Minister
Edukacji

DSKKZ-WKPiE.0915.1.2023.AP
Warszawa, 18 czerwca 2024 r.

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

WYSTĄPIENIE POKONTROLNE

Zgodnie z art. 47 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[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*, 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] (dalej: Ministerstwo) w terminie od 28 listopada 2023 r. do 29 lutego 2024 r. przeprowadziło w Centralnej Komisji Egzaminacyjnej (dalej także: CKE), z siedzibą w Warszawie, przy ul. Józefa Lewartowskiego 6, 00-190 Warszawa, kontrolę[4] pn. *Działanie i bezpieczeństwo wybranych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych*.

Celem kontroli było dokonanie oceny czy systemy teleinformatyczne wykorzystywane do realizacji zadań publicznych, spełniają minimalne wymagania w zakresie elektronicznej wymiany informacji (interoperacyjności), są bezpieczne i dostępne dla obywateli.
Oceniono:

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

---

[1] Dz.U. z 2020 r. poz. 224.
[2] Dz.U. z 2023 r. poz. 57 z późn. zm.
[3] Poprzednio Ministerstwo Edukacji i Nauki. Ministerstwo Edukacji Narodowej z dniem 1 stycznia 2024 r. na podstawie rozporządzenia Rady Ministrów z dnia 16 grudnia 2023 r. *w sprawie utworzenia Ministerstwa Edukacji Narodowej* (Dz.U. z 2023 r. poz. 2694).
[4] Kontrolę przeprowadzili pracownicy Ministerstwa:
1) Adam Paprocki, radca w Wydziale Kształcenia Praktycznego i Egzaminowania w Departamencie Strategii, Kwalifikacji i Kształcenia Zawodowego, na podstawie upoważnień nr 53/2023 z dnia 27 listopada 2023 r.; nr 66/2023 z dnia 18 grudnia 2023 r. i nr 9/2024 z dnia 30 stycznia 2024 r.;
2) Alicja Jakubiak-Kępińska, główny specjalista w Wydziale Kontroli w Departamencie Kontroli i Audytu, na podstawie upoważnień nr 54/2023 z dnia 27 listopada 2023 r.; nr 67/2023 z dnia 18 grudnia 2023 r. i nr 10/2024 z dnia 30 stycznia 2024 r.;
3) Natalia Piętak, główny specjalista w Wydziale Bezpieczeństwa w Biurze Dyrektora Generalnego, na podstawie upoważnień nr 55/2023 z dnia 27 listopada 2023 r., nr 68/2023 z dnia 18 grudnia 2023 r. i nr 11/2024 z dnia 30 stycznia 2024 r.

Kontrolą objęto okres od 7 marca 2022 r. (od dnia wejścia w życie zarządzenia nr 978 dyrektora Centralnej Komisji Egzaminacyjnej z 07.03.2022 r. *w sprawie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji)* do 28 listopada 2023 r. (do dnia rozpoczęcia kontroli).

CKE została utworzona z dniem 1 stycznia 1999 r. na mocy ustawy z dnia 25 lipca 1998 r. *o zmianie ustawy o systemie oświaty*[5]. Nadzór nad działalnością Centralnej Komisji Egzaminacyjnej sprawuje minister właściwy do spraw oświaty i wychowania.[6] W ramach nadzoru minister właściwy do spraw oświaty i wychowania m.in.: przeprowadza kontrole w Centralnej Komisji Egzaminacyjnej.

Organizację CKE określa jej statut nadany przez ministra właściwego do spraw oświaty i wychowania, stanowiący załącznik do zarządzenia Ministra Edukacji Narodowej z dnia 8 października 2015 r. *w sprawie nadania statutu Centralnej Komisji Egzaminacyjnej*.[7] Działalnością CKE kieruje dyrektor, którego - zgodnie z art. 9d ust. 7 *ustawy o systemie oświaty* - powołuje i odwołuje minister właściwy do spraw oświaty i wychowania. W okresie objętym kontrolą Centralną Komisją Egzaminacyjną kierował Pan dr Marcin Smolik, powołany na stanowisko dyrektora tej Komisji 23 maja 2012 r.

Kontrolowany obszar regulują:
- ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[8] (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*[9] (dalej: rozporządzenie KRI);
- rozporządzenie z dnia 14 września 2011 r. Prezesa Rady Ministrów *w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych*[10] (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*[11] (dalej: ustawa o dostępności cyfrowej);
- ustawa z dnia 6 września 2001 r. *o dostępie do informacji publicznej*[12].

Do kontroli zostały wybrane nw. systemy, wykorzystywane do realizacji zadań publicznych:
1) System Informatyczny Obsługi Egzaminów Potwierdzających Kwalifikacje w Zawodzie, działający pod adresem: https://epkz.cke.edu.pl/ (dalej: SIOEPKZ). Informacje o SIOEPKZ zamieszczone są pod adresem: https://cke.gov.pl/egzamin-zawodowy/system-informatyczny-obslugi-egzaminow-zawodowych-sioepkz/;
2) Biuletyn Informacji Publicznej CKE, działający pod adresem: https://bip.cke.gov.pl/ (dalej BIP CKE).

[5] Dz.U. Nr 117, poz. 759.
[6] Zgodnie z art. 9d ust. 1 ustawy z dnia 7 września 1991 r. *o systemie oświaty* (Dz.U. z 2022 r. poz. 2230).
[7] M.P. poz. 1046.
[8] Dz.U. z 2023 r. poz. 57.
[9] Dz.U. z 2017 r. poz. 2247.
[10] Dz.U z 2018 r. poz. 180.
[11] Dz.U. z 2023 r. poz. 1440.
[12] Dz.U. z 2022 r. poz. 902.

W okresie objętym kontrolą w CKE obowiązywały:
- *Regulamin Organizacyjny Centralnej Komisji Egzaminacyjnej* wprowadzony zarządzeniem nr 848 Dyrektora CKE z dnia 10 września 2020 r.,
- *Instrukcja kancelaryjna* wprowadzona zarządzeniem nr 376 Dyrektora Centralnej Komisji Egzaminacyjnej z dnia 24 lipca 2014 r.,
- *Regulamin pracy zdalnej w CKE* ustalony zarządzeniem nr 1060 Dyrektora CKE z dnia 4 kwietnia 2023 r.

W CKE w zakresie systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych obowiązuje Zarządzenie nr 978 dyrektora Centralnej Komisji Egzaminacyjnej z dnia 7.03.2022 r. *w sprawie ustalenia System Zarządzania Bezpieczeństwem Informacji* (dalej: SZBI).
W CKE został powołany Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji.

Ocena ogólna kontrolowanej działalności.

Na podstawie wyników kontroli obszar objęty kontrolą oceniono pozytywnie mimo stwierdzonych nieprawidłowości.

Podczas czynności kontrolnych stwierdzono następujące nieprawidłowości:
1. W BIP CKE zauważono brak informacji w zakresie maksymalnego rozmiaru dokumentu elektronicznego wraz z załącznikami, wyrażonego w megabajtach, możliwego do doręczenia za pomocą elektronicznej skrzynki podawczej.
   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, o maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż 5 megabajtów.
   Informacja w tym zakresie została przez CKE uzupełniona w Biuletynie Informacji Publicznej Centralnej Komisji Egzaminacyjnej w trakcie czynności kontrolnych.
2. Na stronie BIP CKE w opublikowanych opisach procedur obowiązujących przy załatwianiu spraw drogą elektroniczną, z zakresu właściwości CKE, nie zamieszczono informacji o rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru.
   Zgodnie z § 3 ust. 1 pkt 5 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych, *podmioty publiczne informują na swoich stronach podmiotowych BIP, o rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru.*
   Powyższe nie miało istotnego wpływu na kontrolowaną działalność.

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, 5 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.

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.*

  Centralna Komisja Egzaminacyjna 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 CKE na ePUAP oraz informacja o jej udostępnieniu są zamieszczone pod adresem: https://bip.cke.gov.pl/ oraz https://bip.cke.gov.pl//artykul/103/3/name.

  W badanym zakresie nie stwierdzono nieprawidłowości.

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

  Zgodnie z ww. przepisem adres ESP (/cke/skrytka) w Biuletynie Informacji Publicznej Centralnej Komisji Egzaminacyjnej jest podany w formie identyfikatora URI (Uniform Resource Identifier, tłum. Ujednolicony Identyfikator Zasobów).

  W opinii kontrolujących podanie adresu elektronicznej skrzynki podawczej także na stronie internetowej CKE ułatwiłoby użytkownikom strony kontakt z jednostką.

  W badanym zakresie nie stwierdzono nieprawidłowości.

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

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

  CKE przedstawiła następujące wyjaśnienia: *„maksymalny rozmiar dokumentu elektronicznego wraz z załącznikami możliwy do doręczenia za pomocą elektronicznej skrzynki podawczej nie może przekraczać 500 MB (zgodnie ze standardami platformy ePUAP). W nawiązaniu do powyższego przedkładamy, że w trakcie obowiązywania rozporządzenia nie zidentyfikowano problemu technicznego przesyłu dokumentów na udostępnioną elektroniczną skrzynkę podawczą ePUAP widniejącą na stronie BIP CKE. Stosowny zapis umieszczono bezzwłocznie na stronie BIP CKE."*

  Informacja w tym zakresie została przez CKE uzupełniona w BIP CKE i zamieszczona pod adresem: https://bip.cke.gov.pl/artykuly/105/dane-teleadresowe.

