MINISTER EDUKACJI I NAUKI

Warszawa, 20 maja 2021 r.

DWM-WOPG.0915.1.2020.BT, PK, PL

Pani
Anna Radecka
Dyrektor
Ośrodka Rozwoju Polskiej
Edukacji za Granicą

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 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r., poz. 224) Ministerstwo Edukacji Narodowej[1] (dalej MEN) w terminie od 30 października do 11 grudnia 2020 r. przeprowadziło kontrolę w Ośrodku Rozwoju Polskiej Edukacji za Granicą (dalej: ORPEG), z siedzibą w Warszawie przy ulicy Kieleckiej 43, pn. *Działanie i bezpieczeństwo wybranych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych.*

ORPEG jest państwową jednostką budżetową 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* (Dz. Urz. MEN z 2011 r., Nr 1, poz. 17).

Zgodnie ze statutem nadanym ORPEG Zarządzeniem nr 35 Ministra Edukacji Narodowej z dnia 14 listopada 2019 r. *w sprawie nadania statutu Ośrodkowi*

[1] Zespół kontrolujący w składzie:
1) Beata Tarłowska, główny specjalista w Wydziale Oświaty Polskiej za Granicą w Departamencie Współpracy Międzynarodowej, kierownik zespołu kontrolującego, na podstawie upoważnienia nr 31/2020 z 16 października 2020 r.
2) Piotr Kowalewski, główny specjalista w Wydziale Oświaty Polskiej za Granicą w Departamencie Współpracy Międzynarodowej, na podstawie upoważnienia nr 32/2020 z 16 października 2020 r.
3) Paulina Lesiak-Nowocień, główny specjalista na samodzielnym stanowisku do spraw obiegu dokumentów w postaci elektronicznej w Biurze Organizacyjnym, na podstawie upoważnienia nr 33/2020 z 16 października 2020 r.

Rozwoju Polskiej Edukacji za Granicą (Dz. Urz. MEN z 2019 r., poz. 34), ORPEG 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.

Do kontroli został wybrany jeden z systemów teleinformatycznych pn. *Strona kursów doskonalących kursy.orpeg.pl*, wykorzystywany do prowadzenia e-learningowych kursów dla nauczycieli. Liczba użytkowników tego systemu wynosi 2 900 (stan na dzień 10 grudnia 2020 r.). W dniu 11 lutego 2021 r. liczba użytkowników wyniosła 3 942. Ww. system nie był dotychczas kontrolowany przez MEN od uruchomienia produkcyjnego, które nastąpiło pod koniec 2014 r. Kontrolą objęto okres od 1 stycznia 2019 r. do 16 października 2020 r.

Celem kontroli było sprawdzenie czy procedury i regulacje wewnętrzne dotyczące systemów teleinformatycznych wykorzystywanych przez ORPEG do realizacji zadań publicznych, zawierają odpowiednie regulacje, dzięki którym systemy teleinformatyczne spełniają minimalne wymagania w zakresie elektronicznej wymiany informacji (interoperacyjności) oraz bezpieczeństwa i dostępności informacji. W szczególności zadaniem kontroli była ocena funkcjonujących procedur zapewniających:

1) współdziałanie różnych systemów teleinformatycznych poprzez właściwą organizację wymiany informacji w postaci elektronicznej, współpracę z innymi systemami informatycznymi oraz procesy wspomagania świadczenia usług drogą elektroniczną;
2) skuteczne zarządzanie bezpieczeństwem informacji dla badanych systemów teleinformatycznych, w tym zapewnienia dostępności, autentyczności, poufności, niezawodności i integralności danych przetwarzanych przez system;
3) dostępność treści zawartych na stronach internetowych dla osób z niepełnosprawnościami.

Kontrolowany obszar reguluje ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2020 r. poz. 346 z późn. zm. dalej: ustawa o informatyzacji) oraz rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz.U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI).

