lub inne osoby upoważnione do przetwarzania danych osobowych mają obowiązek zapoznać się z: *Polityką Bezpieczeństwa Informacji* i ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych i aktami wykonawczymi do ustawy.

  Zapisy *Regulaminu Pracy* wskazują, że „*przed dopuszczeniem do pracy, nowo zatrudnionego pracownika należy przeszkolić w zakresie bhp, ppoż. oraz ochrony danych osobowych*".

  Na podstawie udostępnionej dokumentacji, w okresie objętym kontrolą, tj. od 1 stycznia 2021 r. do 31 maja 2022 r. z zakresu bezpieczeństwa informacji przeszkolonych zostało 111 osób. ORE posiada plan szkolenia wewnętrznego z zakresu znajomości zasad ochrony danych osobowych w ORE.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 7, 9 i 11 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie*

następujących działań, tj. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

- *monitorowanie dostępu do informacji,*
- *czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,*
- *zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji (pkt 7),*
- *zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie (pkt 9),*
- *ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych (pkt 11).*

Norma PN-ISO/IEC 27002:2014, w pkt. 11.2.1 lit. e, wskazuje aby w celu ochrony sprzętu wprowadzić zabezpieczenia minimalizujące ryzyko związane z potencjalnymi zagrożeniami fizycznymi i środowiskowymi, np. kradzieżą, pożarem, dymem, zalaniem.

W Ośrodku Rozwoju Edukacji jest prowadzony na dany rok *Rejestr ewidencji upoważnionych do przetwarzania danych osobowych*. W rejestrze tym znajdują się dane osoby upoważnionej, nazwa zbioru danych, do którego wydane zostało upoważnienie, data nadania i ustania upoważnienia, zakres upoważnienia, identyfikator oraz status upoważnienia (aktualne/anulowane).

ORE prowadzi także *Arkusz informacji o udostępnieniu danych osobowych* (dalej: Arkusz) stanowiący załącznik nr 9 do *Polityki Bezpieczeństwa Informacji*. W Arkuszu tym zawarte są m.in.: dane odbiorcy (podmiotu wnioskującego o udostępnienie danych osobowych), nazwa zbioru, z którego udostępniono dane osobowe, data udostępnienia, imię i nazwisko osoby, której dane dotyczą czy zakres udostępnionych danych osobowych. Dane osobowe udostępnianie są na pisemny wniosek, zawierający uzasadnienie żądania udostępnienia danych.

W wyjaśnieniach złożonych przez Dyrektora ORE wskazano, że: „*z podmiotami zewnętrznymi biorącymi udział w przetwarzaniu danych których administratorem jest ORE podpisywane są umowy powierzenia danych zawierające wszystkie wymagane przepisami zapisy*."

Obowiązująca w Ośrodku Rozwoju Edukacji *Polityka Bezpieczeństwa Informacji* określa minimalne zabezpieczenia danych osobowych i systemów informatycznych w ORE. Wskazuje sposoby uniemożliwiające osobie nieuprawnionej ujawnienie, modyfikacje, usunięcie lub zniszczenie informacji m.in. poprzez nadawanie uprawnień do danych i systemów informatycznych, odpowiednie zabezpieczenie stanowiska pracy poprzez stosowanie zasady czystego biurka, uwierzytelnienia potwierdzające tożsamość użytkownika poprzez stosowanie indywidualnych haseł, stosowanie zabezpieczeń antywirusowych, aktualizacje systemów operacyjnych i serwerów, przechowywanie danych przetwarzanych w SI na serwerach, cykliczne wykonywanie kopii zapasowych.

Polityka Bezpieczeństwa Informacji w ORE reguluje sposoby ochrony przed zagrożeniami z sieci zewnętrznej i szkodliwym oprogramowaniem, m.in. poprzez zainstalowane systemy antywirusowe, aktualizacje systemów operacyjnych stacji roboczych i serwów, oddzielenie sieci lokalnej od publicznej poprzez Firewall, sprawdzanie poczty elektronicznej pod kątem szkodliwego oprogramowania i SPAMu, odpowiednie przechowywanie danych osobowych. Cyklicznie są wykonywane kopie zapasowe danych.

W *Raporcie* z audytu bezpieczeństwa sieci informatycznej (z 3 grudnia 2021 r.) przedstawiono ocenę bezpieczeństwa fizycznego systemów informatycznych, tj. warunków pracy urządzeń informatycznych oraz zabezpieczeń fizycznych i logicznych

przed nieautoryzowanym dostępem. W Raporcie wskazano m.in. na możliwe do wystąpienia ryzyka i ich potencjalne skutki dotyczące: warunków pracy urządzeń informatycznych w serwerowni mieszczącej się w budynku w Al. Ujazdowskich oraz zabezpieczeń fizycznych i logicznych przed nieautoryzowanym dostępem.