- 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.*

  Centralna Komisja Egzaminacyjna nie sporządza wzorów dokumentów elektronicznych do przekazania do centralnego repozytorium (CRWDE). Na stronie BIP CKE zawarty jest

odnośnik do Elektronicznej Platformy Usług Administracji Publicznej przekierowujący do strony: https://epuap.gov.pl/wps/portal oraz w zakładce: „Podstawowe informacje" → „Dane teleadresowe"[13] zamieszczony jest link zewnętrzny pn. „Formularz tzw. pisma ogólnego do podmiotu publicznego".

W badanym zakresie nie stwierdzono nieprawidłowości.

Interoperacyjność realizowana na podstawie rozporządzenia KRI.

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

  Na stronie internetowej CKE pod adresem https://cke.gov.pl/egzamin-zawodowy/system-informatyczny-obslugi-egzaminow-zawodowych-sioepkz/, znajdują się informacje związane systemem informatycznym obsługi egzaminów zawodowych. Na stronie zamieszczono informacje o sposobie dostępu oraz zakresie użytkowym tego serwisu, tj. wskazano:
  - formuły obowiązywania egzaminu w zależności od podstawy programowej według której kształciły się osoby przystępujące do egzaminu:
    - formuła 2017 dla osób, które kształciły się wg podstawy programowej obowiązującej od 1 września 2017 r.,
    - formuła 2019 dla osób, które kształcą się lub kształciły wg podstawy programowej obowiązującej od 1 września 2019 r.,
  - materiały szkoleniowe z przeprowadzonych webinariów,
  - instrukcje dla poszczególnych użytkowników systemu (m.in. dla pracowników CKE, OKE, ośrodków egzaminacyjnych, egzaminatorów, recenzentów, zdających),
  - pakiet do próbnego uruchomienia elektronicznego systemu przeprowadzania egzaminu przed uzyskaniem upoważnienia.

  W zakładkach dotyczących poszczególnych formuł zawarto informacje w zakresie:
  - podstawy programowej,
  - informatorów zawierających: informacje o kwalifikacjach wyodrębnionych w poszczególnych zawodach, zadania zawodowe i możliwości kształcenia w zawodzie wynikające z podstawy programowej dla zawodu, przykładowe zadania do części pisemnej i części praktycznej egzaminu,
  - informacji o wyposażeniu stanowisk egzaminacyjnych dla wszystkich kwalifikacji,
  - harmonogramów egzaminów, komunikatów i informacji dot. egzaminów,
  - sprawozdania z osiągnięć zdających egzamin zawodowy oraz egzamin potwierdzający kwalifikacje w zawodzie w poszczególnych latach.

  W zakładce BIP są udostępnione harmonogramy, komunikaty i informacje obowiązujące w poszczególnych latach dla każdej z formuł dotyczące egzaminów potwierdzających kwalifikacje w zawodzie oraz egzaminów zawodowych.

  W badanym zakresie nie stwierdzono nieprawidłowości.

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

[13] Dane teleadresowe - Biuletyn Informacji Publicznej Centralna Komisja Egzaminacyjna w Warszawie (cke.gov.pl).

Na podstawie § 3 ust. 1 pkt. 4-5 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych, *podmioty publiczne informują na swoich stronach podmiotowych BIP, o:*

- *rodzajach informatycznych nośników danych, na których może zostać im doręczony dokument elektroniczny;*
- *rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru.*

W BIP CKE pod adresem: https://bip.cke.gov.pl/artykuly/105/dane-teleadresowe zamieszczone zostały wymogi dla dokumentów elektronicznych dostarczanych do CKE wraz z rodzajami informatycznych nośników danych, na których dokument w wersji elektronicznej może zostać doręczony do Centralnej Komisji Egzaminacyjnej. Należą do nich: płyta CD, płyta DVD, pamięć USB.

Podczas kontroli stwierdzono, że na stronie BIP CKE w opublikowanych opisach procedur obowiązujących przy załatwianiu spraw drogą elektroniczną, z zakresu właściwości CKE, nie zamieszczono informacji o rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru. Powyższe nie miało istotnego wpływu na kontrolowaną działalność.

- Zgodnie z § 5 ust. 3 pkt 3 rozporządzenia KRI - *interoperacyjność na poziomie semantycznym osiągana jest przez stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.*
  Zgodnie z § 16 rozporządzenia 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.

System SIOEPKZ ma możliwość wymiany danych z innymi systemami teleinformatycznymi - jest zintegrowany z Rejestrem Szkół i Placówek Oświatowych poprzez Krajowy System Danych Oświatowych[14] w zakresie danych o podmiotach, dla których ten rejestr jest referencyjny w związku z zapisami ustawy z dnia 15 kwietnia 2011 r. *o Systemie Informacji Oświatowej* (dalej SIO)[15]. Implementacja i wdrożenie integracji z systemem SIO (API) zostały przygotowane w oparciu o standardy IETF i W3C, zapewniające bezpieczeństwo, poufność, integralność i rozliczalność przetwarzanych danych. Komunikacja wymagająca dodatkowego zabezpieczenia jest realizowana przy pomocy protokołu warstwy trzeciej IPSec VPN.

W badanym zakresie nie stwierdzono nieprawidłowości.

[14] Na podstawie dokumentu pn. „Integracja z SIO – pobieranie danych o podmiotach (ośrodkach egzaminacyjnych) i obsługa tych danych w systemie SIOEPKZ" wersja 6.0 z dnia 04.12.2020 r.
[15] Dz.U. z 2022 r. poz. 2597 z późn. zm.

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

Zgodnie z zapisami określonymi w *Zasadach Zarządzania Bezpieczeństwem Informacji* (rozdział 12 *Pozyskanie i rozwój oprogramowania)* (w ramach Systemu Zarządzania Bezpieczeństwem Informacji), celem CKE jest zapewnienie, że pozyskanie, tworzenie, rozwój i utrzymanie systemów informatycznych jest realizowane w sposób gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa.
Szczegółowe regulacje w zakresie pozyskiwania i rozwoju oprogramowania opisane zostały w *Polityce Bezpieczeństwa Systemu Informatycznego* (w ramach Systemu Zarządzania Bezpieczeństwem Informacji), a także w procedurach: nadzoru nad konfiguracją i zmianą (PB-16) oraz bezpieczeństwa i rozwoju oprogramowania (PB-18) (w ramach Systemu Zarządzania Bezpieczeństwem Informacji).
Ponadto zgodnie z *Polityką Bezpieczeństwa Danych Osobowych* (rozdział 18 *Domyślna ochrona i ochrona w fazie projektowania)* (w ramach Systemu Zarządzania Bezpieczeństwem Informacji) podczas tworzenia produktów, usług i aplikacji, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, Administrator danych osobowych oraz podmioty przetwarzające podczas opracowywania i projektowania biorą pod uwagę prawo do ochrony danych osobowych oraz wytyczne EROD - Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0. Stosowanie zasad domyślnej ochrony oraz ochrony w fazie projektowania sprowadza się do stosowania zabezpieczeń organizacyjnych i technicznych adekwatnych do oszacowanego ryzyka dla projektowanych lub planowanych operacji przetwarzania danych osobowych w systemach informatycznych.

SIOEPKZ to system utworzony w 2018 r. przez Polską Wytwórnię Papierów Wartościowych S.A., którego głównymi funkcjami są:
- zgłaszanie oraz przesyłanie deklaracji przystąpienia do egzaminu zdających,
- planowanie egzaminu potwierdzającego kwalifikacje w zawodzie oraz egzaminu zawodowego,
- przeprowadzanie elektronicznego egzaminu za pomocą wirtualnego serwera egzaminacyjnego,
- zamawianie i wprowadzanie zadań egzaminacyjnych,
- udostępnianie wyników i statystyk szkołom i zdającym,
- wystawianie dokumentów dla zdających (świadectwa, certyfikaty, dyplomy).

Jest to system o zasięgu krajowym, do którego dostęp mają pracownicy Centralnej i Okręgowych Komisji Egzaminacyjnych oraz dyrektorzy i pracownicy szkół, egzaminatorzy oraz zdający. Obecnie jest około 1,4 miliona użytkowników.
Za utrzymywanie w ruchu w środowisku produkcyjnym, testowym, przedprodukcyjnym oraz rozwoju, w tym wprowadzania modyfikacji (wprowadzania zmian) związanych z rozwojem wdrożonego i funkcjonującego w CKE systemu informatycznego obsługi egzaminów zawodowych SIOEPKZ, odpowiada podmiot zewnętrzny, z którym CKE zawarła umowę (w okresie objętym kontrolą obowiązywała umowa nr CKE-WAG/56/2021 zawarta 24 listopada 2021 r. na *utrzymanie w ruchu i rozwój systemu informatycznego SIOEPKZ w tym prace programistyczne oraz usługi im towarzyszące)*.
Zgodnie z zapisami umowy Wykonawca gwarantuje realizację umowy zgodnie z normami:
1) PN-EN ISO 90001:2015 Systemy zarządzania jakością – Wymagania;

2) PN-EN ISO 27001:2017 Technika informatyczna – Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem Informacji – Wymagania;
3) PN-ISO/IEC 20000-1:2014-01 Technika informatyczna – zarządzanie usługami – Część 1: Wymagania dla systemu zarządzania usługami.