Zgodnie ze statutem, ORPEG jest zespołem szkół i placówek, w skład którego wchodzi Polonijne Centrum Nauczycielskie, będące publiczną placówką doskonalenia nauczycieli o zasięgu ogólnokrajowym (dalej: PCN). Zadaniem PCN, stosownie do przepisów rozporządzenia Ministra Edukacji Narodowej z dnia 28 maja 2019 r. *w sprawie placówek doskonalenia nauczycieli* (Dz.U. 2019 poz. 1045), jest wspieranie i doskonalenie zawodowe nauczycieli pracujących wśród Polonii i Polaków zamieszkałych za granicą m.in. w zakresie metodyki nauczania języka polskiego i innych przedmiotów nauczanych w języku polskim za granicą.

System kursów doskonalących powstał w październiku 2014 r., w odpowiedzi na potrzebę stworzenia miejsca pracy grupowej oraz repozytorium plików dla pracowników ORPEG. Celem systemu było przechowywanie i udostępnianie plików, tworzenie forów dyskusyjnych, udostępnianie i zbieranie danych z ankiet, tworzenie kalendarzy, monitorowanie zadań oraz przeprowadzanie ścieżek szkoleniowych. System kursy.orpeg.pl był rozwiązaniem umożliwiającym przejście ze wszystkimi kursami na platformę kursy.orpeg.pl. Utrzymanie i rozwój Systemu od 2015 r. wynikał z potrzeby poszerzania form doskonalenia umożliwiających dotarcie z ofertą kursów do nauczycieli polonijnych na całym świecie.

ORPEG PCN prowadzi kursy kwalifikacyjne i doskonalące dla nauczycieli. W przypadku kursów kwalifikacyjnych zgłoszenie na kurs zawiera dane osobowe i dokumenty potwierdzające wymagane wykształcenie określone w przepisach rozporządzenia Ministra Edukacji Narodowej z dnia 1 sierpnia 2017 r. *w sprawie szczegółowych kwalifikacji wymaganych od nauczycieli* (Dz.U. 2020 r., poz. 1289). Uczestnik kursu po weryfikacji ww. zgłoszenia otrzymuje dostęp do konkretnego kursu. Po ukończeniu kursu otrzymuje świadectwo i przez miesiąc posiada dostęp do materiałów szkoleniowych zamieszczonych na ww. stronie kursy.orpeg.pl.

W przypadku kursów doskonalących zgłoszenie na kurs zawiera dane osobowe. Po wypełnieniu ankiety kandydat otrzymuje dostęp do wybranego kursu, po ukończeniu otrzymuje zaświadczenie (przesyłane elektronicznie) i jeszcze przez miesiąc posiada dostęp do materiałów szkoleniowych.

Uczestnicy kursów, którzy nie ukończą szkolenia (nie spełnią wymagań określonych w programie kursu) tracą dostęp do materiałów szkoleniowych wraz z zakończeniem kursu.

Ocena ogólna kontrolowanej działalności.

Na podstawie wyników kontroli pozytywnie, pomimo stwierdzonych nieprawidłowości, oceniono funkcjonowanie systemu pn. *Strona kursów doskonalących kursy.orpeg.pl* pod względem spełniania minimalnych wymagań w zakresie elektronicznej wymiany informacji (interoperacyjności), bezpieczeństwa i dostępności.

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 art. 16 ustawy o informatyzacji oraz w § 5, 15 - 18 i 20 - 21 rozporządzenia KRI.

ORPEG udostępnił elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę (zgodnie z art. 16 ust. 1a. ustawy o informatyzacji).

Zgodnie z § 5 ust. 2 pkt 1 rozporządzenia KRI, na stronie Biuletynu Informacji Publicznej ORPEG informuje, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym platformy ePUAP. Dzięki, udostępnionej przez ORPEG elektronicznej skrzynce podawczej na platformie ePUAP, możliwe jest przesyłanie do ORPEG pism w postaci elektronicznej. ORPEG prowadzi i na bieżąco aktualizuje informacje opublikowane w BIP dostępnym pod adresem: bip.orpeg.pl (§ 5 ust. 2 pkt 4 rozporządzenia KRI).

Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury określone w dokumencie pn. *Polityka Bezpieczeństwa Informacji (PBI) przetwarzania danych osobowych wraz z Instrukcją Zarządzania Systemem Informatycznym w Ośrodku Rozwoju Polskiej Edukacji za granicą (ORPEG) w Warszawie*, stanowiącym załącznik do Zarządzenia nr 9/2019 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z dnia 21 stycznia 2019 r. w sprawie przyjęcia dokumentacji z zakresu systemu zarządzenia bezpieczeństwem informacji w Ośrodku Rozwoju Polskiej Edukacji za Granicą (§ 15 ust. 2 rozporządzenia KRI).

System *Strona kursów doskonalących kursy.orpeg.pl* korzysta z LMS (Learning Management System) Moodle w wersji 2.7. środowisko nauczania zdalnego. Moodle jest rozprowadzany za darmo jako otwarte oprogramowanie (open source) zgodnie z licencją GNU GPL. W roku 2020 r. ORPEG podpisał z wykonawcą umowę na integrację stron internetowych oraz podniesienie wersji systemu kursów doskonalących do najnowszej wersji wraz ze zmianą szat graficznych oraz przystosowaniem do WCAG 2.1 na poziomie AA zwyłączeniem dostarczania napisów na żywo. Nowa strona kursów zastąpiła dotychczasową w dniu 18 grudnia 2020 r.

W ramach ww. *Systemu* funkcjonuje ogólnodostępna strona internetowa http://kursy.orpeg.pl/ z Platformą kursów on-line organizowanych przez ORPEG PCN. Osoby zainteresowane udziałem w kursach wypełniają ankietę zgłoszeniową, na podstawie której prowadzona jest weryfikacja uczestników kursu. Po weryfikacji dokumentów otrzymują oni kod dostępu do danego kursu. Po zalogowaniu się na Platformę, każdy uczestnik zakłada swój profil i ma dostęp do danych związanych z kursem. Dane w systemie aktualizowane są na bieżąco. W systemie wydzielone zostały role: administratora portalu i menedżerów kursów, aktualizujących dane w systemie na bieżąco. Dodatkowo, każdy uczestnik kursu, po zalogowaniu, ma dostęp do swojego profilu i może na bieżąco aktualizować swoje dane.

System *Strona kursów doskonalących kursy.orpeg.pl* nie współpracuje z zewnętrznymi systemami informatycznymi innych urzędów (§ 5 ust. 3 pkt 3 rozporządzenia KRI). System wyposażony jest w oprogramowanie pozwalające na integrację z innymi zewnętrznymi systemami za pomocą mechanizmu API REST (Aplication Programming Interface), który z założenia łączy się połączeniem szyfrowanym za pomocą SSL. Wszystkie dane w ramach *Strony kursów doskonalących kursy.orpeg.pl* zostają w obrębie tego konkretnego systemu i nie są udostępniane do innych systemów. Wszystkie

zaimplementowane w *System* możliwości łączenia z zewnętrznymi systemami spełniają warunki określone w obowiązujących przepisach, normach i standardach (§ 16 ust. 1 rozporządzenia KRI).

Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie określa Polityka Bezpieczeństwa informacji przetwarzania danych osobowych oraz Instrukcja Zarządzania Systemami Informatycznymi w ORPEG (zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI).

Wszystkie dokumenty i informacje w ramach *Strony kursów doskonalących kursy.orpeg.pl* przesyłane są według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami danych, zgodnie z § 17 ust. 1 rozporządzenia KRI.

