MINISTER EDUKACJI I NAUKI

Warszawa, 07 lipca 2022 r.

DSKKZ-WZSK.0913.1.2021.LB

Pan
dr hab. Robert T. Ptaszek
Dyrektor
Instytutu Badań Edukacyjnych

WYSTĄPIENIE POKONTROLNE

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

Na podstawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej Ministerstwo Edukacji i Nauki[1] (dalej MEiN) w terminie od 20 października 2021 r. do 21 stycznia 2022 r. przeprowadziło kontrolę w Instytucie Badań Edukacyjnych (dalej: IBE), z siedzibą w Warszawie przy ulicy Górczewskiej 8, pn. *Działanie i bezpieczeństwo wybranych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych związanych z funkcjonowaniem Zintegrowanego Systemu Kwalifikacji*.

Celem kontroli było sprawdzenie czy procedury/regulacje wewnętrzne dotyczące systemów teleinformatycznych wykorzystywanych przez IBE do realizacji zadań publicznych, zawierają odpowiednie uregulowania dzięki, którym ww. 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

[1] Zespół kontrolujący w składzie:

1. Lech Boguta, naczelnik Wydziału Zintegrowanego Systemu Kwalifikacji w Departamencie Strategii, Kwalifikacji i Kształcenia Zawodowego, kierownik zespołu kontrolującego, na podstawie następujących upoważnień: upoważnienie nr 22/2021 z 20 października 2021 r., upoważnienie nr 30/2021 z 19 listopada 2021 r. i upoważnienie nr 40/2021 z 23 grudnia 2021 r.
2. Adam Paprocki, główny specjalista w Wydziale Kształcenia Praktycznego i Egzaminowania w Departamencie Strategii, Kwalifikacji i Kształcenia Zawodowego, na podstawie następujących upoważnień: upoważnienie nr 23/2021 z 20 października 2021 r., upoważnienie nr 31/2021 z 19 listopada 2021 r. i upoważnienie nr 41/2021 z 23 grudnia 2021 r.
3. Natalia Piętak, główny specjalista w Wydziale Bezpieczeństwa w Biurze Dyrektora Generalnego, na podstawie następujących upoważnień: upoważnienie nr 24/2021 z 20 października 2021 r., upoważnienie nr 32/2021 z 19 listopada 2021 r. i upoważnienie nr 42/2021 z 23 grudnia 2021 r.
4. Iwona Włodarczyk, główny specjalista w Wydziale Kontroli dla Działu Oświata i Wychowanie w Departamencie Kontroli i Audytu, na podstawie następujących upoważnień: upoważnienie nr 25/2021 z 20 października 2021 r., upoważnienie nr 33 z 19 listopada 2021 r. i upoważnienie nr 43 z 23 grudnia 2021 r.

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.

Kontrolą objęto okres od 1 stycznia 2020 r. do 20 października 2021 r.

IBE jest instytutem badawczym działającym na podstawie ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2020 r. poz. 1383 z późn. zm.) utworzonym na mocy Zarządzenia nr 21 Ministra Edukacji Narodowej z dnia 29 czerwca 1990 r. w sprawie przekształcenia Instytutu Badań Pedagogicznych w Instytut Badań Edukacyjnych (Dz. Urz. MEN Nr 5, poz.31, z 1994 r. Nr 5, poz. 25). IBE jest jednostką nadzorowaną przez Ministra Edukacji i Nauki.

W okresie objętym kontrolą Dyrektorem IBE od 15 marca 2017 r. do 13 kwietnia 2020 r. był dr hab. Piotr Stankiewicz, następnie od 14 kwietnia 2020 r. do 31 lipca 2021 r. Dyrektorem IBE był dr hab. Łukasz Arendt, od 1 sierpnia 2021 r. stanowisko to pełni dr hab. Robert Tomasz Ptaszek.

W okresie objętym kontrolą organizację IBE określały:
a) *Statut Instytutu Badań Edukacyjnych,* zatwierdzony zarządzeniem nr 17 Ministra Edukacji Narodowej z dnia 15 maja 2017 r. w sprawie zatwierdzenia statutu Instytutu Badań Edukacyjnych w Warszawie,
b) *Zarządzenie nr 19 Ministra Edukacji i Nauki z dnia 11 grudnia 2020 r. w sprawie zatwierdzenia zmiany statutu instytutu Badań Edukacyjnych w Warszawie,*
c) *Regulamin Organizacyjny Instytutu Badań Edukacyjnych,* wprowadzony zarządzeniem nr 1/2018 z dnia 30 marca 2018 r. w sprawie wprowadzenia Regulaminu Organizacyjnego, podpisany przez Dyrektora IBE.,
d) *Zarządzenie nr 12/2021 z dnia 13 maja 2021 r.* w sprawie zmiany Regulaminu Organizacyjnego Instytutu Badań Edukacyjnych.