W umowie oraz załącznikach do umowy określone zostały m.in. wymagania SLA[16], zapewniające odpowiedni poziom usług informatycznych w zakresie rozwiązywania problemów technicznych związanych z prawidłowym działaniem systemu, w tym: określono procedurę zarządzania incydentami zawierającą m.in. analizę ryzyk w zakresie możliwości wystąpienia incydentów z określeniem prawdopodobieństwa i wpływu tych ryzyk na funkcjonowanie SIOEPKZ, zapewniono rejestrowanie wszelkich prac prowadzonych w następstwie zgłoszeń, incydentów i awarii w Servce Desk/Help Desk, określono rodzaje awarii/incydentów/zgłoszeń wraz ze wskazaniem granicznych czasów wykonania czynności (tj. czasu reakcji - potwierdzenia przyjęcia zgłoszenia, czasu zgłoszenia awarii/incydentu odpowiednio do Gwaranta I-S[17] lub Operatora RChO[18], czasu usunięcia awarii/skutków incydentu/rozwiązania zgłoszenia, czasu na odnotowanie czynności w bazie wiedzy).
SIOEPKZ jest monitorowany w trybie ciągłym w zakresie jego poprawnego działania, a także stanu obciążenia zasobów[19]. Zgodnie z przykładowymi miesięcznymi raportami dostępności SIOEPKZ we wrześniu 2022 r. system nie był dostępny przez 7h i 5 min, co stanowi 0,98% całej dostępności systemu w tym miesiącu, w styczniu 2023 r. dostępu do SIOEPKZ nie było przez 24 min.

Biuletyn Informacji Publicznej CKE to system, w którym są udostępniane aktualne informacje publiczne CKE, takie jak np. podstawowe informacje o jednostce (status prawny, dane teleadresowe, kierownictwo), organizacja CKE (statut CKE, Regulamin Organizacyjny CKE, zakresy działania wydziałów i innych komórek organizacyjnych Komisji), zakres działalności CKE, sposób załatwiania spraw.

Obowiązek utworzenia urzędowego publikatora teleinformatycznego, jakim jest BIP CKE, wynika z przepisów art. 8 ust. 1 i 2[20] ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej*. CKE jako podmiot, o którym mowa w art. 4 ust. 1 pkt 5[21] tej ustawy, wykonujący zadania publiczne zobowiązany jest do publikowania informacji w Biuletynie Informacji Publicznej. Publikator ten tworzony jest w formie elektronicznej i udostępniany pod adresami witryn internetowych poszczególnych podmiotów. System ten został utworzony w 1999 r., jest dostępny publicznie bez logowania.

---

[16] Service Level Agreement (SLA) – to umowa pomiędzy dostawcą usług informatycznych a odbiorcą. Umowa SLA opisuje usługę informatyczną, dokumentuje docelowy poziom świadczenia usługi, określa obowiązki dostawcy usług informatycznych i odbiorcy.

[17] Gwarant pierwszego stopnia – podmiot aktualnie zobowiązany warunkami gwarancji w zakresie aplikacji wobec Zamawiającego (CKE).

[18] Operator Rządowej Chmury Obliczeniowej (Ministerstwo Cyfryzacji).

[19] Przykładowe raporty dzienne z monitorowania SIOEPKZ z 02.06.2022 r. i 02.06.2023 r.

[20] 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.

[21] 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.

W okresie objętym kontrolą obowiązywała umowa nr CKE-WAG/ZOI/107/2022 zawarta 22 grudnia 2022 r. pomiędzy CKE a podmiotem zewnętrznym, której przedmiotem była rokroczna subskrypcja na korzystanie z systemu gwarantującego prowadzenie strony Biuletynu Informacji Publicznej CKE pod adresem: https://bip.cke.gov.pl/. W umowie określono m.in. wymagania dotyczące usług hostingowych. Operator zobowiązał się do bezawaryjnego działania systemu wraz z gwarancją podjęcia wszelkich działań zapewniających najwyższą jakość usług, w tym określił dopuszczalny czas niedostępności systemu wynoszący nie dłużej niż 8 godzin i nie częstszy niż raz na sześć miesięcy.

W CKE ustalone zostały procedury, które określają właściciela merytorycznego usług (komórka organizacyjna podmiotu) odpowiedzialnego za zapewnienie obsługi informatycznej. Zgodnie z *Regulaminem organizacyjnym Centralnej Komisji Egzaminacyjnej* stanowiącym załącznik do zarządzenia nr 848 Dyrektora CKE z dnia 10 września 2020 r.:

- za koordynację działań Komisji związanych z funkcjonowaniem SIOEPKZ,
- za nadzór nad witryną internetową oraz Biuletynem Informacji Publicznej Komisji odpowiada Zespół Obsługi Informatycznej (dalej: ZOI).

W badanym zakresie nie stwierdzono nieprawidłowości.

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

  Na podstawie informacji z CKE - kodowanie znaków w plikach, które po pobraniu mogą być poddane edycji, odbywa się według standardu Unicode UTF-8.

  W badanym zakresie nie stwierdzono nieprawidłowości.

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

  Na podstawie informacji zawartych na stronie BIP CKE oraz dokumentacji technicznej systemu SIOEPKZ ustalono, że zasoby informacyjne systemów objętych kontrolą udostępniane są w nw. formatach:
  - *System Informatyczny Obsługi Egzaminów Potwierdzających Kwalifikacje w Zawodzie* – pliki są przechowywane w aplikacji w formacie dostarczonym przez użytkownika. Aplikacja umożliwia wprowadzenie następujących typów plików:
    - audio/wideo: .wav, .mp3, .avi, .mpg, .mpeg, .mp4, .m4a, .mpeg4, .ogg, .ogv, .wmv, .webm;
    - tekstowe: .txt, .rtf, .pdf, .xps, .odt, .ods, .odp, .doc, .xls, .ppt, .docx, .xlsx, .pptx, .csv;
    - graficzne: .jpg, .jpeg, .tiff, .tif, .geotiff, .mpg, .svg;
    - kompresji: .zip, .tar, .gz, .gzip, .7z;
    - stron www: .html, .xhtml, .css;
    - struktura i wizualizacji dokumentu: .xml, .xsd, .gml, .rng, .xsl, .xslt.
  - *Biuletyn Informacji Publicznej CKE* – udostępnia dane w formatach: .doc, .docx, .gif, .jpg (-jpeg), .ods, .odt, .pdf, .png, .rtf, .svg, .tif (.tiff), .txt, .xls, .xlsx, .xml.

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.

- Zgodnie z § 20 ust. 1 rozporządzenia KRI - *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.*

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

  W zakresie Systemu Zarządzania Bezpieczeństwem Informacji w CKE obowiązywało zarządzenie nr 978 dyrektora Centralnej Komisji Egzaminacyjnej z 07.03.2022 r. *w sprawie ustalenia Systemu Zarządzania Bezpieczeństwem Informacji w Centralnej Komisji Egzaminacyjnej*.
  Zgodnie z tym zarządzeniem na dokumentację SZBI składają się: polityki, regulaminy, zasady, procedury, standardy (wykaz stanowi załącznik nr 1 do ww. zarządzenia), tj.:
  1. *Polityka Bezpieczeństwa Informacji* (dalej: PBI) - określająca strategię, podstawy przetwarzania i zobowiązania do przestrzegania zasad bezpieczeństwa.
  2. *Regulamin Bezpieczeństwa Informacji* (dalej: RBI) - stanowiący zestaw zasad postępowania dla osób mających dostęp do informacji chronionych CKE.
  3. *Zasady Zarządzania Bezpieczeństwem Informacji* (dalej: ZZBI) - określające sposoby postępowania oraz zapewnia utrzymanie adekwatnego do ryzyka poziomu poufności, dostępności oraz integralności aktywów informacyjnych.
  4. *Polityka Bezpieczeństwa Danych Osobowych* (dalej: PBDO) - opisująca ogólne zasady ochrony danych osobowych obowiązujące w CKE, zasady zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz ochrony danych osobowych.
  5. *Polityka Bezpieczeństwa Systemu Informatycznego* (dalej: PBSI) - określająca zasady utrzymywania poufności, integralności oraz dostępności systemów teleinformatycznych. Wskazuje zasady utrzymania ciągłości aplikacji i usług informatycznych i zobowiązania do utrzymania parametrów systemów adekwatnych do działalności CKE.
  6. Zasady bezpieczeństwa informacji w relacjach z dostawcami – określające zasady postępowania dla pracowników podmiotów zewnętrznych.
  7. Deklaracja stosowania zabezpieczeń zgodnie z ISO/IEC 27001.
  8. Oświadczenie o stosowaniu zasad SZBI i zachowaniu poufności.
  9. Słownik pojęć używanych w dokumentach SZBI.