W systemie *Strona kursów doskonalących kursy.orpeg.pl* jest możliwość udostępniania zasobów informacyjnych we wszystkich formatach danych wymienionych w Załączniku nr 2 do rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (§ 18 ust. 1 i 2 rozporządzenia KRI). Najczęściej stosuje się formaty danych: .txt; .docx; .doc; .xls; .xlsx; .pdf; .ppt; .jpg; .png. Strona kursy.orpeg.pl umożliwia przyjmowanie dokumentów elektronicznych niezbędnych do realizacji zadań w ramach danego kursu. Dokumenty przyjmowane są w formatach określonych w ww. załączniku, tj.: txt, doc, docx pdf, jpg, png, gif, xls, xlsx, ppt, pptx.

Stwierdzona nieprawidłowość.
Dostosowanie stron internetowych, zgodnie z przepisami art. 27 pkt 2 ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. poz. 848, z późn. zm.), powinno było nastąpić do dnia 23 września 2020 r., natomiast pełne przystosowanie stron internetowych nastąpiło w dniu 30 listopada 2020 r.

Ocena cząstkowa badanego obszaru: pozytywna z nieprawidłowością.

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

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

W ORPEG opracowano, ustanowiono i wdrożono, zgodnie z § 20 ust. 1 i 2 rozporządzenia KRI, System Zarządzania Bezpieczeństwem Informacji (SZBI) pn. Polityka Bezpieczeństwa Informacji (PBI) przetwarzania danych osobowych wraz z Instrukcją Zarządzania Systemem Informatycznym w Ośrodku Rozwoju Polskiej Edukacji za Granicą (ORPEG) w Warszawie.

Dokument został wprowadzony Zarządzeniem nr 9/2019 Dyrektora OPREG z dnia 21 stycznia 2019 r. *w sprawie przyjęcia dokumentacji z zakresu systemu zarządzania bezpieczeństwem informacji w Ośrodku Rozwoju Polskiej Edukacji za Granicą.* Na dokumentację SZBI składają się:

1) Polityka Bezpieczeństwa Informacji (PBI);
2) Instrukcja Zarządzania Systemami Informatycznymi, obejmująca:
   a) Procedurę nadawania i cofania uprawnień w Systemie informatycznym ORPEG;
   b) Procedurę określającą wymogi oraz sposób użytkowania haseł w Systemie informatycznym;
   c) Procedurę rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników Systemu informatycznego;
   d) Procedurę tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych w systemie informatycznym;
   e) Procedurę likwidacji nośników cyfrowych w tym kart elektronicznych;
   f) Procedurę określającą metody i częstotliwość sprawdzania obecności szkodliwego/złośliwego oprogramowania służącego do uszkodzenia, przejęcia danych lub kontroli nad systemem informatycznym przez osobę nieupoważnioną;
   g) Procedurę zarządzania systemem informatycznym w przypadkach awaryjnych;
   h) Procedurę wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;
   i) Instrukcję postępowania w przypadku wystąpienia incydentu związanego z ochroną danych osobowych;
   j) Regulamin użytkowania komputerów przenośnych.

Dokument był poprzedzony Polityką Bezpieczeństwa Informacji wprowadzoną Zarządzeniem nr 20/2015 Dyrektora OPREG z dnia 28 sierpnia 2015 r. *w sprawie wprowadzenia w Ośrodku Rozwoju Polskiej Edukacji za Granicą Polityki Bezpieczeństwa Informacji.*

Funkcjonujący w ORPEG SZBI jest monitorowany, poddawany przeglądom i doskonalony, zgodnie z § 20 ust. 1 rozporządzenia KRI. W marcu 2020 r. przeprowadzono listę kontrolną zadań z zakresu ochrony danych osobowych i sposobu przetwarzania danych osobowych w ORPEG w 2019 r. oraz analizę ryzyk związanych z przetwarzaniem danych osobowych w ORPEG. Dokonano przeglądu i aktualizacji rejestrów, procedur, polityk i instrukcji związanych z bezpieczeństwem danych osobowych przetwarzanych przez Administratora. Przedmiotowe dokumenty są na bieżąco aktualizowane. Przeprowadzono audyt ich zgodności z aktualnym stanem prawnym i faktycznym.

