Minister
Edukacji

DKA-WK.0915.3.2024.AJK
Warszawa, 30 czerwca 2025 r.

Pani
Agnieszka Koterla
p.o. Dyrektor Ośrodka Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5
02-675 Warszawa

WYSTĄPIENIE POKONTROLNE

Zgodnie z art. 47 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1] przekazuję niniejsze wystąpienie pokontrolne.

Na podstawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej* oraz art. 25 ust. 1 pkt 3 lit. b ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[2], Ministerstwo Edukacji Narodowej[3] w terminie od 30 października 2024 r. do 17 stycznia 2025 r. przeprowadziło w Ośrodku Rozwoju Polskiej Edukacji za Granicą, z siedzibą przy ul. Wołoskiej 5, 02-675 Warszawa, kontrolę pn. *Działanie i bezpieczeństwo wybranych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych*.

Celem kontroli było dokonanie oceny działania systemów teleinformatycznych pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych i wymiany informacji w postaci elektronicznej.
Oceniono:
1) współdziałanie systemów teleinformatycznych poprzez właściwą organizację wymiany informacji w postaci elektronicznej, współpracę z innymi systemami informatycznymi oraz procesy wspomagania świadczenia usług drogą elektroniczną;
2) zarządzanie bezpieczeństwem informacji dla badanych systemów teleinformatycznych;
3) dostępność treści zawartych na stronach internetowych dla osób z niepełnosprawnościami.

Kontrolą objęto okres od 1 stycznia 2023 r. do dnia rozpoczęcia kontroli, tj. 30 października 2024 r.

[1] Dz.U. z 2020 r. poz. 224.
[2] Dz.U. z 2024 r. poz. 1557.
[3] Kontrolę przeprowadzili pracownicy Ministerstwa:
1) Alicja Jakubiak-Kępińska, główny specjalista w Wydziale Kontroli w Departamencie Kontroli i Audytu, na podstawie upoważnień nr 52/2024 z dnia 30 października 2024 r. i nr 59/2024 z dnia 16 grudnia 2024 r.;
2) Beata Tarłowska, główny specjalista w Wydziale Oświaty Polskiej za Granicą i Migracji w Departamencie Współpracy Międzynarodowej, na podstawie upoważnień nr 53/2024 z dnia 30 października 2024 r. i nr 60/2024 z dnia 16 grudnia 2024 r.;
3) Jan Pastwa, radca generalny w Wydziale Oświaty Polskiej za Granicą i Migracji w Departamencie Współpracy Międzynarodowej, na podstawie upoważnień nr 54/2024 z dnia 30 października 2024 r. i nr 61/2024 z dnia 16 grudnia 2024 r.

telefon: + 48 22 34 74 100
adres email: sekretariat.b.nowacka@men.gov.pl
gov.pl/edukacja

al. J.Ch. Szucha 25
00-918 Warszawa

Ośrodek Rozwoju Polskiej Edukacji za Granicą (dalej: ORPEG, Ośrodek) jest państwową jednostką budżetową finansowaną z części 30 budżetu państwa – Oświata i wychowanie, utworzoną na mocy zarządzenia nr 35 Ministra Edukacji Narodowej z dnia 24 listopada 2010 r. *w sprawie włączenia Polonijnego Centrum Nauczycielskiego w Lublinie do Zespołu Szkół dla Dzieci Obywateli Polskich Czasowo Przebywających za Granicą z siedzibą w Warszawie oraz zmiany nazwy tego Zespołu*[4].
Zgodnie ze statutem nadanym ORPEG zarządzeniem nr 23 Ministra Edukacji i Nauki z dnia 16 marca 2023 r. *w sprawie statutu Ośrodka Rozwoju Polskiej Edukacji za Granicą*[5], Ośrodek jest zespołem szkół i placówek, którego celem jest koordynacja zadań związanych z organizacją kształcenia dzieci obywateli polskich czasowo przebywających za granicą. Działalnością ORPEG kieruje jego dyrektor.
W okresie objętym kontrolą Ośrodkiem kierowała pani Justyna Kralisz, powołana na stanowisko dyrektora tego Ośrodka 22 listopada 2021 r., następnie stanowisko dyrektora objął pan Adam Kalbarczyk, powołany 19 marca 2024 r. Od 7 lutego 2025 r. p.o. dyrektora ORPEG jest pani Agnieszka Koterla.

Kontrolowany obszar regulują:
- ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[6] (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*[7] (dalej: rozporządzenie KRI z 2012 r.); rozporządzenie straciło moc z dniem 23 maja 2024 r.;
- rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[8] (dalej: rozporządzenie KRI z 2024 r.); rozporządzenie weszło w życie 23 maja 2024 r.;
- 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*[9] (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*[10] (dalej: ustawa o dostępności cyfrowej);
- ustawa z dnia 6 września 2001 r. *o dostępie do informacji publicznej*[11];
- ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* [12].

Do kontroli zostały wybrane nw. systemy, wykorzystywane do realizacji zadań publicznych:
1) strona internetowa Ośrodka działająca pod adresem: https://www.orpeg.pl/,
2) Biuletyn Informacji Publicznej ORPEG działający pod adresem: https://bip.orpeg.pl/ (dalej BIP ORPEG),
3) system ankiet (limesurvey) działający pod adresem: https://forms.orpeg.pl/ (kwestionariusz osobowy - ankieta rekrutacyjna do szkół w systemie kształcenia na

[4] Dz. Urz. MEN z 2011 r., Nr 1, poz. 17.
[5] Dz. Urz. MEN z 2023 r., poz. 23.
[6] Dz.U. z 2023 r. poz. 57, ze zm.
[7] Dz.U. z 2017 r. poz. 2247; rozporządzenie straciło moc z dniem 23 maja 2023 r. na podstawie art. 26 ustawy z dnia 4 kwietnia 2019 r. *o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych* (Dz.U. z 2023 r. poz. 1440).
[8] Dz.U. z 2024 r. poz. 773.
[9] Dz.U z 2018 r. poz. 180.
[10] Dz.U. z 2023 r. poz. 1440.
[11] Dz.U. z 2022 r. poz. 902.
[12] Dz.U. z 2024 r. poz. 1077.

odległość w roku szkolnym 2024/2025, dostępny pod adresem: https://forms.orpeg.pl/index.php/879978?lang=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*;
2) § 3 ust. 1 pkt 1, 2, 4-6 rozporządzenia *w sprawie sporządzania i doręczania dokumentów elektronicznych* w związku z art. 3 oraz art. 19b ust. 3 *ustawy o informatyzacji*;
3) § 5 oraz §15-18 rozporządzenia KRI z 2012 r. oraz rozporządzenie KRI z 2024 r.

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 Polskiej Edukacji za Granicą udostępnia elektroniczną skrzynkę podawczą (dalej: ESP), spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji oraz zapewnia jej obsługę.
Adres elektronicznej skrzynki podawczej ORPEG na ePUAP oraz informacja o jej udostępnieniu są zamieszczone pod adresem: https://www.orpeg.pl/epuap/.

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.*

W Biuletynie Informacji Publicznej Ośrodka Rozwoju Polskiej Edukacji za Granicą Ośrodek nie zamieścił informacji o udostępnionym adresie elektronicznej skrzynki podawczej.
Adres ESP (/Orpeg/SkrytkaESP) został zamieszczony na stronie ORPEG[13] i jest podany w formie identyfikatora URI (Uniform Resource Identifier, tłum. Ujednolicony Identyfikator Zasobów).

Brak informacji w BIP ORPEG o udostępnionym adresie ESP stanowi nieprawidłowość.

- 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*

[13] Pod adresem: https://www.orpeg.pl/epuap/.

rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż 5 megabajtów.

Podczas czynności kontrolnych stwierdzono brak na stronie BIP ORPEG informacji w zakresie maksymalnego rozmiaru dokumentu elektronicznego wraz z załącznikami, wyrażonego w megabajtach, możliwego do doręczenia za pomocą elektronicznej skrzynki podawczej.

Powyższe stanowi nieprawidłowość.

- 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 Polskiej Edukacji za Granicą nie sporządza wzorów dokumentów elektronicznych do przekazania do centralnego repozytorium (CRWDE). Na stronie ORPEG[14] zawarty jest odnośnik do Elektronicznej Platformy Usług Administracji Publicznej przekierowujący do strony: https://epuap.gov.pl/wps/portal/strefa-klienta.

W badanym zakresie nie stwierdzono nieprawidłowości.

Interoperacyjność realizowana na podstawie rozporządzenia KRI z 2012 r. i 2024 r. (dalej: rozporządzenia KRI).