  Procedury:
  - PB-01 Procedura zarządzania ryzykiem w bezpieczeństwie informacji,
  - PB-02 Procedura nadzoru nad dokumentacją i zapisami SZBI,
  - PB-03 Procedura kontroli dostępu do informacji chronionych,
  - PB-04 Procedura audytu wewnętrznego SZBI,

- PB-05 Procedura zarządzania podatnościami systemu informatycznego,
- PB-06 Procedura zarządzania incydentami naruszenia bezpieczeństwa informacji,
- PB-07 Procedura pomiaru i monitorowania zabezpieczeń,
- PB-08 Procedura niszczenia nośników informacji oraz przekazywania do ponownego użycia,
- PB-09 Procedura przeglądu SZBI,
- PB-10 Procedura szkolenia i uświadamiania osób zaangażowanych w proces przetwarzania informacji,
- PB-11 Procedura działań korygujących i doskonalących,
- PB-12 Procedura wykonywania kopii zapasowych,
- PB-13 Procedura inwentaryzacji sprzętu i oprogramowania,
- PB-14 Procedura monitorowania systemu informatycznego,
- PB-15 Procedura wymiany informacji chronionych w formie elektronicznej,
- PB-16 Procedura nadzoru nad konfiguracją i zmianą,
- PB-17 Procedura zarządzania ciągłością działania systemu,
- PB-18 Procedura bezpieczeństwa i rozwoju oprogramowania (zatwierdzona 5.06.2023 r. przez Dyrektora CKE).

Standardy:
- SB-01 Standard pomieszczenia serwerowni,
- SB-02 Standard uwierzytelniania administratora,
- SB-03 Standardy bezpieczeństwa stacji roboczej (SB-03.0), stacji tajnej (SB-03.1) oraz stacji dla recenzentów (SB-03.2).

W CKE częścią Systemu Zarządzania Bezpieczeństwem Informacji są także wprowadzone regulacje w zakresie zarządzania ciągłością działania, tj.:
- *Polityka Ciągłości Działania* - ustanawiająca zasady zarządzania ciągłością działania dla procesów krytycznych,
- *Strategia Ciągłości Działania* - określająca wymagania ochrony CKE przed negatywnymi konsekwencjami sytuacji awaryjnych i nieprzewidzianych.

W ramach przeglądu Systemu Zarządzania Bezpieczeństwem Informacji w CKE podejmowane są odpowiednie czynności, wynikające z zapisów zawartych w *Procedurze przeglądu SZBI* (PB-09). Zgodnie z tą *Procedurą* przeglądy maja odbywać się cyklicznie nie rzadziej niż raz w roku oraz w przypadku wprowadzenia zmian w SZBI. Pełnomocnik ds. SZBI przeprowadził przegląd SZBI w terminie 14-15.12.2022 r., z którego został sporządzony raport[22]. Był to pierwszy przegląd SZBI od czasu jego wdrożenia w CKE, tj. 31.03.2022 r. W ramach przeglądu SZBI w CKE przeprowadzana jest identyfikacja nowych możliwych ryzyk oraz skuteczności wprowadzanych zabezpieczeń. Częstotliwość analizy wyników pomiarów dokonywana jest w okresach rocznych lub półrocznych, w zależności od wskaźnika bezpieczeństwa.

Zgodnie z obowiązującą w CKE *Procedurą zarządzania ryzykiem w bezpieczeństwie informacji* (PB-01) dokonano inwentaryzacji i oceny wartości poszczególnych aktywów informacyjnych, w tym czynności przetwarzania danych osobowych. Na tej podstawie przeprowadzone zostało szacowanie ryzyka. Zasady inwentaryzowania aktywów oraz klasyfikacji informacji i zasady szacowania ryzyka w bezpieczeństwie informacji z uwzględnieniem wymagań dla ochrony danych osobowych zostały opracowane w załączniku nr 3 do PB-01 *Metodyka szacowania ryzyka w bezpieczeństwie informacji*. Szacowanie podlega na określeniu ryzyka utraty poufności, integralności, dostępności

[22] Raport został sporządzony na podstawie zapisów zawartych w *Procedurze zarządzania ryzykiem w bezpieczeństwie informacji* (PB-01), obligującej Pełnomocnika ds. SZBI do przygotowania raportu z przeglądu ryzyka w bezpieczeństwie informacji oraz zgodnie z załącznikiem nr 1 do *Procedury przeglądu SZBI* (PB-09), na formularzu protokołu z przeglądu SZBI.

informacji. W CKE w przyjętej metodzie szacowania ryzyka ryzyko zależy od wartości wpływu, prawdopodobieństwa oraz klasy ochrony aktywa.

W okresie objętym kontrolą opracowane zostały dwa raporty z szacowania ryzyka dla bezpieczeństwa informacji i przetwarzania danych osobowych w CKE – w październiku 2022 r. i listopadzie 2023 r. – związane z szacowaniem ryzyka związanego z zarządzaniem bezpieczeństwa informacji oraz przetwarzaniem danych osobowych. Szczegóły dotyczące ryzyk związanych z bezpieczeństwem informacji zawarte zostały w rejestrze ryzyka, na podstawie którego doskonalony jest SZBI.

Zasady monitorowania i pomiaru zabezpieczeń aktywów informacyjnych w CKE zostały określone w *Procedurze pomiaru i monitorowania zabezpieczeń* (PB-07). Zabezpieczenia aktywów informacyjnych monitorowane są w trzech obszarach – organizacyjnym, fizycznym i technicznym. W *Procedurze* tej określone zostały mierniki i sposób ich pomiaru ze wskazaniem osób odpowiedzialnych za pomiar. Pełnomocnik ds. SZBI dokonując przeglądu SZBI przedstawia wartości z pomiarów wykonanych w ciągu roku dla wybranych bądź wszystkich mierników. Na podstawie wyników uzyskanych z pomiaru i monitorowania bezpieczeństwa informacji, Pełnomocnik ds. SZBI sporządza raport.

W okresie objętym kontrolą opracowane zostały dwa raporty związane z monitorowaniem SZBI – w październiku 2022 r. i listopadzie 2023 r. Zgodnie z informacją zawartą w tych raportach pomiar wskaźników bezpieczeństwa wdrożonego w CKE nie wykazał odchyleń od wartości oczekiwanych.

W okresie objętym kontrolą w CKE podjęte zostały działania mające na celu aktualizację regulacji wewnętrznych związanych z bezpieczeństwem informacji, tj. dokonano następujących zmian:

- *w Polityce Bezpieczeństwa Systemu Informatycznego* (kolejne wersje z 05.06.2023 r. i 23.10.2023 r.) dodano: Zasady bezpieczeństwa informacji przy korzystaniu z usług chmurowych (pkt 6.14), Analizę zagrożeń (pkt 8) oraz informacje o zasadach rozwoju oprogramowania opisanych w nowej procedurze PB-18 (pkt 13.2.12.g);
- w *Polityce Bezpieczeństwa Danych Osobowych* (wersja z 05.06.2023 r.) zmiany dotyczyły treści w zakresie obowiązków i uprawnień Inspektora Ochrony Danych Osobowych (dalej: IOD), w zakresie powołania i odwołania IOD oraz jego podległości służbowej, zmianie uległ wzór upoważnienia do przetwarzania danych osobowych, a także wzór rejestru czynności przetwarzania;
- w *Zasadach Zarządzania Bezpieczeństwem Informacji* (wersje z 05.06.2023 r. i 23.10.2023 r.) zmiany dotyczyły dodania wykazu procesów CKE zależnych od podmiotów zewnętrznych i dostawców (pkt 2.2.5), aktualizacji wykazu istotnych aktów prawnych i wymagań umownych, aktualizacji pkt 12 i 19 w związku z nową procedurą PB-18 *Procedura bezpieczeństwa i rozwoju oprogramowania*, a także dodano pkt 15 związany z pozyskiwaniem i rozwojem oprogramowania;
- w *Regulaminie Bezpieczeństwa Informacji*, dokonano trzech aktualizacji (wersje z: 01.04.2022 r., 27.06.2022 r., 23.10.2023 r.),zmiany dotyczyły osoby powołanej na stanowisko Inspektora Ochrony Danych Osobowych (wersja z 01.04.2022 r. i 27.06.2022 r.) oraz zasad postępowania z informacjami na poziomie IV ochrony –dla dokumentacji archiwalnej oraz w zakresie oznaczania materiałów egzaminacyjnych (wersja z 23.10.2023 r.).

Zgodnie z *Procedurą nadzoru nad dokumentacją i zapisami* (PB-02) po opracowaniu zmian dotyczących SZBI, Pełnomocnik ds. SZBI, przekazuje propozycje zmian do dyrektora CKE, celem akceptacji. Nowa wersja dokumentacji jest publikowana w celu zapoznania z nią wszystkich osób, których dotyczy.