W kontrolowanym okresie, tj. od 1 stycznia do 30 października 2020 r. nie dokonano aktualizacji regulacji SZBI. W trakcie przeprowadzania kontroli, zgodnie z informacjami przekazanymi przez ORPEG, zarządzenie było na etapie prac aktualizacyjnych, stosownie do przepisów § 20 ust. 2 pkt 1 rozporządzenia KRI. Zakończenie prac i wprowadzenie dokumentu zarządzeniem dyrektora ORPEG zaplanowano na koniec lutego 2021 r.

ORPEG nie korzysta z usługi dzierżawy serwerów i hostingu. Posiada własne zasoby serwerowe, które znajdują się w wyspecjalizowanym centrum kolokacyjnym. W każdym momencie może zmieniać konfigurację maszyny wirtualnej, na której jest zainstalowana *Strona kursów doskonalących*

kursy.orpeg.pl, w zależności od obciążenia, może dowolnie skalować wydajność platformy. Posiadane przez ORPEG serwery połączone w są w trybie HA (tryb wysokiej dostępności) i w razie awarii inny serwer przejmuje rolę utrzymania Platformy. Obsługa techniczna jest prowadzona przez Wydział informatyczny znajdujący się w ORPEG. Firma kolokująca serwery ORPEG zapewnia także wsparcie techniczne w podstawowym zakresie sieciowym.

Wszystkie systemy w ORPEG są monitorowane pod względem dostępności z zewnątrz za pomocą zewnętrznych serwisów. Monitorowana jest praca serwerów, maszyn wirtualnych oraz ich obciążenia w ramach środowiska wirtualizacyjnego WMware. W każdym momencie ORPEG ma możliwość połączenia się zdalnie ze swoimi serwerami czy maszynami wirtualnymi.

ORPEG zapewnia bezpieczeństwo danych przechowywanych na serwerach. Posiada system wykonywania kopii zapasowych, w ramach którego codziennie wykonywane są kopie wszystkich kluczowych maszyn wirtualnych. Dodatkowym zabezpieczeniem jest codzienna replikacja kopii zapasowych z serwerów w centrum kolokacyjnym na serwery znajdujące się w siedzibie ORPEG. Na serwerach w kolokacji wszystkie dane znajdują się na przestrzeniach zabezpieczonych przez system RAID 6, gdzie uszkodzenie jednego czy dwóch dysków nie powoduje utraty danych. Dodatkowo serwery połączone są w trybie wysokiej dostępności i na wypadek uszkodzenia jednego lub dwóch serwerów kolejny przejmuje jego rolę i uruchamia w ciągu kilku minut wszystkie maszyny wirtualne. Dane z półki dyskowej przesyłane są za pomocą podwójnych kanałów Fibre Chanel, gdzie w wypadku uszkodzenia jednego z nich kolejny przejmuje przesyłanie danych.

Dane posiadane przez ORPEG znajdują się na maszynach wirtualnych w środowisku VMware. Do wykonywania kopii zapasowych używane są narzędzia, które wykonują codzienne kopie zapasowe przyrostowe, a co 7 dni wykonywana jest pełna kopia każdego systemu. Kopią objęte są wszystkie kluczowe maszyny wirtualne oraz wszystkie bazy danych znajdujące się na serwerach w centrum kolokacyjnym oraz w siedzibie ORPEG. Wykonywanie kopii zaplanowane jest w godzinach nocnych (czasami w ciągu dnia). Wykonywanie kopii zapasowych nie wpływa w stopniu zauważalnym na wydajność systemów i platform dostępnych z zewnątrz.

W marcu 2020 r. przeprowadzono analizę ryzyk występujących w ORPEG w odniesieniu do przetwarzanych danych osobowych, sporządzono arkusz analizy oraz rekomendacje. Przeprowadzono również analizę ryzyka podczas pracy zdalnej związanej z pandemią koronawirusa, sporządzono raport z analizy.