Podczas kontroli Ośrodek Rozwoju Edukacji poinformował o podjętych działaniach naprawczych. W trakcie prowadzonych czynności kontrolnych w siedzibie ORE mieszczącej się w Al. Ujazdowskich 28, jedno z pomieszczeń, gdzie znajdował się serwer (1 z 2 węzłów) było aktualnie remontowane (zakres prac obejmuje wydzieleniu odrębnego pomieszczenia na serwerownię).

Zgodnie z obowiązującym w ORE zarządzeniem nr 24/2019 z dnia 20 maja 2019 r. w sprawie wprowadzenia instrukcji postępowania z kluczami w ORE:
„Ilekroć w niniejszej instrukcji jest mowa o: książka ewidencji - należy przez to rozumieć książkę ewidencji pobierania kluczy, teczek, pieczęci, pojemników oraz wejść i wyjść z serwerowni" (§ 1 pkt. 7);
„Klucze do pomieszczeń serwerowni i poligrafii mogą zostać wydane tylko pracownikom uprawnionym przez Kierownika komórki odpowiedzialnej za zarządzanie kluczami lub innej osoby uprawnionej do zarządzania kluczami. Nieobecność w pracy osoby uprawnionej do poboru klucza serwerowni, wymaga każdorazowo wyznaczenia i uprawnienia innego pracownika do poboru kluczy. Dostęp osób trzecich do tych pomieszczeń odbywa się pod nadzorem osób uprawnionych i odnotowane w książce ewidencji serwerowni." (§ 3 pkt. 7).

W siedzibie Ośrodka w Al. Ujazdowskich 28 u pracownika ochrony znajduje się lista osób uprawnionych do poboru klucza do serwerowni, natomiast w siedzibie przy ul. Polnej 46a kontrolującym nie przedstawiono takiego wykazu.
Kontrolującym udostępniono dwie książki ewidencji – w Al. Ujazdowskich 28 oraz przy ul. Polnej 46a, w których znajdowały się wpisy pobierania kluczy do pomieszczeń. W książkach tych nie były odnotowane wpisy o dostępie osób trzecich do pomieszczeń serwerowni.

- Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

  Zarządzenie nr 11/2018 z dnia 18 czerwca 2018 r. w sprawie zmiany zarządzenia nr 4 z dnia 1.09.2016 r. w sprawie wprowadzenia w ORE dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, zmienionego zarządzeniem nr 7/2018 z dnia 30.05.2018 r. określa[18] minimalne wymagania dotyczące zabezpieczenia komputerów przez pracowników, wykonujących swoje obowiązki poza siedzibą ORE. Wskazano m.in. na: konieczność stosowania loginu i hasła przed uzyskaniem dostępu do danych umieszczonych na komputerze, wymogi jakie powinny spełniać hasła – BIOS/UEFI oraz użytkownika (długość hasła, stosowane znaki, częstotliwość zmiany), zapewnienie systemu typu firewall zabezpieczającego przed atakami zewnętrznymi, zapewnienie bieżącej aktualizacji (systemu firewall, operacyjnego oraz jego składników, sygnatur antywirusowych).

[18] Rozdział 8 – środki techniczne i organizacyjne zastosowane w celu ochrony przetwarzanych danych osobowych pkt 11.

Zarządzeniem nr 13/2018 z dnia 7 sierpnia 2018 r. w sprawie zmiany zarządzenia nr 4 z dnia 1.09.2016 r. (wskazane powyżej) dodano załącznik nr 14 – „*Oświadczenie o wyrażeniu zgody na używanie prywatnego sprzętu teleinformatycznego do celów służbowych oraz o obowiązku zachowania poufności danych osobowych w ORE*". Podpisując przedmiotowe oświadczenie, pracownik zobowiązuje się m.in. do przestrzegania przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, przepisów RODO oraz regulacji wewnętrznych Dyrektora ORE, zachowania poufności, dostosowania komputera prywatnego do wymogów wynikających z zarządzenia nr 11/2018.

W § 18 ust. 13 *Regulaminu Organizacyjnego* ORE wskazano, że „*w uzasadnionych zadaniami merytorycznymi przypadkach, Dyrektor Ośrodka, po zasięgnięciu opinii bezpośredniego przełożonego lub wicedyrektora nadzorującego, może na czas określony zmienić zasady dotyczące miejsca realizacji konkretnego obowiązku pracowniczego, w tym może udzielić zgody* na pracę w domu lub innym wskazanym przez pracownika miejscu."