W CKE nowo przyjęci pracownicy zapoznają się z SZBI podpisując oświadczenie stanowiące załącznik nr 3 do zarządzenia Dyrektora CKE nr 978 z dnia 7 marca 2022 r.[23]

Kontrolujący ustalili, że SZBI jest na bieżąco monitorowany oraz aktualizowany. Monitorowaniu podlegają przyjęte wskaźniki bezpieczeństwa SZBI, kluczowe z punktu widzenia bezpieczeństwa systemu, w tym ochrony danych osobowych, aktywów informacyjnych, procesu zatrudniania, kont użytkowników w Active Directory, incydentów związanych z naruszeniami bezpieczeństwa, ciągłości działania systemu informatycznego, integralności systemu, a także jego poufności i dostępności, bezpieczeństwa fizycznego, podatności systemu informatycznego na naruszenia bezpieczeństwa wewnętrzne i zewnętrzne.

W badanym zakresie nie stwierdzono nieprawidłowości.

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

  Zgodnie z zapisami zawartymi w *Procedurze inwentaryzacji sprzętu i oprogramowania* (PB-13) do inwentaryzacji oprogramowania oraz do monitoringu stacji roboczych użytkowników, będących własnością CKE, używane jest odpowiednie oprogramowanie zarządzane i utrzymywane przez ASI. Arkusze kalkulacyjne wykorzystywane są do prowadzenia inwentaryzacji sprzętu i oprogramowania i stanowią bazę CMDB, w której gromadzone są informacje o posiadanym przez CKE sprzęcie informatycznym i oprogramowaniu służącym do przetwarzania informacji[24]. Dla elementów systemu informatycznego niepodłączonego do sieci lokalnej, inwentaryzacja wykonywana jest w formie spisu z natury. Następnie zebrane w ten sposób informacje o konfiguracji poszczególnych elementów systemu informatycznego są wprowadzane do dedykowanego oprogramowania. W okresie objętym kontrolą CKE dokonało 5 przeglądów licencji, co zostało potwierdzone *Raportami z przeglądu licencji*.

  W badanym zakresie nie stwierdzono nieprawidłowości.

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

  W CKE dokumentem związanym z szacowaniem ryzyka jest *Procedura zarządzania ryzykiem* (PB-01), której celem jest ustalenie odpowiedzialności w zakresie zarządzania ryzykiem dla aktywów informacyjnych i ochrony danych osobowych w CKE, określenie zasad klasyfikacji aktywów informacyjnych, a także określenie zasad szacowania ryzyka dla aktywów informacyjnych i ochrony danych osobowych w CKE. Utrzymanie właściwego poziomu bezpieczeństwa informacji w CKE polega na identyfikacji zagrożeń i podatności oraz stosowaniu i doskonaleniu zabezpieczeń technicznych oraz organizacyjnych aktywów CKE adekwatnych do oszacowanego ryzyka w bezpieczeństwie informacji.

---

[23] Ustalenie na podstawie oświadczenia czterech wybranych nowozatrudnionych pracowników w CKE.

[24] W CKE bazę CMDB (Configuration Management Database) stanowią wykazy komputerów, drukarek oraz oprogramowania.

Przeglądu ryzyka dokonują tzw. *Właściciele ryzyk*, którzy przekazują wyniki do Pełnomocnika ds. SZBI, odpowiedzialnego za przygotowanie raportu z przeglądu ryzyka w bezpieczeństwie informacji i przedstawienie go dyrektorowi CKE. W przypadku ryzyk na poziomie wysokim i bardzo wysokim, *Właściciel ryzyka* sporządza plan postępowania z ryzykiem. W przypadku ryzyk związanych z ochroną danych osobowych *Właściciel ryzyka* informuje IOD o ryzyku i konsultuje konieczność dokonania oceny skutków dla ochrony danych osobowych. *Właściciel ryzyka* na podstawie rekomendacji IOD i przeprowadzonej oceny skutków dla ochrony danych osobowych sporządza plan postępowania dla ryzyka na poziomie wysokim lub bardzo wysokim. Plany postępowania z ryzykiem zatwierdza Wicedyrektor CKE.

W następstwie dokonanej identyfikacji ryzyka, w okresie objętym kontrolą, zostały sporządzone *Rejestry ryzyk na rok 2022 i 2023*, w których opisano ryzyka prawdopodobne do wystąpienia wraz z możliwymi ich skutkami wraz ze wskazaniem obowiązujących mechanizmów kontrolnych w poszczególnym zakresie określających niezbędne rozwiązania organizacyjne i techniczne zabezpieczające proces przetwarzania danych, w tym danych osobowych, a także *Raport z szacowania ryzyka dla bezpieczeństwa informacji i przetwarzania danych osobowych* odpowiednio na rok 2022 i 2023.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj.:*
  - *podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;*
  - *bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

  Obowiązująca w CKE *Procedura kontroli dostępu do informacji chronionych* (PB-03), określa sposób nadawania, zmiany oraz odbierania uprawnień. Dostęp do systemu informatycznego CKE można uzyskać wyłącznie na podstawie zaakceptowanego przez kierownika komórki organizacyjnej (dalej: KKO) zakresu uprawnień na danym stanowisku pracy oraz zakresu upoważnienia do czynności przetwarzania. Uprawnienia w systemie informatycznym nadawane są na podstawie zgłoszenia KKO przesłanego do Administratora Systemów Informatycznych (dalej: ASI) i udostępnionego do wiadomości IOD. Zakres uprawnień do systemów informatycznych służących do przetwarzania danych osobowych jest zgodny z zakresem upoważnienia do przetwarzania danych osobowych[25]. W przypadku rejestrowania, wyrejestrowania, nadawania i odbierania uprawnień oraz nadawania haseł dostępu i konfiguracji drugiego składnika uwierzytelniania w systemie informatycznym nadaje ASI lub wyznaczeni pracownicy Zespołu Obsługi Informatycznej, po otrzymaniu od IOD informacji potwierdzającej nadanie użytkownikowi stosownego upoważnienia do przetwarzania danych osobowych. W systemach nadzorowanych przez Wydział Analiz Wyników Egzaminacyjnych (dalej: WAWE) uprawnienia nadawane są przez Administratora Systemów WAWE na podstawie zgłoszenia Kierownika WAWE. Każde uprawnienie nadawane pracownikowi do systemu informatycznego rejestrowane jest przez ASI.

  W sytuacji: zmiany stanowiska pracy, zakresu uprawnień pracownika, uzasadnionego podejrzenia naruszenia bezpieczeństwa systemu informatycznego przez użytkownika,

[25]Na podstawie upoważnienia nr: IOD/16/2022, IOD/14/2022, upoważnienia nr WAG.0111.III.4.2023, umowy zlecenie WEPKO/000/2023.

rozwiązania z pracownikiem umowy, uprawnienia dostępu do systemów informatycznych są odpowiednio: aktualizowane, blokowane bądź odebrane.

Zgodnie z *Procedurą kontroli dostępu do informacji chronionych* (PB-03), dostęp do poszczególnych części systemu informatycznego jest możliwy wyłącznie poprzez podanie prawidłowego identyfikatora i hasła przyznanych użytkownikowi podczas procesu nadawania uprawnień do systemu informatycznego. Jeżeli system pozwala na wykorzystanie dwuskładnikowego uwierzytelnienia (2FA) ASI konfiguruje taką funkcję.

W przypadku SIOEPKZ, dyrektor OKE udostępnia szkole, placówce lub centrum kształcenia zawodowego, pracodawcy lub podmiotowi prowadzącemu kwalifikacyjny kurs zawodowy elektroniczny system przeprowadzania egzaminu zawodowego[26]. Dla celów przeprowadzania egzaminu zawodowego OKE nadają szkołom, placówkom lub centrom kształcenia zawodowego, pracodawcom i podmiotom prowadzącym kwalifikacyjne kursy zawodowe indywidualne numery identyfikacyjne[27]. Ze względów bezpieczeństwa nieudane próby logowania do aplikacji skutkują czasową blokadą konta użytkownika.

Zgodnie z informacją przekazaną przez CKE, przeglądu uprawnień pracowników oraz współpracowników podmiotów zewnętrznych, dokonują ASI wraz z Administratorami Aplikacji, w regularnych odstępach czasu dla wszystkich systemów i aplikacji CKE, co najmniej raz na 12 miesięcy. Po zakończeniu przeglądu uprawnień tworzony jest *Raport z przeglądu uprawnień użytkowników*[28].