- Zgodnie z § 5 ust. 2 pkt 1 ww. rozporządzeń 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 ORPEG pod adresem https://www.orpeg.pl/ksztalcenie-na-odleglosc/rekrutacja-2024-2025/ znajdują się informacje dotyczące rekrutacji uczniów do szkół w systemie kształcenia na odległość, takie jak: przebieg procesu rekrutacji wraz z oferowanymi przez szkoły w systemie kształcenia na odległość programami nauczania (pełnym i uzupełniającym), wymagana dokumentacja rekrutacyjna, w tym ankieta rekrutacyjna (kwestionariusz osobowy, rekrutacyjny) do szkół w systemie kształcenia na odległość, dostępna pod adresem: https://forms.orpeg.pl/index.php/879978?lang=pl.

System ankiet LimeSurvey służy do publikacji ankiet oraz gromadzenia i analizy odpowiedzi udzielonych przez respondentów. Ww. kwestionariusz rekrutacyjny jest dostępny przy użyciu systemu ankiet, wykorzystywany przez ORPEG przy rekrutacji do szkół kształcących na odległość, tj. do:

- Szkoły Podstawowej im. Komisji Edukacji Narodowej,
- Liceum Ogólnokształcącego im. Komisji Edukacji Narodowej

funkcjonujących w Ośrodku Rozwoju Polskiej Edukacji za Granicą.
Na stronie https://forms.orpeg.pl/ zamieszczone były informacje o sposobie dostępu oraz zakresie użytkowym serwisu ankiet.

W badanym zakresie nie stwierdzono nieprawidłowości.

[14] Pod adresem: https://www.orpeg.pl/epuap/.

- Zgodnie z § 5 ust. 2 pkt 4 ww. rozporządzeń 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*.

Na podstawie § 3 ust. 1 pkt. 4-6 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych, *podmioty publiczne informują na swoich stronach podmiotowych BIP, o:*

pkt 4 - *rodzajach informatycznych nośników danych, na których może zostać im doręczony dokument elektroniczny;*

pkt 5 - *rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru;*

pkt 6 - *innych wymaganiach określonych przepisami prawa dotyczących doręczania dokumentów elektronicznych.*

W BIP ORPEG nie zostały opublikowane procedury obowiązujące przy załatwianiu spraw drogą elektroniczną z zakresu właściwości Ośrodka. Nie zamieszczono także wymogów dla dokumentów elektronicznych dostarczanych do ORPEG wraz z rodzajami informatycznych nośników danych, na których dokument w wersji elektronicznej może zostać doręczony do Ośrodka.

Od 1 stycznia 2025 r. wszedł w życie obowiązek stosowania e-Doręczeń przez podmioty publiczne[15], wskazane w ustawie z dnia 18 listopada 2020 r. *o doręczeniach elektronicznych*[16]. Podczas kontroli stwierdzono, że na stronie BIP ORPEG pod adresem: https://bip.orpeg.pl/edoreczenia/ zostały opublikowane informacje o systemie e-Doręczenia, który ma zastąpić korespondencję przez ePUAP, w tym opublikowany został adres doręczeń elektronicznych Ośrodka.

- Zgodnie z § 5 ust. 3 pkt 3 ww. rozporządzeń 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 rozporządzeń KRI:

ust. 1. *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*.

ust. 2. *W przypadku gdy w danej sprawie brak jest przepisów, norm lub standardów, o których mowa w ust. 1, stosuje się standardy uznane na poziomie międzynarodowym, w szczególności opracowane przez:*

1) *Internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC),*
2) *World Wide Web Consortium (W3C) i publikowane w postaci W3C Recommendation (REC)*

- adekwatnie do potrzeb wynikających z realizowanych zadań oraz bieżącego stanu technologii informatycznych.

[15] Zgodnie z Komunikatem Ministra Cyfryzacji z dnia 12 lipca 2024 r. zmieniającym komunikat w sprawie określenia terminu wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym.

[16] Dz.U. z 2024 r. poz. 1045, 1841.

Wybrane do kontroli systemy informatyczne, wykorzystywane do realizacji zadań publicznych ORPEG nie wymieniają danych z zewnętrznymi systemami informatycznymi innych podmiotów publicznych.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 15 ww. rozporządzeń 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*.

W okresie objętym kontrolą w ORPEG obowiązywała umowa 24/2020/ORPEG zawarta 1 lipca 2020 r. pomiędzy Ośrodkiem a podmiotem zewnętrznym, której przedmiotem była „budowa i wdrożenie oprogramowania informatycznego pozwalającego na integrację stron internetowych ORPEG wraz ze zmianą szat graficznych”[17]. Umowa dotyczyła przeniesienia istniejącej strony internetowej Ośrodka na nowy system wraz z wykonaniem szaty graficznej, stworzenia systemu BIP jako integralnej części nowej strony ORPEG, integracji istniejącego systemu zamawiania podręczników i bazy szkół polonijnych z nową stroną ORPEG, wykonania nowej szaty graficznej dla platformy kursów on-line, przeniesienia istniejących stron internetowych Szkół Polskich na nowy system umożliwiający centralne ich zarządzanie. Przedmiot umowy został określony w opisie przedmiotu zamówienia (dalej: OPZ), stanowiącym załącznik nr 1 do ww. umowy. W OPZ określono m.in. specyfikację techniczno-funkcjonalną serwisu internetowego, zasady architektoniczne, standardy technologiczne, wymagania dla mechanizmów bezpieczeństwa oraz licencjonowania.

Strona internetowa ORPEG funkcjonuje na nowym systemie CMS[18] od 2021 r. i jest to serwis dostępny publicznie bez logowania. Na stronie Ośrodka udostępniane są podstawowe informacje o jednostce oraz informacje dotyczące: kształcenia na odległość, szkół polskich, europejskich i polonijnych, Standardów Ochrony Małoletnich, podjęcia pracy za granicą przez zainteresowanych nauczycieli, kształcenia i doskonalenia nauczycieli polonijnych oraz polskojęzycznych, projektów realizowanych w ramach FERS.

Biuletyn Informacji Publicznej ORPEG – obowiązek utworzenia urzędowego publikatora teleinformatycznego, jakim jest BIP ORPEG, wynika z przepisów art. 8 ust. 1 i 2[19] ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej*. ORPEG jako podmiot, o którym mowa w art. 4 ust. 1 pkt 5[20] 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

---

[17] § 2 ust. 1 umowy nr 24/2020/ORPEG.

[18] System zarządzania treścią (ang. content management system, CMS).

[19] 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”.

ust. 2. Informacje publiczne są udostępniane w Biuletynie Informacji Publicznej przez podmioty, o których mowa w art. 4 ust. 1 i 2.

[20] 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.

podmiotów. System ten został utworzony w 2021 r.[21], jest dostępny publicznie bez logowania.
Biuletyn Informacji Publicznej ORPEG to system, w którym są udostępniane aktualne informacje publiczne ORPEG, takie jak: ogólne informacje o jednostce (m.in. struktura organizacyjna Ośrodka, zadania Ośrodka i komórek organizacyjnych, statut, dostęp do informacji publicznej, ochrona danych osobowych), aktualne i archiwalne oferty pracy, zamówienia publiczne, dokumenty (Plany działalności Ośrodka na dany rok, sprawozdania z wykonania planu działalności Ośrodka w poszczególnych latach, informacja o prowadzonych w Ośrodku rejestrach), informacje w zakresie przyjmowania i rozpatrywania skarg i wniosków w Ośrodku, informacje w zakresie e-Doręczeń oraz dane kontaktowe.

System ankiet LimeSurvey[22] został uruchomiony w 2019 r. Jest to bezpłatne oprogramowanie (open source) przeznaczone do tworzenia i przeprowadzania różnorodnych ankiet online. *LimeSurvey* umożliwia zbieranie odpowiedzi w czasie rzeczywistym oraz ich analizę za pomocą wbudowanych narzędzi statystycznych. Wyniki można eksportować do różnych formatów (np. CSV, Excel). System może być zintegrowany z innymi narzędziami i systemami, dzięki czemu dane z ankiet mogą być wykorzystywane w innych obszarach działalności[23].

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 17 ust. 1 ww. rozporządzeń 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*.

ORPEG zawarł w dniu 1 lipca 2020 r. umowę nr 24/2020/ORPEG na „budowę i wdrożenie oprogramowania informatycznego pozwalającego na integrację stron internetowych ORPEG wraz ze zmianą szat graficznych", zgodnie z którą wykonawca umowy zobowiązał się do zmodernizowania i częściowego zintegrowania istniejących wówczas serwisów internetowych ORPEG, tj.: strony ORPEG (która ma posiadać stronę BIP spełniającą ogólnie przyjęte standardy), Podręcznika Internetowego Włącz Polskę, platformy kursów on-line dla podnoszenia kwalifikacji nauczycieli polonijnych, Portalu Polska Szkoła, stron szkół polskich[24].