Zarządzenie nr 36/2020 z dnia 29 grudnia 2020 r. w sprawie wprowadzenia w ORE pracy zdalnej, wprowadza system organizacji pracy, przewidujący wykonywanie pracy poza stałym miejscem jej wykonywania (w formie pracy zdalnej).

Zgodnie z zapisami zarządzenia nr 24/2022 z dnia 24 sierpnia 2022 r. w sprawie zasad korzystania przez pracowników Ośrodka Rozwoju Edukacji w Warszawie ze służbowych telefonów komórkowych, kart SIM, Internetu mobilnego, laptopów oraz tabletów, na urządzeniach służbowych można korzystać wyłącznie z oprogramowania oficjalnie nabytego przez ORE i wykorzystywanego do celów służbowych. Zgodnie z § 4 ust. 1 i 2 ww. zarządzenia pracownik jest zobowiązany zapewnić ochronę urządzenia służbowego, z którego korzysta. W zarządzeniu określono sposoby ochrony tych urządzeń.[19]

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

  Ośrodek Rozwoju Edukacji podpisywał umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych, w których były zawarte zapisy dotyczące zapewnienia bezpieczeństwa informacji.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

[19] Pracownikowi zabrania się pozostawiania urządzenia służbowego w miejscach, w których pracownik nie ma możliwości sprawowania nadzoru nad urządzeniem, gromadzenia i przechowywania na nieszyfrowanych urządzeniach służbowych informacji prawnie chronionych oraz informacji, których utrata, ujawnienie lub udostępnienie osobie nieuprawnionej lub podmiotowi nieuprawnionemu mogłyby spowodować szkodę ORE lub naruszyć prawnie chroniony interes innych osób lub podmiotów, przeglądania na służbowym urządzeniu stron internetowych zawierających treści podejrzane lub niebezpieczne, pobierania na służbowe urządzenie plików oraz otrzymanych pocztą elektroniczną załączników, których pochodzenie lub zawartość budzi wątpliwości, podłączania urządzeń służbowych do publicznie dostępnych lub nieznanych sieci bezprzewodowych.

Według zapisów załącznika A normy PN-EN ISO/IEC 27001:2017 należy zidentyfikować informacje[20], aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów[21]; informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację[22].

Zgodnie z normą PN-ISO/IEC 27001 przez incydent związany z bezpieczeństwem informacji należy rozumieć pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Bezzwłoczne zgłaszanie incydentów z zakresu naruszenia bezpieczeństwa informacji[23] ma na celu zapewnienie szybkiej reakcji i podjęcie odpowiednich działań.

W wyjaśnieniach dotyczących ustanowienia przez ORE procedury postępowania z naruszeniami bezpieczeństwa informacji, Ośrodek poinformował, że: *„w kwestii procedur i postępowania z naruszeniami w ORE zostało przyjęte Zarządzenie nr 4/2016 Polityka Bezpieczeństwa Informacji ORE. W dziale VI ust. 3 widnieje zapis - zobowiązanie pracowników do zgłaszania naruszeń bezpieczeństwa do przełożonego lub IOD. (...) Dalsza procedura wynika z przepisów i wytycznych UODO.*"[24]

ORE poinformował, że: *„Pracownicy zobowiązani są do zgłaszania stwierdzonych incydentów bezpośrednim przełożonym lub IOD. Po otrzymaniu zgłoszenia IOD podejmuje czynności wyjaśniające. Raport z przeprowadzanych czynności zawierający opis i stwierdzone przyczyny zaistnienia incydentu wraz z zaleceniami przekazywany jest Dyrektorowi ORE. W przypadku stwierdzenia, że incydent stanowi wysokie ryzyko naruszenia praw i wolności osób fizycznych incydenty zgłaszane są do PUODO oraz powiadamiane są osoby poszkodowane.*"[25]

W dziale VI ust. 3 *Polityki Bezpieczeństwa Informacji* w ORE wskazano, że *osoby upoważnione – pracownicy lub współpracownicy ORE, upoważnieni do przetwarzania danych osobowych mają obowiązek zgłaszać naruszenia bezpieczeństwa informacji do przełożonego lub IOD*.

---

[20] Sformułowanie definicji informacji jest ściśle powiązane z określeniem kryteriów bezpieczeństwa (tzw. triada CIA - skrót ten pochodzi od pierwszych liter nazw kryteriów w języku angielskim, tj. Confidentiality - poufność, Integrity – integralność, Availability - dostępność), do których zalicza się:
- poufność informacji oznaczająca, że informacje są dostępne tylko i wyłącznie dla tych osób, które są do tego uprawnione;
- integralność/nienaruszalność informacji oznaczająca zagwarantowanie dokładności i kompletności informacji oraz metod i sposobów ich przetwarzania;
- dostępność informacji oznaczająca zapewnienie, że upoważnieni użytkownicy mają dostęp do informacji i związanych z nimi zasobów, zawsze wtedy gdy jest to wymagane.