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:*
  - *a) zagrożenia bezpieczeństwa informacji,*
  - *b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,*
  - *c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*

  Zgodnie z wprowadzoną w CKE *Procedurą szkoleń i uświadamiania osób zaangażowanych w proces przetwarzania informacji* (PB-10), w szkoleniach wewnętrznych z zakresu SZBI oraz ochrony danych osobowych uczestniczy każdy pracownik CKE uzyskujący dostęp do aktywów informacyjnych CKE. Nowo zatrudnieni pracownicy realizują szkolenia z zasad bezpieczeństwa informacji przed rozpoczęciem przetwarzania informacji chronionych w CKE. Pracownicy pełniący kluczowe role w zakresie zapewnienia bezpieczeństwa informacji (ASI, Pełnomocnik ds. SZBI, IOD) dodatkowo uczestniczą w szkoleniach specjalistycznych, uzupełniających kompetencje w wybranych obszarach bezpieczeństwa informacji. Ponadto w CKE prowadzone są działania uświadamiające, mające charakter ciągły i realizowane są przez KKO, Pełnomocnika ds. SZBI oraz IOD. W szczególności działania te obejmują: informowanie o nowych zagrożeniach bezpieczeństwa informacji, o incydentach bezpieczeństwa informacji, o zmianach w SZBI, o aktualnych wymaganiach SZBI i zmianach w otoczeniu, o aktualnych i nowych celach SZBI.

[26] art. 44zzzd ust. 5 ustawy z dnia 7 września 1991 r. *o systemie oświaty* (Dz.U. z 2022 r. poz. 2230 z późn.zm.).
[27] art. 9c ust. 2b ustawy *o systemie oświaty*.
[28] Na podstawie raportu z przeglądu uprawnień użytkowników z dnia 14 sierpnia 2023 r.

W CKE opracowany został *Ramowy plan szkoleń w zakresie SZBI*. Na podstawie udostępnionej kontrolującym dokumentacji[29] stwierdzono, że w 2022 r. przeszkolonych zostało 150 pracowników CKE, a w 2023 r. 117 pracowników CKE.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 2 pkt 7, 9 i 11 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:*
  - *monitorowanie dostępu do informacji,*
  - *czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,*
  - *zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji (pkt 7),*
  - *zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie (pkt 9),*
  - *ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych (pkt 11).*

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

  Zgodnie z wprowadzoną w CKE *Procedurą kontroli dostępu do informacji chronionych* (PB-03), dostęp do systemu informatycznego CKE można uzyskać wyłącznie na podstawie złożonego przez KKO wniosku o nadanie uprawnień zgodnym z zakresem czynności, po podpisaniu przez Dyrektora CKE upoważnienia do przetwarzania danych osobowych, jeśli dana osoba będzie miała do nich dostęp.

  Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każda osoba musi podpisać zobowiązanie do zachowania poufności danych osobowych przetwarzanych w CKE, które jest jednocześnie potwierdzeniem, że pracownik przyjął treść upoważnienia do wiadomości, zapoznał się z *Regulaminem Bezpieczeństwa Informacji* (RB-01), znane mu są zasady bezpieczeństwa informacji i przetwarzania danych osobowych, a ponadto zasady te akceptuje i zobowiązuje się ich przestrzegać.

  W sytuacji zmiany stanowiska lub zakresu uprawnień pracownika stosuje się odpowiednio zasady nadawania uprawnień celem aktualizacji uprawnień. W sytuacji, gdy z pracownikiem rozwiązywana jest umowa, odebranie uprawnień odbywa się poprzez złożenie przez KKO wniosku o odebranie uprawnień. W przypadku podmiotów

[29] Udostępniona dokumentacja obejmowała:
1) raporty z przeprowadzonych szkoleń pracowników CKE w latach 2022-2023 dotyczących bezpieczeństwa informacji i ochrony danych osobowych,
2) umowę nr CKE-WAG/15/2023 zawartą na organizację szkoleń w dniach 8.11.2023 r. i 15.11.2023 r. pn. *„System Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001:2022 w Centralnej Komisji Egzaminacyjnej”* wraz z certyfikatami udziału uczestników w szkoleniu,
3) umowę nr CKE-WAG/ZOI/44/2023CKE zawartą na przeprowadzenie w okresie 19-21 lipca 2023 r. szkolenia specjalistycznego wraz z certyfikatami udziału uczestników w szkoleniu,
4) Certyfikat PCC-CERT poświadczający uzyskanie przez pracownika CKE tytułu Pełnomocnika i Audytora Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001:2022.

zewnętrznych zakres uprawnień w poszczególnych systemach i aplikacjach ustawia się adekwatnie do przedmiotu umowy i zakresu powierzonych danych osobowych.

Każda umowa związana z przetwarzaniem aktywów informacyjnych CKE musi być zweryfikowana pod kątem zgodności z przepisami przez prawników CKE.

Pracownicy i współpracownicy podmiotów zewnętrznych świadczący lub dostarczający usługi związane z dostępem do aktywów informacyjnych CKE muszą być zapoznani z dokumentem *Zasady bezpieczeństwa informacji w relacjach z dostawcami*. Wyjątek mogą stanowić dostawcy usług, których zasady bezpieczeństwa świadczonych przez nich usług zostały zaakceptowane przez Dyrektora CKE.

Dostęp do poszczególnych części systemu informatycznego jest możliwy wyłącznie poprzez podanie prawidłowego identyfikatora i hasła przyznanych użytkownikowi podczas procesu nadawania uprawnień do systemu informatycznego. Jeżeli dany system pozwala na wykorzystanie dwuskładnikowego uwierzytelnienia (2FA), ASI ma możliwość konfiguracji takiej funkcji.

W SIOEPKZ cała wymiana danych pomiędzy serwerem IIS a użytkownikiem końcowym jest szyfrowana, co stanowi zabezpieczenie przed utratą danych wrażliwych.

W CKE prowadzona jest również kontrola dostępu fizycznego. Przetwarzanie danych w systemie jest prowadzone wyłącznie w pomieszczeniach odpowiednio zabezpieczonych przed nieuprawnionym dostępem, uszkodzeniem bądź zniszczeniem sprzętu i danych systemu informatycznego. Ponadto w CKE wprowadzony został *Standard pomieszczenia serwerowni* (SB-01), określający minimalne wymagania dotyczące pomieszczeń, w których znajdują się serwerownie. Standard ten określa zabezpieczenia pomieszczeń przed utratą danych.

Zasady zabezpieczenia dostępu do zasobów CKE zlokalizowanych w kolokacji zarządzanej przez firmę zewnętrzną określono w zawartych umowach[30] z dostawcą usługi kolokacji.

W CKE prowadzona jest ewidencja zdarzeń (rejestr incydentów bezpieczeństwa informacji) wraz z ich kategoryzacją w zakresie naruszenia danych lub informacji[31], zgodnie z załącznikiem nr 4 do *Procedury zarządzania incydentami naruszenia bezpieczeństwa informacji* (PB-06).

W badanym zakresie nie stwierdzono nieprawidłowości.

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

  W dokumencie *Zasady Zarządzania Bezpieczeństwem Informacji* określony został m.in. dostęp zdalny do systemów informatycznych CKE. Dostęp zdalny odbywa się z wykorzystaniem szyfrowanych kanałów VPN FortiGate. W przypadku połączenia do zasobów dostępnych ze strony Internetu, bez konieczności stosowania kanałów VPN wymagane jest stosowanie uwierzytelnienia 2FA. Zasady nadawania i zabezpieczenia dostępu zdalnego zostały określone w *Procedurze kontroli dostępu do informacji chronionych* (PB-03), w załączniku nr 1 do tej procedury – *Zasady zabezpieczenia dostępu zdalnego*, jak również w RBI. ZOI prowadzi wykaz osób oraz wykaz podmiotów zewnętrznych

[30] Umowa nr CKE-WAG/ZOI/94/2022 i umowa nr CKE-ZOI/65/2023.

[31] *Ewidencja Zdarzeń* zawierająca zdarzenia, które wystąpiły w CKE w okresie od 07.12.2022 r. do 28.02.2023 r.

posiadających dostęp zdalny do zasobów systemu informatycznego CKE. Konta dostępu zdalnego są monitorowane co najmniej raz na miesiąc.

Zarządzeniem nr 1060 z dnia 4 kwietnia 2023 r. dyrektor CKE ustanowił *Regulamin pracy zdalnej w CKE*, zgodnie z którym obowiązkiem pracownika wykonującego pracę zdalną jest ochrona wszelkich informacji, których ujawnienie mogłoby narazić Pracodawcę na szkodę, tj. wszelkich danych i informacji zawartych w dokumentach oraz na informatycznych nośnikach wykorzystywanych do pracy zdalnej, a także wszelkich danych osobowych.

W badanym zakresie nie stwierdzono nieprawidłowości.

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

  W dokumencie *Zasady bezpieczeństwa informacji w relacjach z dostawcami* (wersja v101 z 05.06.2023 r.) określono minimalne wymagania w zakresie bezpieczeństwa informacji dla dostawców, którzy na mocy zawartych umów mają dostęp do informacji chronionych, a także minimalne wymagania w zakresie zabezpieczeń systemów informatycznych dostawcy. W dokumencie zawarto:
  1) zasady postępowania dla dokumentów papierowych i danych elektronicznych zawierających informacje chronione;
  2) zasady haseł użytkowników aplikacji i systemów informatycznych wykorzystywanych do przetwarzania informacji chronionych;
  3) zasady zabezpieczeń komputerów zawierających informacje chronione;
  4) zasady zabezpieczania komputerów przenośnych zawierających informacje chronione;
  5) wymagania wobec dostawców usług zarządzanych zewnętrznie w tym w chmurze;
  6) metody ochrony komercyjnych aplikacji internetowych;
  7) metody ochrony sieci oraz urządzeń sieciowych;
  8) procedurę zgłaszania incydentu bezpieczeństwa informacji.