Podczas kontroli ustalono, że kodowanie znaków odbywa się według standardu Unicode UTF-8 (na podstawie OPZ stanowiącego załącznik do umowy nr 24/2020/ORPEG oraz na podstawie specyfikacji systemu ankiet LimeSurvey).

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 18 ww. rozporządzeń KRI:

ust. 1. *Systemy teleinformatyczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia KRI*.

[21] Na podstawie danych zawartych w zestawieniu systemów teleinformatycznych używanych do realizacji zadań publicznych, stanowiących załącznik nr 2 do pisma ORPEG z 18.10.2024 r., znak: ORPEG-3507/2024-WA-AKa-072-72(1).
[22] Pod adresem: https://www.limesurvey.org/manual/LimeSurvey_Manual/pl dostępna jest specyfikacja systemu.
[23] Informacja ORPEG z 25 listopada 2024 r.
[24] Zgodnie z Opisem Przedmiotu Zamówienia (dalej: OPZ): *Integracja stron internetowych ORPEG wraz ze zmianą szat graficznych*, stanowiącym załącznik nr 1 do umowy.

ust. 2. *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.*

Zgodnie z warunkami technicznymi ww. umowy nr 24/2020/ORPEG system wspiera następujące typy plików: rtf, pdf, doc, docx, xls, xlsx, ppt, pptx, xml, odt, jpg, jpeg, gif, png, svg. System LimeSurvey pozwala wybrać następujące formaty wyeksportowane wyników: csv, doc, docx, xls, xlsx, xml, pdf.[25]

W badanym zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa badanego obszaru: pozytywna z nieprawidłowościami.

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

Wymogi dotyczące systemu zarządzania bezpieczeństwem informacji zostały określone w § 20 rozporządzenia KRI z 12 kwietnia 2012 r. oraz § 19 rozporządzenia KRI z 21 maja 2024 r.

- Zgodnie z § 20 ust. 1 rozporządzenia KRI z 2012 r. oraz § 19 ust. 1 rozporządzenia KRI z 2024 r. – *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 z 2012 r. oraz § 19 ust. 2 pkt 1 rozporządzenia KRI z 2024 r. – *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.*

W obszarze zarządzania bezpieczeństwem informacji w ORPEG wprowadzono zarządzenie nr 88/2021 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 30 lipca 2021 r. *w sprawie przyjęcia nowego brzmienia Polityki Bezpieczeństwa Informacji (PBI) przetwarzania danych osobowych wraz z Instrukcją Zarządzania Systemem Informatycznym w Ośrodku Rozwoju Polskiej Edukacji za Granicą w Warszawie.*
Załącznikiem nr 1 do niniejszego zarządzenia jest: *Polityka Bezpieczeństwa Informacji (PBI) Przetwarzania Danych Osobowych wraz z Instrukcją Zarządzania Systemem Informatycznym w Ośrodku Rozwoju Polskiej Edukacji za Granicą (ORPEG) w Warszawie* (dalej: Polityka Bezpieczeństwa Informacji), z następującymi załącznikami:

- załącznik 1 Wykaz organizacyjnych i technicznych środków bezpieczeństwa wdrożonych w celu ochrony danych osobowych;
- załącznik 2 Ewidencja budynków i pomieszczeń w których przetwarzane są dane osobowe;
- załącznik 3 Procedura analizy ryzyka;
- załącznik 4 Procedura oceny skutków dla ochrony danych;
- załącznik 5 Procedura szkoleń i nadawania upoważnień do przetwarzania danych osobowych;
- załącznik 6 Wzór upoważnienia do przetwarzania danych osobowych w ORPEG;
- załącznik 7 Wzór unieważnienia upoważnienia do przetwarzania danych osobowych;
- załącznik 8 Rejestr upoważnień do przetwarzania danych osobowych;

[25] https://www.limesurvey.org/manual/Export_responses/pl

- załącznik 9 Wzór wniosku o nadanie, zmianę, odebranie uprawnień w systemie informatycznym;
- załącznik 10 Rejestr osób, którym nadano uprawnienia do przewarzania danych osobowych w systemach informatycznych;
- załącznik 11 Wzór oświadczenia o znajomości przepisów i zasad ochrony danych osobowych i Polityki Bezpieczeństwa ORPEG;
- załącznik 12 Procedura postępowania w przypadku wystąpienia incydentu związanego z ochroną danych osobowych;
- załącznik 13 Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych;
- załącznik 14 Rejestr naruszeń ochrony danych osobowych;
- załącznik 15 Procedura realizacji praw osób, których dane dotyczą;
- załącznik 16 Wzór protokołu realizacji żądań osoby, której dane dotyczą;
- załącznik 17 Rejestr realizacji praw jednostki;
- załącznik 18 Wzór ogólny zgody na przetwarzanie danych osobowych;
- załącznik 19 Wzór klauzul informacyjnych;
- załącznik 20 Wzór umowy powierzenia przetwarzania danych osobowych;
- załącznik 21 Wzór ewidencji zawartych umów powierzenia przetwarzania danych osobowych/umów w ramach których powierzono przetwarzanie danych;
- załącznik 22 Wzór umowy powierzenia komputera przenośnego;
- załącznik 23 Wzór protokołu odbioru sprzętu IT;
- załącznik 24 Wzór rejestru konserwacji sprzętu;
- załącznik 25 Rejestr czynności przetwarzania danych osobowych;
- załącznik 26 Rejestr kategorii czynności przetwarzania danych osobowych.

Zgodnie z Polityką Bezpieczeństwa Informacji:

1) Inspektor Ochrony Danych (dalej: IOD) nadzoruje przestrzeganie zasad ochrony danych osobowych przetwarzanych w ORPEG, a m.in. prowadzi okresowe przeglądy stanu bezpieczeństwa i sporządza raporty wraz z zaleceniami zmian[26], monitoruje funkcjonowanie systemu zabezpieczeń, w tym także prowadzenie ewidencji z zakresu ochrony danych osobowych[27];
2) obowiązki Administratora Systemów Informatycznych (dalej: ASI) obejmują w szczególności przegląd, konserwacje oraz uaktualnienie systemów służących do przetwarzania danych[28];
3) Administrator Danych Osobowych (dalej: ADO) realizuje zadania w zakresie ochrony danych osobowych, w tym m.in.: wdraża odpowiednie środki techniczne i organizacyjne, zgodne z RODO, które poddawane są przeglądom i są uaktualniane[29].

W załączniku nr 2 do Polityki Bezpieczeństwa Informacji pn. „*Ewidencja budynków i pomieszczeń, w których przetwarzane są dane osobowe*", określono m.in. zabezpieczenia fizyczne poszczególnych pomieszczeń użytkowanych przez komórki organizacyjne Ośrodka. Dokument ten odnosi się do pomieszczeń i sposobu ich zabezpieczeń poprzedniej siedziby Ośrodka przy ul. Kieleckiej 43 w Warszawie.
Od dnia 1 października 2022 r. siedziba Ośrodka Rozwoju Polskiej Edukacji za Granicą mieści się przy ul. Wołoskiej 5 w Warszawie. ORPEG nie zaktualizował procedur w zakresie bezpieczeństwa fizycznego pomieszczeń w związku ze zmianą siedziby Ośrodka.

Instrukcja Zarządzania Systemem Informatycznym w Ośrodku Rozwoju Polskiej Edukacji za Granicą (dalej: Instrukcja zarządzania SI, Instrukcja) – zawarta w pkt 14 ww. Polityki Bezpieczeństwa Informacji, określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych przez ADO, w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom

[26] 3.3.1. pkt 5 Polityki Bezpieczeństwa Informacji.
[27] 3.3.1. pkt 9 Polityki Bezpieczeństwa Informacji.
[28] 3.4.1. pkt 7 lit. a Polityki Bezpieczeństwa Informacji.
[29] 4.1. pkt 1 Polityki Bezpieczeństwa Informacji.

nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem[30]. Instrukcja ta określa zasady i tryb wykonywania czynności w Systemie informatycznym ORPEG związanym z ochroną danych osobowych (pkt 14.3. Instrukcji).

Podczas kontroli ustalono, że ww. Polityka Bezpieczeństwa Informacji w ORPEG dotyczy wyłącznie zakresu ochrony danych osobowych.