[21] Pkt A.8.1.1;

[22] Pkt A.8.2.1;

[23] „Bezpieczeństwo informacji można rozumieć jako wypadkową bezpieczeństwa prawnego, fizycznego, teleinformatycznego i osobowo-organizacyjnego." [Mariusz Pala Rozdział 8. „Współczesne zagrożenia dla bezpieczeństwa" w: „Bezpieczeństwo Informacyjne w XXI wieku", red. Naukowa Mariusz Kubiak, Stanisław Topolewski, wyd. Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, 2016, s 137];

[24] Osobom kontrolującym zostały udostępnione wytyczne Urzędu Ochrony Danych Osobowych z czerwca 2019 r. *„Obowiązki administratorów związane z naruszeniami ochrony danych osobowych;*

[25] Wyjaśnienia zawarte w *Ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań publicznych* udostępnione ORE do wypełnienia.

Powyższe zapisy zobowiązujące pracowników do zgłaszania naruszeń bezpieczeństwa informacji do przełożonego lub IOD nie określają sposobu zgłaszania incydentów naruszenia bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 13 rozporządzenia KRI. W opinii kontrolujących zapis ten sugeruje zawężoną grupę osób, tj. upoważnionych do przetwarzania danych osobowych, mających obowiązek zgłaszania naruszeń bezpieczeństwa informacji.

Polityka Bezpieczeństwa Informacji stanowi załącznik nr 1 do zarządzenia nr 4 z dnia 1 września 2016 r. w sprawie wprowadzenia w ORE dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.
Zgodnie z Wprowadzeniem do *Polityki Bezpieczeństwa Informacji,* dokument ten jest „*podstawowym elementem dokumentacji opisującej zasady przetwarzania danych osobowych w ORE oraz opisuje środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych adekwatną do zagrożeń oraz kategorii danych objętych ochroną. Polityka Bezpieczeństwa Informacji opisuje sposób realizacji przez ORE wymogów określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 992), a także w aktach wykonawczych do Ustawy. Definiuje procedury i zasady stosowane przez ORE w celu zapewnienia ochrony przetwarzanych danych osobowych zgodnie z wymogami obowiązującego prawa*."

W opinii kontrolujących nazwa ww. Zarządzenia jak i ww. opis zamieszczony w *Polityce Bezpieczeństwa Informacji* wskazują, że regulacja dotyczy wyłącznie zakresu ochrony danych osobowych.

W Ośrodku Rozwoju Edukacji prowadzony jest *Rejestr przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych*. W okresie objętym kontrolą został stwierdzony 1 incydent bezpieczeństwa skutkujący możliwością wystąpienia ryzyka utraty poufności danych osobowych. Incydent ten został zgłoszony do Inspektora Ochrony Danych (dalej: IOD), odnotowany w Rejestrze, w którym szczegółowo opisano zaistniałe naruszenie oraz sposób jego usunięcia poprzez odpowiednio podjęte działania (nie stwierdzono konieczności powiadamiania organu nadzorczego).

- Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*

  Ministerstwo Administracji i Cyfryzacji (MAiC) oraz Ministerstwo Finansów (MF) z uwagi na trudności interpretacyjne dotyczące zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w powyższym zapisie, opracowały wspólne stanowisko w powyższym zakresie. Zgodnie ze *Wspólnym stanowiskiem Departamentu Informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji*[26] intencją projektodawcy wyżej przywołanego zapisu KRI było zobowiązanie podmiotów realizujących zadania publiczne do realizowania okresowego audytu wewnętrznego, bez szczegółowego wskazywania na rodzaj audytu oraz tryb jego

[26] https://mf-arch2.mf.gov.pl/web/bip/ministerstwo-finansow/dzialalnosc/finanse-publiczne/kontrola-zarzadcza-i-audyt-wewnetrzny/audyt-wewnetrzny-w-sektorze-publicznym/metodyka/-/asset_publisher/SVp7/content/audyt-bezpieczenstwa-informacji?redirect=https%3A%2F%2Fmf-arch2.mf.gov.pl%2Fweb%2Fbip%2Fministerstwo-finansow%2Fdzialalnosc%2Ffinanse-publiczne%2Fkontrola-zarzadcza-i-audyt-wewnetrzny%2Faudyt-wewnetrzny-w-sektorze-publicznym%2Fmetodyka%3Fp_p_id%3D101_INSTANCE_SVp7%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_count%3D1

przeprowadzania. Użycie w KRI sformułowania „audyt wewnętrzny" nie miało na celu obligatoryjnego przypisania tego obowiązku komórkom audytu wewnętrznego, funkcjonującym w jednostkach sektora finansów publicznych na mocy przepisów Działu VI ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[27] (Dz.U. z 2013 r. poz. 885, z późn. zm.). Jak wyżej wskazano, ustawodawca nie określił sposobu, trybu, rodzaju audytu, ani też osób czy komórek organizacyjnych, którym należałoby powierzyć prowadzenie ww. audytu. Zatem decyzja co do tego, komu zostanie powierzone prowadzenie omawianego audytu, spoczywa na kierownictwie podmiotu.