Na bieżąco są podejmowane działania w celu zapobieżenia ryzyku: zapewnienie odpowiednich warunków przetwarzania danych osobowych (m.in. zamykane na klucz szafy, odpowiednie archiwum, zabezpieczenia systemu informatycznego), zapewnienie i stosowanie odpowiednich środków technicznych (m.in. szyfrowanie i hasłowanie danych, zasilanie awaryjne, bezpieczniki, kontrolowane wejścia - wideofon, indywidualne hasła w systemie), oraz organizacyjnych (rejestry, polityki i instrukcje, procedury, szkolenia

personelu) (§ 20 ust. 2 pkt 1 i 3 rozporządzenia KRI).

Wydział Informatyczny ORPEG do utrzymania aktualności inwentaryzacji sprzętu i oprogramowania wykorzystuje aplikację LogSystem, dzięki której może zarządzać i rozliczać licencje dla użytkowników oraz sprzętu, monitoruje komputery, wykonuje audyty, a także prowadzi listę dostępów, ma na bieżąco podgląd konfiguracji sprzętu komputerowego zainstalowanego w ORPEG. Każdy komputer zainstalowany w ORPEG posiada zainstalowanego agenta, który na co zadany czas lub na żądanie wysyła informacje o zainstalowanym oprogramowaniu, konfiguracji sprzętu lub innych elementach monitorowanych danych. Sprawy dotyczące inwentaryzacji sprzętu i oprogramowania reguluje Instrukcja Zarządzania Systemami Informatycznymi. Aktualizacja wykonywana jest nie rzadziej niż 2 razy w roku (§ 20 ust. 2 pkt 2 rozporządzenia KRI).

Zgodnie z § 20 ust. 2 pkt 4, 5 rozporządzenia KRI, 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. Zgodnie z wyjaśnieniami ORPEG, zakres uprawnień ww. osób jest bezzwłocznie zmieniany w przypadku zmiany zadań tych osób, stosownie do procedury nadawania i cofania uprawnień w Systemie informatycznym ORPEG opisanej w PBI.

Stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI, osoby zaangażowane w proces przetwarzania informacji w okresie objętym kontrolą uczestniczyły w szkoleniach w zakresie bezpieczeństwa informacji. Szkolenie z zakresu RODO ukończyli wszyscy pracownicy, w tym nauczyciele ORPEG, mający dostęp do platformy kursy.orpeg.pl. Każdy nowy pracownik otrzymuje link do szkolenia on-line (realizowane przez firmę zewnętrzną) z zakresu RODO, który jest zakończony testem sprawdzającym. W kontrolowanym okresie szkolenia on-line realizowane były w: listopadzie 2019 r. i maju 2020 r. Szkolenia obejmowały ogólne informacje na temat bezpieczeństwa i ochrony danych w organizacji, w szczególności: sposób przetwarzania danych osobowych kadrowych (dane pracowników) zgodnie z wymogami RODO i Kodeksu Pracy; środki ochrony danych osobowych wymagane przez RODO; obowiązki administratorów danych oraz podmiotów przetwarzających nałożone przez RODO oraz przepisy szczegółowe; rejestr czynności przetwarzania danych osobowych, analiza ryzyka i ocena skutków dla ochrony danych.

Podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość (§ 20 ust. 2 pkt 8 rozporządzenia KRI) ustanowiono w szczególności w regulaminie użytkowania komputerów przenośnych PBI.

Umowy serwisowe podpisane ze stronami trzecimi, zgodnie ze wzorem umowy powierzenia danych osobowych określonym w PBI, zawierają zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji (§ 20 ust. 2 pkt 10 rozporządzenia KRI). ORPEG prowadzi ewidencję zawartych umów powierzenia przetwarzania danych osobowych oraz umów, w ramach których powierzono przetwarzanie danych.

Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI, podejrzenia incydentów naruszenia bezpieczeństwa informacji, zgodnie z wyjaśnieniami ORPEG są bezzwłocznie zgłaszane w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących, zgodnie z Instrukcją postępowania w przypadku wystąpienia incydentu związanego z ochroną danych osobowych PBI. Od 2019 r. wszystkie zgłoszenia są rejestrowane przez system Helpdesk ułatwiający pracę z użytkownikami i ich zgłoszeniami. ORPEG prowadzi rejestr incydentów naruszenia bezpieczeństwa w bazie systemu pomocy technicznej. Zgłoszenia dotyczące incydentów przyjmowane są za pomocą systemu oraz telefonicznie.

W okresie kontrolowanym nie wykonano audytu wewnętrznego w zakresie BI (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: zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok). Ostatni audyt BI był wykonany w 2018 r.

W celu zapewnienia ochrony przetwarzanych informacji (§ 20 ust. 2 pkt 7, 9, 11, 12 rozporządzenia KRI) ORPEG stosuje nw. środki techniczne i organizacyjne:

1. Środki ochrony fizycznej:

1) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi);
2) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zamykanymi, do których klucz posiada wyłącznie osoba uprawniona;
3) zbiory danych archiwalnych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są od włamania;
4) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych jest niemożliwy w czasie nieobecności zatrudnionych tam pracowników;
5) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie;
6) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętym pomieszczeniu serwerowni i archiwum;
7) pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy;
8) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów lub przekazywane do firmy bezpiecznego niszczenia nośników danych;
9) dopuszczenie do przetwarzania danych jedynie osób posiadających upoważnienie nadane przez administratora danych;
10) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
11) przeszkolenie osób zatrudnionych przy przetwarzaniu danych z zakresu:
    a) przepisów dotyczących ochrony danych osobowych,
    b) zabezpieczeń systemów informatycznych;

12) zobowiązanie osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania ich w tajemnicy poprzez podpisanie stosownych oświadczeń;
13) ustawianie ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
14) przechowywanie kopii zapasowych zbiorów danych osobowych odbywa się w tym samym pomieszczeniu, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco, ta sama kopia jest automatycznie przesyłana do kolokacji;
15) opuszczanie stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
16) niepozostawianie bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach;
17) kasowanie po wykorzystaniu danych na dyskach przenośnych;
18) niezapisywanie hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku i niepozostawianie w miejscu widocznym;
19) niszczenie w niszczarce lub chowanie do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
20) niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
21) chowanie do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
22) umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
23) zniszczenie fizycznie uszkodzonych nośników przed ich wyrzuceniem;
24) niewykorzystywanie powtórnie, do sporządzania brudnopisów pism, jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;
25) niszczenie w niszczarce wydruków zawierających dane osobowe po wykorzystaniu. Czynność tę należy wykonywać codziennie przed zakończeniem pracy. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

2. Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:
1) zastosowano urządzenia typu UPS i wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
2) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
3) zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity;
4) system informatyczny wykorzystywany do przetwarzania danych osobowych:
   a) rejestruje zmiany dokonywane w zbiorach danych osobowych;
   b) reguluje zakres uprawnień do przetwarzania poszczególnych zbiorów dla każdego z pracowników;

c) wymaga uwierzytelnienia z wykorzystaniem identyfikatora i hasła;
d) wymusza okresową zmianę hasła dostępowego;
e) wykorzystuje szyfrowanie w trakcie przesyłania danych;
f) automatycznie blokuje dostęp w przypadku dłuższej nieaktywności użytkownika;

5) na komputerach gdzie przetwarzane są dane osobowe zastosowano zabezpieczenie przed nieautoryzowanym dostępem (wymagane hasło).

System pn. *Strona kursów doskonalących kursy.orpeg.pl* został zaprojektowany, wdrożony i jest eksploatowany z uwzględnieniem jego funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych standardów i metodyk (§15 ust. 1 rozporządzenia KRI).