W wyjaśnieniach z 26 lutego 2025 r. Ośrodek poinformował, że: „w ORPEG nie została wdrożona procedura dotycząca zapewnienia odpowiedniej ochrony aktywów informacyjnych Ośrodka".
Następnie w uzupełnieniu[31] do powyższej informacji wyjaśniono, że: „(…) ORPEG rozpoczął prace nad opracowaniem i wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji w naszej jednostce. Zakończyliśmy proces wyboru wykonawcy, który wesprze nas w stworzeniu kompleksowego zbioru zasad, procesów i technologii mających na celu ochronę informacji przed potencjalnymi zagrożeniami. (…)".
Ośrodek poinformował, że trwają uzgodnienia warunków umowy z wykonawcą.

Ograniczenie Polityki Bezpieczeństwa Informacji w ORPEG wyłącznie do przepisów odnoszących się do tematyki ochrony danych osobowych stanowi nieprawidłowość.

- Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 2 rozporządzenia KRI z 2024 r. – *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

W okresie objętym kontrolą w ORPEG, w zakresie przeprowadzania inwentaryzacji składników majątkowych Ośrodka, obowiązywały następujące regulacje wewnętrzne:

1) zarządzenie nr 48/2018 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 8 listopada 2018 r. *w sprawie: wprowadzenia Instrukcji obiegu i kontroli dokumentów finansowo-księgowych w Ośrodku Rozwoju Edukacji Polskiej za Granicą;* załącznik nr 5 – *Instrukcja inwentaryzacji majątku Jednostki;*
2) zarządzenie nr 138/2024 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 11 września 2024 r. *w sprawie zmiany zarządzenia nr 48/2018 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 8 listopada 2018 r. w sprawie wprowadzenia Instrukcji obiegu i kontroli dokumentów finansowo-księgowych w Ośrodku Rozwoju Edukacji Polskiej za Granicą;* załącznik nr 1 – *Instrukcja inwentaryzacji majątku Jednostki;*
3) zarządzenie nr 142/2024 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 25 września 2024 r. *w sprawie przeprowadzenia inwentaryzacji wszystkich składników majątkowych w Ośrodku Rozwoju Edukacji Polskiej za Granicą;*
4) zarządzenie nr 143/2024 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 30 września 2024 r. *w sprawie zmiany zarządzenia nr 142/2024 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 25 września 2024 r. w sprawie w sprawie przeprowadzenia inwentaryzacji wszystkich składników majątkowych w Ośrodku Rozwoju Edukacji Polskiej za Granicą*, - zarządzeniem rozszerzono skład komisji inwentaryzacyjnej o zespoły spisowe.

W ww. *Instrukcji inwentaryzacji majątku Jednostki* zostały określone terminy i częstotliwość przeprowadzania inwentaryzacji, zgodnie z którymi inwentaryzacja środków trwałych znajdujących się na terenie strzeżonym jest dokonywana raz w ciągu 4 lat, w terminie na

[30] Cel stosowania instrukcji wskazany w pkt 14.1.1. Instrukcji zarządzania SI.
[31] Korespondencja mailowa z 28 lutego 2025 r.

ostatni dzień roku obrotowego z możliwością przeprowadzenia spisu w okresie czwartego kwartału roku obrotowego oraz 15 dni następnego roku obrotowego[32].

Inwentaryzacja w OPREG została przeprowadzona w 2020 r.; następna została rozpoczęta we wrześniu 2024 r. Ośrodek przedstawił dokument pn. „Obowiązujący wykaz sprzętu i oprogramowania w ORPEG" sporządzony podczas inwentaryzacji przeprowadzonej w 2020 roku, w którym wykazane zostały zinwentaryzowane sprzęty i oprogramowania wchodzące w skład majątku Ośrodka.

Zgodnie z zapisami Polityki Bezpieczeństwa Informacji (pkt 3.2.2.) ADO może powołać ASI, zarządzającego oprogramowaniem, który przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania.
ASI realizuje zadania w zakresie odpowiedzialności za funkcjonowanie systemu informatycznego oraz odpowiada za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, w szczególności inwentaryzuje sprzęt i oprogramowanie informatyczne[33].
Administratorem Danych Osobowych jest ORPEG, reprezentowany przez Dyrektora jednostki. Administratorem Systemów Informatycznych w ORPEG jest specjalista ds. systemów informatyczno-administracyjnych sieci, będący pracownikiem Wydziału Informatycznego, którego jednym z podstawowych obowiązków jest administrowanie siecią informatyczną[34].

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 3 rozporządzenia KRI z 2024 r. – *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*.
- *Zgodnie z § 20 ust. 4 rozporządzenia KRI z 2012 r. oraz § 19 ust. 4 rozporządzenia KRI z 2024 r. – niezależnie od zapewnienia przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*

Załącznikiem nr 3 do Polityki Bezpieczeństwa Informacji w ORPEG jest *Procedura Analizy Ryzyka*, opisująca metodykę analizy ryzyka danych osobowych, w celu określenia rekomendowanych minimalnych poziomów bezpieczeństwa danych[35]. W *Procedurze Analizy Ryzyka* opisane zostały działania wynikające z realizacji procesu zarządzania ryzykiem w ochronie danych osobowych, w tym ocena ryzyka bezpieczeństwa informacji, w ramach której należy przeprowadzić[36]:

a) identyfikację zagrożeń bezpieczeństwa informacji,
b) identyfikację podatności zasobów,
c) określenie istotności aktywów uczestniczących w przetwarzaniu danych osobowych,
d) określenie powagi podatności dla zasobów,

[32] § 5 ust. 1 pkt 1 lit. a Instrukcji inwentaryzacji majątku Jednostki będącej załącznikiem nr 5 do zarządzenia nr 48/2018 oraz załącznikiem nr 1 do zarządzenia nr 138/2024.
[33] 3.4.2. pkt 13 Polityki Bezpieczeństwa Informacji.
[34] Na podstawie zakresu obowiązków pracownika (sygn. nr ORPEG-464/2015/WFK-EK-11-6(15a) z 17 lutego 2015 r.).
[35] Pkt 1.1. Postanowienia ogólne *Procedury Analizy Ryzyka*.
[36] Krok 5 w Opisie procesu zarządzania ryzykiem, działanie pn. „Ocena ryzyka bezpieczeństwa informacji".

e) ocenę skutków urzeczywistnienia się zagrożeń bezpieczeństwa informacji,
f) ocenę prawdopodobieństwa urzeczywistnienia się zagrożenia bezpieczeństwa informacji,
g) ocenę powagi ryzyka bezpieczeństwa informacji".

W ww. *Procedurze* wskazano, że „w wyniku przeprowadzonej oceny ryzyka może zaistnieć potrzeba ustanowienia/zmodyfikowania lub zmiany dotychczasowych stosowanych zabezpieczeń organizacyjnych lub/i technicznych w organizacji" (pkt 6. Wyniki analizy ryzyka).
Zgodnie z *Procedurą Analizy Ryzyka*, przegląd ryzyka powinien być dokonywany przynajmniej raz w roku, a „każdy taki przegląd winien być dla celów dowodowych utrwalony w formie pisemnego raportu zawierającego – w razie wystąpienia – informacje o nieprawidłowościach czy słabościach przyjętych rozwiązań i mechanizmów" (pkt 10 - Zarządzanie ryzykiem).

Zgodnie z zapisami Polityki Bezpieczeństwa Informacji:
- ADO dokonuje cyklicznej (nie rzadziej niż raz do roku) analizy ryzyka dla zasobów biorących udział w przetwarzaniu danych (pkt 7.1.);
- ADO cyklicznie (nie rzadziej niż raz na rok) przeprowadza ocenę skutków dla ochrony danych osobowych oraz analizę ryzyka i plan postepowania z ryzykiem dla wszystkich procesów oraz wszystkich produktów/usług w ORPEG (pkt 9.3.).

W Polityce Bezpieczeństwa Informacji określono zadania ADO, który: „wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą. Środki te są uwzględniane przy określaniu sposobów przetwarzania oraz w czasie samego przetwarzania, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania." (pkt 4.1.3.).

W okresie objętym kontrolą w ORPEG nie przeprowadzano określonych w ww. § 20 ust. 2 pkt 3 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 3 rozporządzenia KRI z 2024 r. okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. ORPEG nie przeprowadzał analizy ryzyka danych osobowych wskazanej w Polityce Bezpieczeństwa Informacji - nie przedstawiono pisemnego raportu.

Powyższe stanowi nieprawidłowość.