W ramach realizacji ww. obowiązków zapewnienia okresowego audytu w zakresie bezpieczeństwa informacji, w ORE został przeprowadzony w okresie 23.11-15.12.2021 r. przez firmę zewnętrzną audyt bezpieczeństwa sieci informatycznej Ośrodka Rozwoju Edukacji (wskazany wyżej). W ramach realizacji ww. audytu powstał „*Raport audytu bezpieczeństwa sieci informatycznej*".

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 12 lit. a-d, h rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:*
  a) dbałości o aktualizację oprogramowania,
  b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
  c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
  d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów,
  e) ...
  f) ...
  g) ...
  h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

  Ośrodek Rozwoju Edukacji wyjaśnił, że „*oprogramowania, które dają możliwość zaktualizowania są na bieżąco aktualizowane. W przypadku oprogramowania nieobjętego wsparciem producenta, ICEiN przekazuje do ORE rekomendacje zakupu wsparcia lub nowej wersji oprogramowania."*

  Zgodnie z Opisem Przedmiotu Zamówienia, będącym załącznikiem do umowy nr CIE-36/2019 na utrzymanie hostingu, system zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa. Oprogramowanie antywirusowe musi posiadać funkcjonalność określenia harmonogramu lub częstotliwości pobierania aktualizacji bezpieczeństwa od producenta oprogramowania, aktualizacji bazy wirusów, wszelkich poprawek oprogramowania oraz umożliwiać określenie centralnego punktu dystrybucji uaktualnień i poprawek oprogramowania w infrastrukturze zamawiającego. Producent musi zapewnić aktualizację systemu, uwzględniając co najmniej: sygnatury ataków, listę reguł polityki bezpieczeństwa oraz monitorowania aktywności użytkowników na bazach danych, listę testów podatności baz danych oraz listę raportów.

  Natomiast zgodnie z umową nr ICEiN-8/2022 z 1 marca 2022 r. na wsparcie techniczne i administrowanie platformą internetową *Systemu Ewaluacji Oświaty* świadczenie usługi administrowania Platformą polega m.in. na prowadzeniu i aktualizowaniu dokumentacji

[27] j.t. Dz.U. z 2022 r. poz. 1634 ze zm.

administracyjnej i użytkownika Platformy a wsparcie techniczne Platformy to m.in. aktualizowanie systemów operacyjnych i ich komponentów oraz oprogramowania na potrzeby Platformy.

Zgodnie z pkt 12.3.1 lit. e normy PN-ISO/IEC 27002:2013 nośniki kopii zapasowych powinny być testowane aby można było na nich polegać w przypadku awaryjnego odtwarzania.

Ogólne zasady dotyczące tworzenia kopii zapasowych, w tym minimalizowania ryzyka utraty informacji w wyniku awarii, są zapisane w *Polityce Bezpieczeństwa Informacji.* W części dotyczącej ochrony danych przed utratą wskazano, że: kopie zapasowe danych trzymanych na serwerach wykonywane są cykliczne, adekwatnie do częstotliwości zmian w systemie, a kopie zapasowe danych osobowych trzymanych na stacjach roboczych tworzone są okresowo. Zabronione jest samowolne tworzenie kopii zapasowych na nośniki przenośne (USB, CD/DVD, inne) oraz wynoszenie kopii zapasowych poza siedzibę ORE bez zgody ABI. Nośniki, na których zapisane są kopie zapasowe powinny być zabezpieczone przed kradzieżą oraz działaniem negatywnych czynników zewnętrznych, natomiast serwery są zabezpieczone przed utratą danych w przypadku awarii zasilania poprzez urządzenia podtrzymujące napięcie (UPS).

Kopie zapasowe tworzone są zgodnie z Opisem Przedmiotu Zamówienia będącym załącznikiem do umowy nr CIE-36/2019 na utrzymanie hostingu, w którym wskazano wymagane dwa systemy kopii zapasowych (podstawowe CPD i zapasowe DRC), wykonujące niezależne kopie. ORE w złożonych wyjaśnieniach wskazał jak często wykonywany jest backup maszyn wirtualnych, na których utrzymywane są systemy ORE, przez jaki okres przechowywane są kopie zapasowe oraz kto odpowiada za tworzenie kopii zapasowych.