Stosownie do § 20 ust. 4 rozporządzenia KRI ustanowiono dodatkowe zabezpieczenia w postaci reCAPTCHA V3 będące udoskonalonym mechanizmem do rozpoznania użytkowników i dodatkowe zabezpieczenie ruchu sieciowego poprzez IPS (ochronę przed włamaniami) oraz ochronę DLP (ochrona przed wyciekiem danych). Dodatkową zmianą w ww. systemie jest wprowadzone szyfrowanie danych pomiędzy serwerem a komputerem użytkownika przeglądającego stronę.

Systemy dzienników funkcjonujące w systemach i platformach ORPEG są skonfigurowane odpowiednio do wymagań § 21 ust. 2 rozporządzenia KRI. Dzienniki (logi) systemowe i aplikacje rejestrują wszystkie niezbędne działania użytkowników i obiektów systemowych a w szczególności do systemu z uprawnieniami administracyjnymi, konfiguracji systemu, w tym konfiguracji zabezpieczeń a także przetwarzanych w systemie danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Każdy system teleinformatyczny oraz system komputerowy zainstalowany w ORPEG posiada system logów, który swoim zakresem obejmuje chronologiczny rejestr zdarzeń odnotowujący działania użytkowników jak i obiektów systemowych na różnych poziomach dostępu. Zakres ten obejmuje, zgodnie z rozporządzeniem KRI § 21. ust 3, działania użytkowników nieposiadających uprawnień administracyjnych, zdarzenia systemowe nieposiadające krytycznego znaczenia dla funkcjonowania systemu oraz zdarzenia i parametry środowiska, w którym eksploatowany jest system teleinformatyczny. Dane zbierane przez systemy oparte są także o zakres wynikający z analizy ryzyka.

W systemie pn. *Strona kursów doskonalących kursy.orpeg.pl* ustawienia zapisywania informacji w logach systemowych zostały skonfigurowane tak, aby dane były dostępne od dnia ich zapisu przez okres 2 lat (§ 21 ust. 4 rozporządzenia KRI).

Stwierdzona nieprawidłowość:
Nie zapewniono okresowego audytu wewnętrznego w zakresie BI co najmniej raz w roku.

Ocena cząstkowa badanego obszaru: pozytywna z nieprawidłowością.

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

WCAG (web content accessability guidelines) to zbiór rekomendacji, których należy przestrzegać, aby zapewnić dostęp do treści internetowych możliwie szerokiej grupie użytkowników, włączając w to osoby niepełnosprawne. Obecnie obowiązuje wersja dokumentu WCAG 2.1. Wymogi określone w ww. dokumencie zostały wprowadzone do obowiązującego prawa i zapisane w § 19 i załączniku 4 do rozporządzenia KRI.

Strona kursów doskonalących kursy.orpeg.pl spełnia wymagania WCAG 2.1 na poziomie AA z wyłączeniem dostarczania napisów na żywo. Strona zapewnia wersję kontrastową, możliwość powiększenia czcionki, podkreślenie linków, zatrzymywanie animacji.

Deklaracja dostępności zawiera informacje na temat poziomu dostępności strony internetowej oraz aplikacji mobilnej, a także dostosowania budynku, w którym mieści się instytucja, do potrzeb osób niepełnosprawnych i z ograniczeniami. Zgodnie z art. 10 ustawy o dostępności cyfrowej deklaracja dostępności została zamieszczona na *Stronie kursów doskonalących kursy.orpeg.pl*.

Ocena cząstkowa badanego obszaru: pozytywna.

Mając na uwadze stwierdzone podczas kontroli nieprawidłowości, na podstawie art. 46 ust. 3 pkt 1 ustawy o kontroli w administracji rządowej zalecam zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Na podstawie art. 49 ustawy o kontroli w administracji rządowej, przekazując powyższe wystąpienie pokontrolne, proszę o przekazanie w terminie 14 dni od daty otrzymania niniejszego wystąpienia informacji o sposobie wykonania zalecenia.

Od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach.

Z upoważnienia
MINISTRA EDUKACJI I NAUKI

Włodzimierz Bernacki
Sekretarz Stanu
/ – podpisany cyfrowo/