- Zgodnie z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 4 i 5 rozporządzenia KRI z 2024 r. – *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:*

pkt 4 - *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;*
pkt 5 - *bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

W Polityce Bezpieczeństwa Informacji została opisana procedura nadawania i cofania uprawnień w systemie informatycznym, zgodnie z którą „konta użytkowników systemu informatycznego tworzy oraz usuwa ASI na wniosek kierownika komórki organizacyjnej ORPEG, na podstawie zgody ADO."[37]. Uprawnienia w systemie informatycznym nadaje ASI,

[37] Pkt 14.5.1 Polityki Bezpieczeństwa Informacji.

lub inne upoważnione do tego osoby[38]. Wzór wniosku o nadanie, zmianę, odebranie uprawnień w systemie informatycznym stanowi załącznik nr 9 do Polityki Bezpieczeństwa Informacji.
Zgodnie z zapisami w Polityki Bezpieczeństwa Informacji do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. (…) Podpisany dokument jest dołączany do akt osobowych pracownika (pkt 6.6.1.3.).

W przypadku cofnięcia upoważnienia do korzystania z systemu informatycznego (w tym cofnięcia upoważnienia do przetwarzania danych osobowych)[39]:

a) kierownik wydziału/Dyrektor ORPEG w stosunku do pracowników na samodzielnych stanowiskach w ORPEG zobowiązany jest powiadomić o tym IOD oraz wypełnić wniosek o odebranie uprawnień i przekazać go ASI lub innej osobie wyznaczonej przez ADO;
b) wydział Informatyczny umieszcza informację o cofnięciu upoważnienia w ewidencji upoważnień do przetwarzania danych osobowych w systemach informatycznych;
c) ASI unieważnia bądź zablokowuje identyfikator i hasło wyrejestrowanego użytkownika oraz podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

W ORPEG prowadzony jest rejestr upoważnień do przetwarzania danych osobowych (załącznik nr 8 do Polityki Bezpieczeństwa Informacji) oraz rejestr osób, którym nadano uprawnienia do przetwarzania danych osobowych w systemach informatycznych (załącznik nr 10 do Polityki Bezpieczeństwa Informacji). Oba rejestry ewidencjonują następujące dane: imię i nazwisko osoby upoważnionej, data nadania i ustania uprawnień oraz ich zakres (numer zbioru), a w przypadku kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępowy do tego programu.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 6 rozporządzenia KRI z 2024 r. – *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.

Zgodnie z pkt 6.6.1 ppkt 5 i 6 Polityki Bezpieczeństwa Informacji każdy pracownik ORPEG co najmniej raz na rok musi odbyć szkolenie z zakresu ochrony danych osobowych. Za organizację szkoleń odpowiedzialny jest IOD. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych (szkolenie wstępne z ochrony danych osobowych). Procedura szkoleń i nadawania upoważnień stanowi Załącznik nr 5 do Polityki Bezpieczeństwa Informacji. Ponadto każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z Polityką Bezpieczeństwa Informacji i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi załącznik nr 11. Podpisany dokument jest dołączany do akt osobowych.

W ORPEG została opracowana *Procedura szkoleń i nadawania upoważnień do przetwarzania danych osobowych* stanowiąca załącznik nr 5 do Polityki Bezpieczeństwa Informacji.

[38] Pkt 14.5.4 Polityki Bezpieczeństwa Informacji.
[39] Pkt 14.5.8 Polityki Bezpieczeństwa Informacji.

Z zakresu ochrony danych osobowych w ORPEG w 2023 r. przeszkolono 30 osób[40], a w 2024 r. – 10 osób[41]. Zakres przeprowadzanego w latach 2023-2024 szkolenia pn. „Ochrona danych osobowych w Ośrodku Rozwoju Polskiej Edukacji za Granicą oraz w sektorze oświaty" obejmował w szczególności następujące zagadnienia[42]:

- zasady i podstawy prawne przetwarzania danych osobowych;
- transfer danych poza UE,
- obowiązek poufności — *Prawo oświatowe*;
- obowiązki wynikające z RODO;
- bezpieczeństwo przetwarzania danych osobowych — środki techniczne i organizacyjne, zasady opisane w Polityce oraz dobre praktyki (dane przetwarzane w formie i elektronicznej), podstawowe zagrożenia oraz stosowane środki zaradcze;
- odpowiedzialność i naruszenia ochrony danych, obowiązki pracownika i Administratora;
- zadania i rola organu nadzorczego — UODO, zadania Inspektora Ochrony Danych.

Ponadto pracownicy Wydziału Informatycznego ORPEG w okresie objętym kontrolą brali udział w nw. szkoleniach specjalistycznych[43]:

- szkolenie z kontroli dostępu – PRMaster („szkolenie dotyczyło zasad zarządzania uprawnieniami dostępu do systemów informatycznych, w tym konfiguracji i nadzorowania dostępu użytkowników do zasobów organizacji; omówiono mechanizmy autoryzacji, metody uwierzytelniania oraz procedury kontroli logowania w systemie PRMaster") [44];
- szkolenie dla Trenerów – e-Doręczenia („tematem szkolenia była usługa rejestrowanego doręczenia elektronicznego (…), jej zastosowanie oraz aspekty prawne i organizacyjne, (…) bezpieczeństwo przesyłanych danych, zgodność z regulacjami RODO oraz metody weryfikacji tożsamości nadawców i odbiorców") [45];
- szkolenie Microsoft: Implement and Manage Microsoft Intune („szkolenie obejmowało wdrażanie i zarządzanie usługą Microsoft Intune, która umożliwia kompleksowe zabezpieczenie i zarządzanie urządzeniami w organizacji; omówiono polityki bezpieczeństwa, ochronę danych, kontrolę dostępu oraz monitorowanie zgodności urządzeń z wymaganiami organizacyjnymi") [46].

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 7, 9 i 11 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 7, 9 i 11 rozporządzenia KRI z 2024 r. – *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:*

pkt 7 - *zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:*

a) monitorowanie dostępu do informacji,

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

[40] Ustalenie na podstawie listy obecności osób uczestniczących w szkoleniu z ochrony danych osobowych, które odbyło się 13 marca 2023 r.

[41] Ustalenie na podstawie listy obecności osób uczestniczących w szkoleniu z ochrony danych osobowych, które odbyło się 11 kwietnia 2024 r.

[42] Zakres szkolenia został wskazany na certyfikatach o ukończeniu szkolenia.

[43] Wyjaśnienia ORPEG z 28 lutego 2025 r.

[44] Szkolenie odbyło się 20 września 2023 r.

[45] Szkolenie odbyło się 26 września 2023 r.

[46] Szkolenie odbyło się 30 września – 2 października 2024 r.

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

pkt 9 - *zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;*

pkt 11 - *ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*

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

ORPEG w wyjaśnieniach z 28 lutego 2025 r. wskazał, że „serwerownia została wyposażona w szereg zabezpieczeń, które mają na celu zapewnienie zarówno fizycznej ochrony infrastruktury IT, jak i bezpieczeństwa dostępu dla upoważnionych osób. (…)" Elementami systemu ochrony ww. serwerowni są: monitoring wizyjny, system kontroli dostępu, ograniczony dostęp osób uprawnionych, klimatyzacja, gaśnica do gaszenia elektroniki, drzwi przeciwpożarowe.
W wyniku oględzin pomieszczenia serwerowni ustalono, że w Ośrodku zapewniono odpowiednie rozwiązania w zakresie zabezpieczenia serwerowni.

Zgodnie z pkt 3.4.2. ppkt 10-12 Polityki Bezpieczeństwa Informacji ASI zapewnia dostęp do systemu informatycznego wyłącznie użytkowników posiadających wymagane uprawnienia oraz odpowiednie i ważne poświadczenia bezpieczeństwa, przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki oraz prowadzi wykaz osób mających dostęp do systemu informatycznego.

W Polityce Bezpieczeństwa Informacji określone zostały obowiązki osoby przetwarzającej dane osobowe w ORPEG (pkt 3.5.1.10 – 3.5.1.20).

W *Instrukcji Zarządzania Systemem Informatycznym w ORPEG* (Instrukcja zawarta w pkt 14 ww. Polityki Bezpieczeństwa Informacji) określono *Procedury tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych w systemie informatycznym* (pkt 14.8. Instrukcji). Zgodnie z tą procedurą za sporządzanie kopii zapasowych systemów informatycznych i danych znajdujących się na serwerach odpowiedzialni są pracownicy Wydziału Informatycznego wyznaczeni przez ADO oraz inne osoby wyznaczone przez ADO (pkt.14.8.11 Instrukcji).
W Instrukcji wprowadzono także *Procedurę określająca metody i częstotliwość sprawdzania obecności szkodliwego/złośliwego oprogramowania służącego do uszkodzenia, przejęcia danych lub kontroli nad systemem informatycznym przez osobę nieupoważnioną* (pkt 14.10 Instrukcji), zgodnie z którą w celu zabezpieczenia systemu informatycznego przed atakami szkodliwego/złośliwego oprogramowania ASI wdraża:

a) identyfikację i uwierzytelniania użytkowników uzyskujących dostęp do systemu poprzez kontrolę praw dostępu do zasobów systemu informatycznego;
b) rejestrację informacji o dostępach lub próbach dostępu do zasobów i usług systemu;
c) rejestrację i śledzenie komunikatów o błędach w pracy systemów informatycznych.