W *Polityce Bezpieczeństwa Informacji*, w części dotyczącej dostępu fizycznego i zabezpieczeń środowiskowych, określono stosowane w ORE środki zabezpieczeń sprzętu informatycznego poprzez umieszczenie serwerów wykorzystywanych przez systemy informatyczne w pomieszczeniach zabezpieczonych, zarówno przed nieautoryzowanym dostępem, jak i przed niekorzystnym wpływem czynników atmosferycznych.

Kontrolowane serwerownie są wyposażone w urządzenia wentylacyjno-klimatyzacyjne oraz w urządzenia podtrzymujące zasilanie (UPS).

W wyjaśnieniach przedstawionych przez ORE wskazano, że mechanizmami kryptograficznymi stosowanymi w kontrolowanych systemach w celu zabezpieczenia go przed nieuprawnionym dostępem są: SSL – zabezpieczenie transmisji danych podczas korzystania z systemu oraz VPN (Palo Alto Networks) – zabezpieczenie i ograniczenie dostępu do infrastruktury na potrzeby wykonywania czynności administracyjnych.

Zgodnie ze statutem ICEiN przedmiotem działalności Centrum jest m.in. obsługa informatyczna Ośrodka Rozwoju Edukacji. ICEiN jest jednostką posiadającą SZBI zgodne z normą PN-ISO/IEC 27001, a usługi świadczone na rzecz ORE są zgodne z przedmiotową normą.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 21 ust. 1 rozporządzenia KRI - *rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).*

Jednym z elementów kontroli systemów informatycznych[28] w zakresie bezpieczeństwa jest przegląd dziennika systemu jako mechanizm śledzenia zdarzeń (tzn. które rekordy lub pola zostały zmienione, w jakim zakresie i kto oraz kiedy dokonał zmian). Kontrolującym nie zostały udostępnione dzienniki zdarzeń zarówno *Systemu Ewaluacji Oświaty,* jak i systemu *Szkolenie kandydatów na ekspertów.* ORE wyjaśnił, że „*logi systemowe oraz aplikacyjne są przechowywane na maszynie wirtualnej i razem z nią backupowane przez firmę hostingową. Dodatkowo logi są kopiowane na przeznaczony do tego serwer*."

W badanym zakresie nie stwierdzono nieprawidłowości.

Stwierdzone nieprawidłowości w obszarze drugim

W *Polityce Bezpieczeństwa Informacji* nie określono sposobu zgłaszania incydentów naruszenia bezpieczeństwa informacji.
Na podstawie § 20 ust. 2 pkt 13 rozporządzenia KRI - zgłaszanie incydentów naruszenia bezpieczeństwa informacji powinno być realizowane w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Ocena cząstkowa badanego obszaru: pozytywna pomimo stwierdzonej nieprawidłowości.

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

Zgodnie z § 19 rozporządzenia KRI - *w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia*.

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. Obecnie obwiązuje wersja 2.1 tych wytycznych.

Zgodnie z *Regulaminem Organizacyjnym* ORE zatwierdzonym 1 grudnia 2016 r. do zadań Wydziału Upowszechniania Zasobów należy m.in. zapewnienie zgodności serwisów i materiałów wypracowanych przez merytoryczne komórki organizacyjne Ośrodka z wymogami WCAG 2.0 na poziomie AA poprzez nadzór i wspieranie pozostałych komórek organizacyjnych w realizacji tego zadania oraz zapewnienie zgodności serwisów teleinformatycznych Ośrodka z wymogami WCAG 2.0 na poziomie AA, między innymi poprzez nadzór i współpracę z wykonawcami systemów. Wydział Wydawnictw odpowiada m.in. za przygotowanie publikacji Ośrodka zgodnie z zasadami WCAG 2.0 AA w formie elektronicznej do zamieszczania w Internecie.

Zgodnie z przedstawioną przez Ośrodek Rozwoju Edukacji informacją, zarządzanie usługami realizowanymi przez systemy teleinformatyczne w ORE odbywa się w oparciu o:
– *Instrukcję Zarządzania Systemami Informatycznymi służącymi do Przetwarzania Danych Osobowych*,[29]

[28] Na podstawie Podręcznika kontroli systemów informatycznych dla najwyższych organów kontroli opracowany przez INTOSAI Working Group on IT Audit (WGITA) opracowanego przez Departament Metodyki Kontroli i Rozwoju Zawodowego Najwyższej Izby Kontroli, Warszawa 2016 r.