  Kontrolą objęto następujące umowy z dostawcami: umowa nr 3495/DM/23, umowa nr CKE-WAG/15/2023, umowa CKE-WAG/ZOI/44/2023. W umowach tych zawarto zapisy dotyczące zapewnienia bezpieczeństwa informacji.

  W badanym zakresie nie stwierdzono nieprawidłowości.

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

Według zapisów załącznika A normy PN-EN ISO/IEC 27001, należy zidentyfikować informacje[32], aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów.[33] Informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację[34].

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[35] ma na celu zapewnienie szybkiej reakcji i podjęcie odpowiednich działań.

Wobec powyższego w CKE obowiązuje *Procedura zarządzania incydentami naruszenie bezpieczeństwa informacji* (PB-06). Każdy pracownik posiadający dostęp do aktywów informacyjnych CKE, w tym danych osobowych, zobowiązany jest do niezwłocznego powiadomienia odpowiednich osób o incydencie. Jednym z załączników do powyższej procedury jest wzór rejestrów incydentów bezpieczeństwa informacji (zał. nr 4). W CKE prowadzony jest rejestr zdarzeń[36].

W badanym zakresie nie stwierdzono nieprawidłowości.

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

[32] 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.

[33] Pkt A.8.1.1.

[34] Pkt A.8.2.1.

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

[36] Na podstawie rejestru zdarzeń, które wystąpiły w kontrolowanym okresie, tj. od 7.03.2022 r. do 28.11.2023 r.

okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.[37]
W CKE obowiązuje *Procedura audytu wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji* (PB-04), zgodnie z którą audyt wewnętrzny SZBI odbywa się cyklicznie nie rzadziej niż raz w roku.
W kontrolowanym okresie zostały przeprowadzone dwa audyty systemu zarządzania bezpieczeństwem informacji - w roku 2022 i 2023, z których sporządzone zostały raporty z audytu odpowiednio za 2022 i 2023 rok. Ogólna ocena funkcjonowania SZBI w CKE audytowanych obszarów w każdym roku była pozytywna. Nie stwierdzono niezgodności na poziomie krytycznym. Podczas audytów zostały zidentyfikowane obszary bezpieczeństwa, które powinny ulec poprawie, wydawano zalecenia oraz rekomendacje, które CKE systematycznie wdrażało.

W badanym zakresie nie stwierdzono nieprawidłowości.

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

  W *Polityce Bezpieczeństwa Systemu Informatycznego* (PBSI) (w rozdziale 13.5) określono zasady aktualizacji oprogramowania, zgodnie z którymi każde wykorzystywane w CKE oprogramowanie służące do przetwarzania danych osobowych powinno mieć wsparcie producenta w zakresie publikacji uaktualnień w szczególności poprawek związanych z bezpieczeństwem. W przypadku braku wsparcia należy oszacować ryzyka i wprowadzić działania zaradcze. W CKE ASI jest odpowiedzialny za bieżące śledzenie podatności wykorzystywanego w CKE oprogramowania oraz instalację i konfigurację systemów informatycznych zgodnie z zaleceniami producenta oprogramowania oraz najlepszymi praktykami IT. Partner technologiczny CKE, z którym zawarta została umowa

[37] 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*[37] „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.".

na utrzymanie ruchu i rozwój systemu informatycznego SIOEPKZ[38], odpowiada za wprowadzanie wszelkich zmian w tym systemie. CKE na bieżąco zleca partnerowi technologicznemu wprowadzanie zmian do SIOEPKZ, których celem jest zwiększenie bezpieczeństwa pracy w systemie, a także zwiększenie funkcjonalności systemu[39].
Zgodnie z przykładowymi raportami wykonania usługi SIOEPKZ z 2022 r. i 2023 r. w okresie od 22.08.2022 r. do 31.01.2023 r., zostało zrealizowanych ok. 1 100 zgłoszeń, które zostały podzielone ze względu na priorytet ich realizacji.

W PBSI (w rozdziale 6.12) określone zostały zasady wykorzystania zabezpieczeń kryptograficznych, zgodnie z którymi miejsca stosowania kryptografii powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi, w szczególności należy stosować zabezpieczenia kryptograficzne: na dyskach twardych komputerów przenośnych; na nośnikach danych wynoszonych poza strefy przetwarzania danych osobowych; na pendrive'ach; na nośnikach kopii zapasowych przechowywanych poza Systemem Informatycznym; na urządzeniach typu smartfon oraz tablet w aplikacjach, które przechowują dane objęte ochroną np. dane osobowe; tunelach VPN; w połączeniach z siecią WLAN; połączeniach do usług poczty elektronicznej; w załącznikach wiadomości poczty elektronicznej zawierających dane osobowe wrażliwe. Właściciel podpisu elektronicznego lub certyfikatu umieszczonego na nośniku zewnętrznym zabezpiecza go przed dostępem osób nieupoważnionych. W przypadku uszkodzenia bądź utraty podpisu elektronicznego lub certyfikatu właściwy pracownik, zawiadamia niezwłocznie ASI z podaniem okoliczności zdarzenia.

Połączenie do systemu SIOEPKZ odbywa się za pośrednictwem przeglądarki internetowej i jest odpowiednio szyfrowane. SIOEPKZ jest monitorowany w trybie ciągłym w zakresie jego poprawnego działania, a także stanu obciążenia zasobów[40].

Zgodnie z *Procedurą wymiany informacji chronionych w formie elektronicznej* (PB-15) określone zostały zasady bezpieczeństwa podczas przesyłania informacji chronionych pocztą email. W przypadku przesyłania informacji chronionych poza CKE wykorzystywane są odpowiednie mechanizmy kryptograficzne.

CKE posiada regulacje wewnętrzne, w których określono zasady tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów i zostały zawarte w *Procedurze wykonywania kopii zapasowych* (PB-12). Procedura ta m.in. określa harmonogram wykonywania kopii zapasowych oraz testów kopii zapasowych, których wyniki odnotowywane są w raportach. Podczas kontroli przedstawiono 10 raportów z wykonywanych testów kopii zapasowych.

Serwerownie i punkty dostępowe wyposażone zostały w system monitorujący parametry środowiska.[41]
W *Procedurze zarządzania ciągłością działania systemu informatycznego* (PB-17) ustalone zostały zasady postępowania w procesie zarządzania ciągłością działania i przeciwdziałanie w funkcjonowaniu systemów informatycznych w CKE oraz ochrona tych systemów przed rozległymi awariami lub katastrofami. Procedura ta określa również działania zapewniające wznowienie działania systemu informatycznego w wymaganym czasie.

W CKE wprowadzone zostały rozwiązania minimalizujące ryzyko utraty informacji w wyniku awarii - ustanowiono *Politykę Ciągłości Działania*, a także *Strategię Ciągłości Działania*, których celem jest określenie wymagań ochrony CKE przed negatywnymi

[38] Umowa nr CKE-WAG/56/2021.
[39] Protokoły z wprowadzania zmian z 15.09.2022 r. i 20.03.2023 r.
[40] Przykładowe raporty dzienne z monitorowania SIOEPKZ z 02.06. 2022 r. i 02.06.2023 r.
[41] Na podstawie rejestru testów agregatu prądotwórczego od 23.01.2023 r. do 16.02.2024 r.

konsekwencjami sytuacji awaryjnych i nieprzewidzianych, mogących dotyczyć systemów informatycznych CKE.

W jednostce przeprowadzana jest analiza wpływu na ciągłość działania procesów realizowanych w CKE, w oparciu o którą sporządzane są plany ciągłości dla systemów informatycznych. Opracowane procedury określające reakcję na zdarzenie będące poważną awarią lub katastrofą, których celem jest przywrócenie działania systemów informatycznych w wymaganym czasie, należy do ASI oraz Pełnomocnika ds. SZBI.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 ust. 4 rozporządzenia KRI - *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*

  W CKE zostały oszacowane ryzyka dla systemów informatycznych CKE. W opracowanych *Planach postępowania z ryzykiem*[42] zidentyfikowane zostały ryzyka (opisano zdarzenia powodujące ryzyko) wraz z określeniem podjętych działań oraz wskazaniem osób odpowiedzialnych za ich realizację. Potwierdzenie zrealizowania planu postępowania z danym ryzykiem było dokonywane przez Pełnomocnika ds. SZBI.

  W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 21 rozporządzenia KRI:
  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.*

  Zgodnie z PBSI (rozdział 7.2 Zasady monitorowania) system informatyczny CKE podlega monitorowaniu i ciągłemu doskonaleniu w celu identyfikacji incydentów naruszenia bezpieczeństwa oraz zapewnienia wymaganego poziomu ochrony przetwarzanych danych. Monitorowaniu podlegają wszystkie transmisje sieciowe do i z systemu informatycznego. W przypadku przetwarzania danych osobowych zakres monitorowania ustala IOD (który weryfikuje zgodności zakresu monitorowania z zasadami ochrony danych osobowych) w porozumieniu z ASI (odpowiedzialnym za nadzór nad odpowiednią konfiguracją urządzeń i oprogramowania monitorującego).