Zasady zabezpieczenia dostępu do zasobów ORPEG zlokalizowanych w kolokacji zarządzanej przez firmę zewnętrzną określono w zawartych umowach nr 122/2022/ORPEG i umowa nr 97/2023/ORPEG z dostawcą usługi kolokacji, zobowiązujące wykonawcę usługi w szczególności do:

- zapewnienia warunków eksploatacji urządzeń przekazanych przez Zamawiającego, w tym pomieszczenia o odpowiedniej kubaturze z chronionym dostępem, zasilaniem energetycznym i warunkami klimatycznymi dla ciągłej pracy serwerów;
- zabezpieczenia sieciowego umożliwiającego blokowanie niepożądanego ruchu przychodzącego z sieci Internet;
- zapewnienia bezpieczeństwa fizycznego i środowiska.

W ORPEG prowadzona jest również kontrola dostępu fizycznego, określona w zawartej 2 czerwca 2022 r. umowie najmu powierzchni biurowej pomiędzy Ośrodkiem (najemcą) a Wynajmującym będącym właścicielem budynków mieszczących się przy ul. Wołoskiej 5. W regulaminie nieruchomości, stanowiącym załącznik do ww. umowy wskazano, że wejścia do budynku są dostępne za pomocą kart dostępu wydawanych przez Biuro Zarządcy Nieruchomości.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 8 rozporządzenia KRI z 2024 r. – *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.*

W *Procedurze określającej metody i częstotliwość sprawdzania obecności szkodliwego/złośliwego oprogramowania służącego do uszkodzenia, przejęcia danych lub kontroli nad systemem informatycznym przez osobę nieupoważnioną* określono obowiązek stosowania na komputerach stacjonarnych, serwerach i urządzeniach mobilnych programów antywirusowych oraz programów przeciwdziałających oprogramowaniu służącemu do przejęcia danych lub kontroli nad systemem informatycznym przez osobę nieuprawnioną (pkt 14.10.4 Instrukcji).

W pkt 14.14. Instrukcji określono *Pozostałe zasady funkcjonowania systemów informatycznych*, gdzie wskazano, m.in., że:

- podczas przekazywania danych osobowych za pomocą urządzeń teletransmisji danych użytkownik powinien (pkt. 14.14.2 Instrukcji):
  a) zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym w postaci np. identyfikatora i hasła, szyfrowania przesyłanych danych,
  b) zapewnić kontrolę nad tym, jakie dane, kiedy i przez kogo zostały wprowadzone oraz komu są przekazywane;
- udostępnianie zasobów może odbywać się tylko i wyłącznie w sieciach zabezpieczonych sprzętową lub programową zaporą ogniową (firewall) przed dostępem do publicznej sieci telekomunikacyjnej (pkt 14.14.6 Instrukcji);
- w przypadku zdalnego dostępu do systemu i danych lub przesyłania tych danych w publicznej sieci telekomunikacyjnej, należy stosować kryptograficzne środki ochrony wobec danych wykorzystywanych do uwierzytelnienia poprzez VPN (pkt 14.14.7 Instrukcji);
- użytkownik komputera przenośnego zawierającego dane osobowe zobowiązany jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania, w tym zobowiązany jest stosować kryptograficzne środki ochrony wobec wszystkich przetwarzanych danych osobowych (pkt 14.14.8 Instrukcji).

Zarządzeniem nr 38/2024 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 9 kwietnia 2024 r. *w sprawie Regulaminu pracy zdalnej w Ośrodku Rozwoju Polskiej Edukacji za Granicą* (dalej: Regulamin pracy zdalnej) ustalono zasady wykonywania pracy zdalnej obowiązujące w ORPEG, zgodnie z którymi pracownik zobowiązany jest w szczególności (§ 4 ust. 7 Regulaminu pracy zdalnej):

1) bezpiecznie użytkować powierzony mu sprzęt, tj. zgodnie z jego przeznaczeniem i instrukcjami wydanymi przez producenta tego sprzętu;

2) bezpiecznie przechowywać sprzęt, tj. zabezpieczając go przed mechanicznym uszkodzeniem (...), a także przed dostępem jakichkolwiek osób trzecich (...) do sprzętu oraz jakichkolwiek informacji w nim zapisanych lub utrwalonych (...).

Zgodnie z zapisami Regulaminu pracy zdalnej rozpoczęcie wykonywania pracy zdalnej może nastąpić po złożeniu przez pracownika oświadczenia o zapoznaniu się z treścią Regulaminu i zobowiązaniu się do przestrzegania regulacji zawartych w Regulaminie (§ 3 ust. 12 Regulaminu pracy zdalnej).

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 10 rozporządzenia KRI z 2024 r. – *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.*

Kontrolą objęto następujące umowy z dostawcami:
- umowa nr 24/2020/ORPEG zawarta 1 lipca 2020 r. na budowę i wdrożenie oprogramowania informatycznego pozwalającego na integrację stron internetowych ORPEG wraz ze zmianą szat graficznych,
- umowa nr 122/2022/ORPEG zawarta 21 grudnia 2022 r. na świadczenie usługi wynajmu przestrzeni w serwerowni i udostępnianie infrastruktury niezbędnej do pracy serwerów i innych urządzeń zwaną „usługą kolokacji",
- umowa nr 97/2023/ORPEG zawarta 13 grudnia 2023 r. na świadczenie usługi wynajmu przestrzeni w serwerowni i udostępnianie infrastruktury niezbędnej do pracy serwerów i innych urządzeń zwaną „usługą kolokacji".

W umowach tych zawarto zapisy dotyczące zapewnienia bezpieczeństwa informacji.

Opis przedmiotu zamówienia stanowiący załącznik nr 1 do umowy nr 24/2020/ORPEG określa wymogi bezpieczeństwa systemu CMS służącego do zarządzania stroną internetową ORPEG takie jak:
- częstotliwość tworzenia kopii zapasowych serwisu;
- wyposażenie w narzędzia do blokowania ataków typu Brute Force;
- zapewnienie bezpieczeństwa nad niepowołanym dostępem z zewnątrz i nieuprawnioną manipulacją danych.

W ramach umów nr 122/2022/ORPEG i nr 97/2023/ORPEG Wykonawca usług kolokacji był zobowiązany m.in. do opracowania i wdrożenia procedur bezpieczeństwa.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 13 rozporządzenia KRI z 2024 r. – *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.*

Według zapisów załącznika A normy PN-EN ISO/IEC 27001 należy zidentyfikować informacje[47], aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów[48]. Informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację[49].
Zgodnie z definicją incydentu określoną w art. 2 ust. 5 ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*[50] - incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.
Przez incydent związany z bezpieczeństwem informacji, zgodnie z normą PN-ISO/IEC 27001, 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 ma na celu zapewnienie szybkiej reakcji i podjęcie odpowiednich działań.

W Polityce Bezpieczeństwa Informacji, w pkt 12. *Zarządzanie incydentami*, określono zasady zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu, zgodnie z którymi IOD zgłaszając ADO naruszenie sporządza raport naruszenia ochrony danych osobowych, którego wzór stanowi załącznik nr 13 do Polityki Bezpieczeństwa Informacji (pkt 12.1.4.); ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze oraz prowadzi rejestr naruszeń ochrony danych osobowych (stanowiący załącznik nr 14 do Polityki Bezpieczeństwa Informacji).

W załączniku nr 12 Polityki Bezpieczeństwa Informacji określono *Procedurę postępowania w przypadku wystąpienia incydentu związanego z ochroną danych osobowych*.

W ORPEG został określony sposób zgłaszania wyłącznie incydentów naruszenia bezpieczeństwa danych osobowych, co stanowi nieprawidłowość.

- Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 14 rozporządzenia KRI z 2024 r. – *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj.*

[47] 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.
[48] Pkt A.8.1.1.
[49] Pkt A.8.2.1.
[50] Dz.U. z 2024 r. poz. 1077.

zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.[51]

W *Procedurze Analizy Ryzyka* stanowiącej załącznik nr 3 do Polityki Bezpieczeństwa Informacji, w pkt 6. *Wynik analizy ryzyka* określono, że wyniki przeprowadzonej analizy ryzyka mogą doprowadzić do konieczności podjęcia działań m.in. „przeprowadzenia kontroli lub/i audytów wewnętrznych, zewnętrznych w organizacji lub w podmiotach, którym powierzono lub planowane jest powierzenie przetwarzania danych osobowych.".