[29] Będąca załącznikiem nr 2 do zarządzenia Nr 4 Dyrektora Ośrodka Rozwoju Edukacji z dnia 1 września 2016 r. w sprawie wprowadzenia w Ośrodku Rozwoju Edukacji w Warszawie dokumentacji opisującej sposób przetwarzania danych osobach oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;

- *Instrukcję Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych*[30],
- *Standardy przygotowywania i publikowania treści oraz projektowania serwisów internetowych zgodnie z wytycznymi WCAG 2.0 na poziomie AA* (stanowiące załącznik do decyzji Dyrektora ORE z dnia 25 kwietnia 2016 r.),
- *Standardy przygotowywania treści zgodnie z wytycznymi WCAG 2.1 na poziomie AA*[31], (stanowiące załącznik do decyzji nr 1/2021 Dyrektora ORE z dnia 22 lutego 2021 r. zmieniającą decyzję Dyrektora ORE z dnia 25 kwietnia 2016 r.).

Zgodnie z art. 10 ust. 7 pkt 1 ustawy o dostępności cyfrowej - *podmiot publiczny publikuje deklarację dostępności strony internetowej - na tej stronie internetowej*.

Na podstawie art. 11 ustawy o dostępności cyfrowej - *podmioty publiczne dokonują przeglądu i aktualizacji deklaracji dostępności do dnia 31 marca każdego roku oraz niezwłocznie w każdym przypadku, gdy strona internetowa lub aplikacja mobilna podlega zmianom mogącym mieć wpływ na jej dostępność cyfrową*.

Deklaracja dostępności została zamieszczona na stronie *Biuletynu Informacji Publicznej* ORE (https://bip.ore.edu.pl/358-2/) i zawiera informacje nt. poziomu dostępności tej strony, tj.: „*strona internetowa jest częściowo zgodna z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych.* Niezgodności lub wyłączenia dotyczą *części zamieszczonych dokumentów PDF, szczególnie tych najstarszych, które nie są dostępne cyfrowo przez co nie są obsługiwane przez czytniki ekranu*. (…) *Na stronie internetowej można korzystać ze standardowych skrótów klawiaturowych*."

Zgodnie z informacją podaną na stronie deklarację sporządzono na podstawie samooceny przeprowadzonej przez podmiot publiczny. Widniejąca data dokonania ostatniego przeglądu deklaracji dostępności to 30.04.2021 r.

Na stronie *Szkolenie kandydatów na ekspertów* (https://ekspert.ore.edu.pl/deklaracja-dostepnosci.html) zamieszczono deklarację dostępności, która zawiera informacje nt. poziomu dostępności tej strony, tj.: „*strona internetowa jest częściowo zgodna z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych (…) Strona startowa zawierająca informacje wstępne i tematy szkoleń e-learningowych jest dostępna (…)* Niezgodności lub wyłączenia dotyczą platformy Moodle, „*która nie jest obsługiwana przez czytniki ekranu*". (…) Docelowo prowadzenie szkoleń e-learningowych ma się odbywać na dostępnej Zintegrowanej Platformie Edukacyjnej. „*Na stronie startowej serwisu brakuje tzw. kotwic służących do szybszej nawigacji oraz możliwości zmiany kontrastu i regulowania rozmiarem czcionki. Nie jest również widoczny fokus. (…) Na stronie internetowej można korzystać ze standardowych skrótów klawiaturowych."*

Zgodnie z informacją podaną na stronie deklarację sporządzono na podstawie samooceny przeprowadzonej przez podmiot publiczny. Widniejąca data dokonania ostatniego przeglądu deklaracji dostępności to 25.03.2020 r.

Na stronie *Platformy System Ewaluacji Oświaty* (https://np.gov.pl/, https://badania.np.gov.pl) nie została zamieszczona deklaracja dostępności tej strony.

Stwierdzone nieprawidłowości w obszarze trzecim

[30] Stanowiąca załącznik nr 3 do zarządzenia Nr 4 Dyrektora Ośrodka Rozwoju Edukacji z dnia 1 września 2016 r. w sprawie wprowadzenia w Ośrodku Rozwoju Edukacji w Warszawie dokumentacji opisującej sposób przetwarzania danych osobach oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

[31] Dostępne na stronie: https://www.ore.edu.pl/wp-content/uploads/2022/01/standardy-przygotowywania-tresci-zgodnie-z-wytycznymi-wcag-2.1_ore_2021.pdf

1) Niezamieszczenie na stronie *Platformy Systemu Ewaluacji Oświaty* (https://np.gov.pl/, https://badania.np.gov.pl) deklaracji dostępności.
   Zgodnie z art. 10 ust. 7 pkt 1 ustawy o dostępności cyfrowej, *podmiot publiczny publikuje deklarację dostępności strony internetowej - na tej stronie internetowej*.
2) Terminy przeglądu i aktualizacji deklaracji dostępności widniejące na stronach: *Biuletynu Informacji Publicznej* ORE (https://bip.ore.edu.pl/358-2/) oraz *Szkolenie kandydatów na ekspertów* (https://ekspert.ore.edu.pl/deklaracja-dostepnosci.html) nie były zgodne z terminem wskazanym w ustawie o dostępności cyfrowej na ich dokonanie, tj. do dnia 31 marca każdego roku.