  Zasoby systemu informatycznego tworzą dziennik audytu, który jest przeglądany raz dziennie. W CKE prowadzony jest dziennik logowań do SIOEPKZ zawierający m.in.

[42] Rejestry ryzyk z lat 2022 i 2023 oraz *Plany postępowania z ryzykiem* (nr 1 - 21).

informacje o użytkowniku systemu, jak: login, rola w systemie, data logowania do systemu, wynik logowania do systemu, adres IP, z którego nastąpiło logowanie do systemu. Dodatkowo prowadzone są zapisy logów systemowych zawierające informację o nazwie maszyny wirtualnej, usłudze do której następuje logowanie, komunikat o błędzie, data wystąpienia błędu, adres IP, wpis dotyczący błędu, a także status analizy błędu przez partnera technologicznego CKE[43].

Ponadto zgodnie z wprowadzonymi w CKE Standardami (SB-02, SB-03.0, SB-03.1, SB-03.2) dotyczącymi uwierzytelniania administratora systemu informatycznego, bezpieczeństwa stacji roboczych, bezpieczeństwa stacji tajnej oraz bezpieczeństwa stacji wykorzystywanych przez recenzentów, tworzone są dzienniki (logi) związane z bezpieczeństwem informacji.

W badanym zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa badanego obszaru: pozytywna.

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

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

WCAG (Web Content Accessability Guidelines) to zbiór rekomendacji, których należy przestrzegać, aby zapewnić dostęp do treści internetowych możliwie szerokiej grupie użytkowników, włączając w to osoby niepełnosprawne. Obecnie obwiązującą wersją jest WCAG 2.1.

Biuletyn Informacji Publicznej CKE, działający pod adresem: https://bip.cke.gov.pl/.

W CKE został przeprowadzony audyt dostępności serwisu www, w ramach którego została zbadana dostępność serwisu https://cke,gov.pl (Badanie zgodności z WCAG 2.1). Wyniki z audytu przedstawiono w dokumencie pn. *„Raport z audytu dostępności serwisu www*".

System Informatyczny Obsługi Egzaminów Potwierdzających Kwalifikacje w Zawodzie działający pod adresem: epkz.cke.edu.pl jest dostępna po zalogowaniu.

W dokumentacji powykonawczej warstwy aplikacji SIOEPKZ, znajduje się zapis odnośnie zgodności aplikacji z WCAG. W dokumencie tym wymieniono działania, które zostały podjęte w celu realizacji czterech najważniejszych zasad dotyczących spełnienia wymagań WCAG, tj.:

1. Zasadę postrzegalności – spełnienie tej zasady zostało osiągnięte przez:
   - stosowanie alternatyw tekstowych i pozatekstowych treści takich jak obrazki, grafiki;
   - wprowadzenie treści opisującej dołączany dokument - dla dokumentów multimedialnych;
   - stosowanie dodatkowej kolorystyki strony, tzw. kolorystyka kontrastowa;
   - możliwość powiększania czcionki i skalowania strony.
2. Zasadę operacyjności – spełnienie tej zasady zostało osiągnięte przez zapewnienie operacyjności elementom interfejsu użytkownika oraz nawigacji. Pełne zarządzanie witryną jest możliwe poprzez przyciski klawiatur, bez czasowych ograniczeń pomiędzy

[43] CKE_RWU z września 2022 r. i stycznia 2023 r.

uderzeniami klawiszy. Wszystkie strony mają nadane tytuły oraz treści wydzielone nagłówkami, które umożliwiają przeszukiwanie strony z wykorzystaniem filtrów i wyszukiwarki. Użytkownik, za pomocą ścieżki adresowej, zawsze jest informowany o miejscu aplikacji, w którym się znajduje.
3. Zasadę zrozumiałości – spełnienie tej zasady zostało osiągnięte poprzez zrozumiałe i czytelne dla użytkownika określenie sposobu działania interfejsu,
4. Zasadę solidności – wykorzystanie do implementacji HTML 5 i zewnętrznych kontrolek TwitterBootstrap MVC zapewniają prawidłowe działania aplikacji na wielu urządzeniach/terminalach użytkownika.

Zgodnie z art. 10 ust. 7 pkt 1 ustawy o dostępności cyfrowej - *podmiot publiczny publikuje deklarację dostępności strony internetowej - na tej stronie internetowej.*
Zgodnie z art. 10 ust. 4 pkt 2 *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.*

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.*

Biuletyn Informacji Publicznej CKE, działający pod adresem: https://bip.cke.gov.pl/.

Deklaracja dostępności została zamieszczona na stronie bip.cke.gov.pl (https://bip.cke.gov.pl/deklaracja-dostepnosci) i zawiera oświadczenie nt. poziomu dostępności stron: bip.cke.gov.pl oraz o treści:
„CKE oświadcza, że jej strony internetowe są w pełni zgodne z przepisami ustawy. Niniejsze oświadczenie sporządzono dnia 2020-04-23 r. Oświadczenie sporządzono na podstawie samooceny przeprowadzonej przez podmiot publiczny w zakresie spełniania warunków dostępności cyfrowej określonych w ustawie. W szczególności strony internetowe CKE zostały ocenione pod kątem:
- *funkcjonalności, czyli właściwości stron internetowych umożliwiającej użytkownikowi skorzystanie ze wszystkich oferowanych przez nie funkcji;*
- *kompatybilności, czyli właściwości stron internetowych umożliwiającej tym stronom współpracę z możliwie największą liczbą programów, w tym z narzędziami i programami wspomagającymi osoby niepełnosprawne;*
- *postrzegalności, czyli właściwości stron internetowych umożliwiającej ich odbiór przez użytkownika za pomocą zmysłu słuchu, wzroku lub dotyku;*
- *zrozumiałości, czyli właściwości stron internetowych umożliwiającej użytkownikowi tych stron zrozumienie treści i sposobu ich prezentacji."*

Wskazana data ostatniej istotnej aktualizacji to: 17.08.2022 r.
Wskazana data ostatniego przeglądu deklaracji to: 30.03.2023 r.

Na stronie BIP CKE (https://bip.cke.gov.pl/deklaracja-dostepnosci) zamieszczono informacje dotyczące dostępności strony CKE (https://cke.gov.pl/o-komisji/dostepnosc-cyfrowa). Należy zauważyć, że zgodnie z art. 10 ust. 7 pkt 1 ustawy o dostępności cyfrowej, *podmiot publiczny publikuje deklarację dostępności strony internetowej - na tej stronie internetowej*, co oznacza, że deklaracja dostępności strony internetowej odnosi się do danej strony, nie zaś do innych stron prowadzonych przez jednostkę.

System Informatyczny Obsługi Egzaminów Potwierdzających Kwalifikacje w Zawodzie działający pod adresem: epkz.cke.edu.pl jest dostępny po zalogowaniu.

Deklaracja dostępności strony internetowej epkz.cke.edu.pl (https://epkz.cke.edu.pl/Account/Login?ReturnUrl=%2F), jest dostępna po zalogowaniu i zawiera informację, że: *„CKE oświadcza, że strona internetowa jest częściowo zgodna z przepisami ustawy, z powodu poniższych wyłączeń (…) Niniejsze oświadczenie sporządzono dnia 2019-09-23 r. Oświadczenie sporządzono na podstawie samooceny strony internetowej przeprowadzonej przez CKE."* W oświadczeniu wskazano niezgodności z przepisami ustawy oraz wyłączenia.

Wskazana data ostatniej dużej aktualizacji: 13.11.2023 r.

Ocena cząstkowa badanego obszaru: pozytywna.

Mając na uwadze ustalenia dokonane w trakcie kontroli, na podstawie art. 46 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*, przedstawiam następujące zalecenie:

- zgodnie z § 3 ust. 1 pkt 5 rozporządzenia *w sprawie sporządzania i doręczania dokumentów elektronicznych*, na stronie Biuletynu Informacji Publicznych CKE zamieścić informację o rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru.

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

Od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z upoważnienia
Ministra Edukacji

Robert Bartold
Dyrektor Generalny
/ – podpisano cyfrowo/

Potwierdzam zgodność wydruku z dokumentem wydanym w postaci elektronicznej:

Identyfikator dokumentu	2613193.10566700.9037748
Nazwa dokumentu	Wystąpienie pokontrolne - CKE.docx
Tytuł dokumentu	Wystąpienie pokontrolne - CKE
Sygnatura dokumentu	DSKKZ-WKPiE.0915.1.2023.AP.1
Skrót dokumentu	E198363F425DA00812DFCCFFFED1E13C8CAA75CE
Wersja dokumentu	1.10
Data podpisu	18.06.2024
Sygnatariusz	Robert Bartold
Stanowisko	Dyrektor Generalny
Rodzaj certyfikatu	Certyfikat kwalifikowany podpisu elektronicznego
	EZD 3.122.10.10.
Data wydruku:	19.06.2024 09:55:53
Autor wydruku:	Jakubiak-Kępińska Alicja