W wyjaśnieniach ORPEG z 4 grudnia 2024 r. wskazano, że w 2023 roku nie był przeprowadzany audyt wewnętrzny w zakresie bezpieczeństwa informacji. W 2024 roku przeprowadzono audyt pn. „Wybrane zagadnienia w obszarze zarządzania ciągłością działania jednostki (bezpieczeństwo informacji)"[52].

W 2023 roku w ORPEG nie zapewniono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, co stanowi nieprawidłowość.

- Zgodnie z § 20 ust. 2 pkt 12 lit. a-d, h rozporządzenia KRI z 2012 r. oraz § 19 ust. 2 pkt 12 lit. a-d, h rozporządzenia KRI z 2024 r. – *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. 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,
(...)
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

---

[51] 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 w 2014 roku 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* „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 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*. (...) 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."
Źródło: 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

[52] Na podstawie *Sprawozdania z prowadzenia audytu wewnętrznego za rok 2024* z dnia 30 stycznia 2025 r.

Zgodnie z Polityką Bezpieczeństwa Informacji w ORPEG:

- ADO jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (pkt. 3.2.1.);
- IOD prowadzi kontrolę zgodności działań z zakresu ochrony danych osobowych z obowiązującymi przepisami prawa (pkt 3.3.1.3.);
- ASI utrzymuje zgodność konfiguracji i parametrów systemu informatycznego z dokumentacją bezpieczeństwa systemu (pkt 3.4.2.6.), systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń i poprawność działania systemu informatycznego (pkt 3.4.2.7.) oraz odpowiada za nadzór nad aktualizacją programów antywirusowych (14.10.5 Instrukcji Zarządzania Systemem Informatycznym).

W Instrukcji Zarządzania Systemem Informatycznym w ORPEG zawarto m.in.:

- częstotliwość tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do ich przetwarzania (pkt 14.8.5.);
- wymóg okresowego sprawdzania pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu (14.8.13a);
- wymóg stosowania środków ochrony kryptograficznej przed dostępem osób nieupoważnionych (14.8.12.).

Strona internetowa ORPEG i Biuletyn Informacji Publicznej ORPEG mają określone[53] wymogi bezpieczeństwa systemu CMS, który:

- posiada zainstalowany certyfikat SSL[54];
- w razie dostępności, pozwala na samodzielną aktualizację systemu i wtyczek/modułów;
- pozwala na podłączenie narzędzia pingującego stronę i sprawdzającego czy działa;
- może stosować protokoły zapewniające poufność przesyłanych informacji z wykorzystaniem kryptograficznych metod ochrony[55].

W umowie nr 24/2020/ORPEG oraz załączniku nr 1 do umowy (Opis Przedmiotu Zamówienia: Integracja stron internetowych ORPEG wraz ze zmianą szat graficznych) określone zostały m.in. wymagania SLA[56], zapewniające odpowiedni poziom usług informatycznych w zakresie poprawnego i nieprzerwanego działania systemów oraz zapewniające świadczenie dodatkowych usług wspomagających korzystanie z systemów w tym: przyjmowanie zgłoszeń o błędach systemu, raportowanie zgłoszeń wraz z danymi pozwalającymi m.in. na śledzenie czasu ich usunięcia, a w szczególności czasu reakcji oraz czasu naprawy i usuwanie błędów.

W ramach umów nr 122/2022/ORPEG i nr 97/2023/ORPEG na usługi kolokacji serwerowni ORPEG, zostały określone podstawowe parametry SLA, m.in. takie jak: gwarantowany przez

[53] Ustalenie na podstawie opisu przedmiotu zamówienia stanowiącego załącznik nr 1 do umowy nr 24/2020/ORPEG *na budowę i wdrożenie oprogramowania informatycznego pozwalającego na integrację stron internetowych ORPEG wraz ze zmianą szat graficznych.*

[54] SSL (ang. Secure Socket Layer) to protokół sieciowy, który stał się powszechnie przyjętym standardem szyfrowania danych w Internecie. Umożliwia nawiązywanie bezpiecznych połączeń pomiędzy przeglądarką internetową, a serwerem na którym znajduje się strona internetowa. Zapewnia tym samym poufność wszystkim przesyłanym w obie strony informacjom.

[55] W przypadku przesyłania haseł przez sieci teleinformatyczne.

[56] SLA (ang. Service Level Agreement) – 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.

Wykonawcę poziom dostępności wszystkich serwerów ORPEG, określone czasy przestojów w związku z zaplanowanymi działaniami serwisowymi, czas reakcji w przypadku wystąpienia jakiejkolwiek awarii, funkcjonowanie Asysty Technicznej. W ww. umowach wskazano sposób zgłaszania awarii, czas na odtworzenie stanu poprawnego działania systemu po zgłoszeniu awarii, kary umowne za niedotrzymanie warunków dotyczących dostępności: zasilania, usług telekomunikacyjnych z protekcją, dostępu zdalnego, wszystkich powierzonych serwerów.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 21 rozporządzenia KRI z 2012 r. oraz § 20 rozporządzenia KRI z 2024 r.:

ust. 2. – *W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:*
1) *systemu z uprawnieniami administracyjnymi;*
2) *konfiguracji systemu, w tym konfiguracji zabezpieczeń;*
3) *przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa*.

ust. 3. – *Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:*
1) *działań użytkowników nieposiadających uprawnień administracyjnych*,
2) *zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu*,
3) *zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny*

- w zakresie wynikającym z analizy ryzyka.

ust. 4. - *Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata*.

W załączniku nr 12 do Polityki Bezpieczeństwa Informacji określona została *Procedura postępowania w przypadku wystąpienia incydentu związanego z ochroną danych osobowych*, w której w części Postępowanie z incydentami (pkt 3b) zawarto, że „Gromadzenie materiału dowodowego dla dokumentów na nośnikach komputerowych zaleca się utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię)".

Strona internetowa ORPEG i Biuletyn Informacji Publicznej ORPEG
W umowie oraz OPZ[57] określono m.in.:
- dostęp do systemów i przetwarzanych w nich informacji (odpowiednie zasady kontroli, zasada minimalnych uprawnień w przyznawaniu dostępu, indywidualne traktowanie każdego przypadku);
- stosowanie unikalnych identyfikatorów i haseł jako podstawowego środka uwierzytelniania (hasła muszą spełniać określone wymagania, hasła nie podlegają udostępnieniu);
- konieczność wykonywania na bieżąco kopii zapasowych danych;

[57] Ustalenie na podstawie opisu przedmiotu zamówienia stanowiącego załącznik nr 1 do umowy nr 24/2020/ORPEG *na budowę i wdrożenie oprogramowania informatycznego pozwalającego na integrację stron internetowych ORPEG wraz ze zmianą szat graficznych.*

– stosowanie rozwiązań mających włączone mechanizmy monitorowania i rejestrowania zdarzeń pozwalających na zachowanie jednoznaczności operacji i identyfikację procesu lub użytkownika wykonującego istotne dla działania systemu lub jego bezpieczeństwa operacje.

System ankiet LimeSurvey
Jest bezpłatnym oprogramowaniem typu open source przeznaczonym do tworzenia i przeprowadzania ankiet online. Na stronie[58] zamieszczone zostały informacje o wprowadzonych zmianach do kolejnych wersji systemu (aktualizacjach), w tym o dodaniu nowych funkcji czy naprawieniu błędów.

W badanym zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa badanego obszaru: pozytywna z nieprawidłowościami.

III. Zapewnienie dostępności informacji zawartych na stronie internetowej dla osób niepełnosprawnych.

Wszystkie strony internetowe i aplikacje mobilne podmiotów publicznych muszą być dostępne cyfrowo, co wynika z ustawy z 4 kwietnia 2019 r. *o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.*
Ustawa o dostępności cyfrowej określa m.in.:
1) wymagania dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;
2) wymagania dotyczące treści, przeglądu i aktualizacji deklaracji dostępności stron internetowych i aplikacji mobilnych podmiotów publicznych oraz ich publikacji.

W okresie objętym kontrolą obowiązywało 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;* rozporządzenie straciło moc z dniem 23 maja 2024 r.
Zgodnie z § 19 ww. rozporządzenia 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 - *Wymagania Web Content Accessibility Guidelines (WCAG 2.0) dla systemów teleinformatycznych w zakresie dostępności dla osób niepełnosprawnych.*
WCAG stanowią wytyczne dotyczące dostępności treści internetowych. Wytyczne te wyjaśniają, jak tworzyć strony internetowe i aplikacje, aby udostępnić je osobom z niepełnosprawnościami. Strony internetowe i aplikacje mobilne, które spełniają wytyczne WCAG, nazywa się dostępnymi cyfrowo. Obwiązującą wersją jest WCAG 2.1.