Ocena cząstkowa badanego obszaru: pozytywna pomimo stwierdzonych nieprawidłowości.

Mając na uwadze stwierdzone podczas kontroli nieprawidłowości oraz przedstawione uwagi, na podstawie art. 46 ust. 3 pkt 1 ustawy o kontroli w administracji rządowej przedstawiam następujące zalecenia i wnioski.

Zalecenia:

1) Zamieszczenie na stronie internetowej ORE informacji o sposobie dostępu oraz zakresie użytkowym serwisu: *Platforma Systemu Ewaluacji Oświaty*, w sposób umożliwiający skuteczne zapoznanie się z serwisem.
2) Zamieszczenie na stronie BIP ORE, w opublikowanych opisach procedur obowiązujących przy załatwianiu spraw drogą elektroniczną, informacji o rodzajach informatycznych nośników danych, na których może zostać:
   – doręczony ORE dokument elektroniczny,
   – zapisane urzędowe poświadczenie odbioru.
3) Określenie w *Polityce Bezpieczeństwa Informacji* sposobu zgłaszania incydentów naruszenia bezpieczeństwa informacji.
4) Stosowanie art. 10 ust. 7 pkt 1 ustawy o dostępności cyfrowej, zgodnie z którym podmiot publiczny publikuje deklarację dostępności strony internetowej - na tej stronie internetowej.
5) Dokonywanie przeglądu i aktualizacji deklaracji dostępności do dnia 31 marca każdego roku oraz niezwłocznie w każdym przypadku, gdy strona internetowa lub aplikacja mobilna podlega zmianom mogącym mieć wpływ na jej dostępność cyfrową.

Wnioski:

1) Mając na uwadze bezpieczeństwo informacji, zgodnie z zapisami zawartymi w zarządzeniu nr 24/2019 z dnia 20 maja 2019 r. w sprawie wprowadzenia instrukcji postępowania z kluczami w ORE dokonywanie w książkach ewidencji wpisów o dostępie osób trzecich do pomieszczeń serwerowni.
2) Podczas kontroli stwierdzono, że obowiązująca w ORE *Polityka Bezpieczeństwa Informacji* była wielokrotnie aktualizowana zarządzeniami Dyrektora ORE. Dobrą praktyką, dla zwiększenia czytelności tekstu, jest np. opracowanie tekstu ujednoliconego uwzględniającego wprowadzone zmiany.
3) Nazwa zarządzenia nr 4 z dnia 1 września 2016 r. *w sprawie wprowadzenia w ORE dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych*, jak i opis zamieszczony we Wprowadzeniu do *Polityki Bezpieczeństwa Informacji* będącej załącznikiem do ww. Zarządzenia wskazują, że regulacje te dotyczą wyłącznie zakresu ochrony danych osobowych. Zasadne jest dokonanie analizy zawężania ww. Zarządzenia do przepisów odnoszących się do tematyki ochrony danych osobowych.
4) Zapewnić spełnienie przez systemy ORE wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia KRI.

Na podstawie art. 49 ww. ustawy o kontroli w administracji rządowej, przedstawiając powyższe wystąpienie pokontrolne, proszę o przekazanie w terminie 30 dni od daty otrzymania niniejszego wystąpienia informacji o sposobie wykonania zaleceń i wykorzystania wniosków.

Od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z upoważnienia
Ministra Edukacji i Nauki
Włodzimierz Bernacki
Sekretarz Stanu
/ – podpisano cyfrowo/

Potwierdzam zgodność kopii wydruku z dokumentem elektronicznym:

Identyfikator dokumentu	1836050.7777082.6624464
Nazwa dokumentu	2022.12.14 Wystąpienie pokontrolne.docx
Tytuł dokumentu	2022.12.14 Wystąpienie pokontrolne
Sygnatura dokumentu	DKO-WKiDN.0915.1.2022
Data dokumentu	
Skrót dokumentu	CB8B8BC90A061B6F1AC805BBCBEBCF2E9900DEF6
Wersja dokumentu	1.6
Data podpisu	21.12.2022 10:59:09
Podpisane przez	Włodzimierz Bernacki Sekretarz Stanu
Rodzaj certyfikatu	Certyfikat kwalifikowany podpisu elektronicznego karta

EZD 3.109.241.241.

Data wydruku: 22.12.2022

Autor wydruku: Jakubiak-Kępińska Alicja (Główny Specjalista)