Z dniem 23 maja 2024 r. weszło w życie rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.* W rozporządzeniu tym usunięto wymagania cyfrowej dostępności - są one zawarte w ustawie o dostępności cyfrowej.

Zgodnie z ustawą o dostępności cyfrowej podmiot publiczny:
– zapewnia dostępność cyfrową przez spełnienie przez jego stronę internetową, zarządzane elementy strony internetowej, jego aplikację mobilną lub zarządzane elementy aplikacji mobilnej wymagań określonych w załączniku do ustawy – załącznik: *Wytyczne dla dostępności treści internetowych 2.1 stosowane do stron*

[58] Pod adresem: https://github.com/LimeSurvey/LimeSurvey/blob/master/docs/release_notes.txt

internetowych i aplikacji mobilnych w zakresie dostępności dla osób niepełnosprawnych (art. 5 ust. 1 ww. ustawy);
- sporządza w sposób dostępny cyfrowo deklarację dostępności dla każdej wersji językowej strony internetowej lub aplikacji mobilnej, w języku wersji strony internetowej lub aplikacji mobilnej, do której się odnosi (art. 10 ust. 1 ww. ustawy);
- publikuje deklarację dostępności posiadanej strony internetowej - na tej stronie internetowej (art. 10 ust. 7 pkt 1 ww. ustawy).

Deklaracja dostępności zawiera datę ostatniej aktualizacji strony internetowej lub aplikacji mobilnej, po dokonaniu istotnej zmiany jej zawartości, polegającej w szczególności na zmianie wyglądu lub struktury prezentowanych informacji lub zmianie sposobu publikowania informacji (art. 10 ust. 4 pkt 2 ww. ustawy).
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.

Strona internetowa Ośrodka https://www.orpeg.pl/
Biuletyn Informacji Publicznej ORPEG https://bip.orpeg.pl/

W załączniku nr 1 (Opis Przedmiotu Zamówienia) do umowy nr 24/2020/ORPEG zawartej *na budowę i wdrożenie oprogramowania informatycznego pozwalającego na integrację stron internetowych ORPEG wraz ze zmianą szat graficznych* określono, że strona ma spełniać minimalne wymagania dla systemów teleinformatycznych opisane w rozdziale IV rozporządzenia KRI oraz być zgodna z wymaganiami określonymi przez wytyczne WCAG 2.1 na poziomie AA z wyłączeniem dostarczania napisów na żywo. Ponadto projekty graficzne wraz z arkuszami CSS[59] powinny uwzględniać potrzeby osób słabowidzących i udostępniać takie rozwiązania jak opcja wysokiego kontrastu, zmiana wielkości czcionki. Strona powinna informować użytkowników starszych (niekompatybilnych) przeglądarek o konieczności ich aktualizacji w celu poprawnego wyświetlenia strony.
Na ww. stronach, tj. https://www.orpeg.pl/ i https://bip.orpeg.pl/ widoczne są takie funkcjonalności jak: zmiana kontrastu, możliwość powiększenia/pomniejszenia czcionki, włączenie podkreślenia linków, zatrzymywanie/wznowienie animacji.

Deklaracja dostępności strony internetowej Ośrodka została zamieszczona na tej stronie pod adresem: https://www.orpeg.pl/deklaracja-dostepnosci/.
Zgodnie z ww. deklaracją (treść zawarta w deklaracji dostępności w czasie przeprowadzania czynności kontrolnych):
Strona internetowa jest częściowo zgodna z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Na stronie internetowej znajdują się filmy, do których nie dodano napisów dla osób niesłyszących i głuchych. Na stronie internetowej można korzystać ze standardowych skrótów klawiaturowych. Deklarację sporządzono na podstawie samooceny. Data ostatniego przeglądu deklaracji: 2023 -03-01.

Deklaracja dostępności Biuletynu Informacji Publicznej ORPEG została zamieszczona na tej stronie pod adresemhttps://bip.orpeg.pl/deklaracja-dostepnosci/.
Zgodnie z ww. deklaracją (treść zawarta w deklaracji dostępności w czasie przeprowadzania czynności kontrolnych):
Deklarację sporządzono na podstawie samooceny. Data ostatniego przeglądu deklaracji: 2022-03-21. Strona internetowa jest częściowo zgodna z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Na stronie internetowej można korzystać ze standardowych skrótów klawiaturowych.

[59] Kaskadowe arkusze stylów (ang. Cascading Style Sheets, w skrócie CSS) – język służący do opisu formy prezentacji (wyświetlania) stron WWW.

System ankiet (limesurvey) https://forms.orpeg.pl/index.php/879978?lang=pl

Z zamieszczonego pod adresem https://www.limesurvey.org/manual/Accessibility# opisu specyfikacji systemu, nie wynika by system LimeSurvey spełniał wytyczne WCAG.

Deklaracja dostępności systemu ankiet LimeSurvey, została zamieszczona na tej stronie pod adresem: https://forms.orpeg.pl/Deklaracja_dostepnosci.pdf.
Zgodnie z ww. deklaracją (treść zawarta w deklaracji dostępności w czasie przeprowadzania czynności kontrolnych):
Strona internetowa jest częściowo zgodna z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Na stronie internetowej można korzystać ze standardowych skrótów klawiaturowych. Deklarację sporządzono na podstawie samooceny. Data ostatniego przeglądu deklaracji 2022-03-21.

Stwierdzone nieprawidłowości:
Zgodnie art. 11 ustawy o dostępności cyfrowej podmioty publiczne dokonują przeglądu i aktualizacji deklaracji dostępności do dnia 31 marca każdego roku.
W okresie objętym kontrolą, tj. 1.01.2023 r.-20.10.2024 r., terminy przeglądu deklaracji dostępności widniejące na ww. stronach nie były zgodne z terminem wskazanym w ustawie o dostępności cyfrowej na ich dokonanie, tj. do dnia 31 marca każdego roku.

Deklaracje dostępności ww. kontrolowanych systemów, tj. strony internetowej Ośrodka, Biuletynu Informacji Publicznej ORPEG oraz systemu ankiet (LimeSurvey) zawierają informacje o dostępności architektonicznej budynku, w którym mieści się Ośrodek.

Ocena cząstkowa badanego obszaru: pozytywna z nieprawidłowościami.

Mając na uwadze stwierdzone podczas kontroli nieprawidłowości, na podstawie art. 46 ust. 3 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*, przedstawiam następujące zalecenia:

1) zamieścić na stronie BIP ORPEG informacje o:
   - udostępnionym adresie elektronicznej skrzynki podawczej, podanym w formie identyfikatora URI;
   - maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż 5 megabajtów;

   zgodnie z § 3 ust. 1 pkt 1 i 2 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych;
2) opracować i ustanowić system zarządzania bezpieczeństwem informacji, nie tylko w odniesieniu do ochrony danych osobowych;
3) zaktualizować procedury w zakresie bezpieczeństwa fizycznego pomieszczeń Ośrodka;
4) przeprowadzać okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji, o których mowa § 19 ust. 2 pkt 3 rozporządzenia KRI z 2024 r.;
5) zapewniać okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI z 2024 r.;
6) dokonywać 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, zgodnie art. 11 ustawy o dostępności cyfrowej.

Na podstawie art. 49 ww. ustawy, proszę o przekazanie w terminie 14 dni od daty otrzymania wystąpienia pokontrolnego, informacji o sposobie wykonania zaleceń.

Od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z upoważnienia
Ministra Edukacji

Robert Bartold
Dyrektor Generalny
/ – podpisano cyfrowo/

Potwierdzam zgodność kopii wydruku z dokumentem elektronicznym:

Identyfikator dokumentu	2896008.11803349.10108609
Nazwa dokumentu	Wystąpienie pokontrolne - Ośrodek Rozwoju Polskiej Edukacji za Granicą.docx
Tytuł dokumentu	Wystąpienie pokontrolne - Ośrodek Rozwoju Polskiej Edukacji za Granicą
Sygnatura dokumentu	DKA-WK.0915.3.2024.AJK
Data dokumentu	
Skrót dokumentu	6D02F7705284CAD04F13536012650CC01FAEB381
Wersja dokumentu	1.1
Data podpisu	30.06.2025 11:17:55
Podpisane przez	Robert Lucjan Bartold Dyrektor Generalny
Rodzaj certyfikatu	Certyfikat kwalifikowany podpisu elektronicznego

EZD 3.128.1.1.

Data wydruku: 30.06.2025

Autor wydruku: Jakubiak-Kępińska Alicja (Radca)