Zgodnie ze statutem nadanym IBE Zarządzeniem nr 17 Ministra Edukacji Narodowej z dnia 15 maja 2017 r. *w sprawie zatwierdzenia statutu Instytutu Badań Edukacyjnych w Warszawie* (Dz. Urz. MEN z 2017 r. poz. 29), IBE prowadzi interdyscyplinarne badania naukowe nad funkcjonowaniem i efektywnością systemu edukacji w Polsce.

Zgodnie z ww. Regulaminem Organizacyjnym Instytutu Badań Edukacyjnych w IBE utworzony jest Zespół ds. Systemu Kwalifikacji, który prowadzi działania wspomagające ugruntowanie systemu kwalifikacji i szerokie jego wykorzystywanie, w tym działania analityczne, badawcze i monitorujące proces wdrażania, wzmacniające dialog i zaangażowanie interesariuszy, diagnozujące drożność systemu i jego funkcjonalność z punktu widzenia różnych grup użytkowników. Ponadto proponuje rozwiązania usprawniające system i utrzymuje kontakty międzynarodowe związane z jego wdrażaniem (§ 13 ww. Regulaminu Organizacyjnego IBE). Zespołem ds. Systemu Kwalifikacji kieruje Zastępca Dyrektora ds. Zintegrowanego Systemu Kwalifikacji (§ 14 ww. Regulaminu Organizacyjnego).

W IBE utworzony jest Zespół Administracji, zgodnie z § 27 ww. Regulaminu Organizacyjnego, który wspiera zespoły w realizowanych zadaniach, w tym m.in. zapewnia łączność teleinformatyczną.

Kontrolowany obszar reguluje:

- ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 670 z późn. zm.) (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 (t.j. Dz.U. z 2017 r. poz. 2247) (dalej rozporządzenie KRI),
- ustawa z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (t.j. Dz. U. z 2020 r. poz. 226) (dalej ustawa o ZSK),
- ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2019 r. poz. 848) (dalej: ustawa o dostępności cyfrowej).

Do kontroli zostały wybrane nw. systemy, które są wykorzystywane do realizacji zadań publicznych związanych z funkcjonowaniem Zintegrowanego Systemu Kwalifikacji, tj.:

1) Zintegrowany Rejestr Kwalifikacji;
2) Portal Zintegrowanego Systemu Kwalifikacji;
3) Strona internetowa https://bip.ibe.edu.pl.

Na podstawie art. 2 ust 13 ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji, ministrem koordynatorem Zintegrowanego Systemu Kwalifikacji jest minister właściwy do spraw oświaty i wychowania.

Zintegrowany System Kwalifikacji (ZSK) to wyodrębniona część Krajowego Systemu Kwalifikacji, w której obowiązują określone w ustawie standardy opisywania kwalifikacji oraz przypisywania poziomu Polskiej Ramy Kwalifikacji do kwalifikacji, zasady włączania kwalifikacji do Zintegrowanego Systemu Kwalifikacji i ich ewidencjonowania w Zintegrowanym Rejestrze Kwalifikacji, a także zasady i standardy certyfikowania kwalifikacji oraz zapewniania jakości nadawania kwalifikacji (art. 2 ust 25 ustawy o ZSK).

Zintegrowany Rejestr Kwalifikacji (dalej: ZRK) to rejestr publiczny w rozumieniu art. 3 pkt 5 ustawy o informatyzacji, prowadzony w systemie teleinformatycznym, ewidencjonującym kwalifikacje włączone do Zintegrowanego Systemu Kwalifikacji.

Zintegrowany Rejestr Kwalifikacji został utworzony na podstawie ustawy o ZSK. ZRK udostępnia się za pośrednictwem portalu Zintegrowanego Systemu Kwalifikacji. ZRK jest rejestrem jawnym. Informacje do Zintegrowanego Rejestru Kwalifikacji przekazuje się za pośrednictwem systemu teleinformatycznego (art. 82 ustawy o ZSK).

System Informatyczny ZRK (dalej: SI ZRK) składa się z dwóch części: ZRK1 pod adresem https://rejestr.kwalifikacje.gov.pl oraz ZRK2 pod adresem https://kwalifikacje.gov.pl. Obydwa systemy posiadają swoje własne bazy danych. Pierwszy z systemów służy do składania oraz procedowania wniosków

(m.in. włączenie kwalifikacji do ZSK), drugi zaś służy do udostępniania informacji o kwalifikacjach oraz podmiotach z nimi powiązanych.

Podmiotem prowadzącym Zintegrowany Rejestr Kwalifikacji jest Instytut Badań Edukacyjnych w Warszawie (art. 82a ustawy o ZSK).

Do zadań podmiotu prowadzącego ZRK (zgodnie z art. 87 ust. 1 ustawy o ZSK) należy:

1) dokonywanie wpisów w Zintegrowanym Rejestrze Kwalifikacji i aktualizacji wpisów w Zintegrowanym Rejestrze Kwalifikacji (w zakresie określonym w art. 83);
2) dokonywanie oceny formalnej wniosków, o których mowa w art. 14 ust. 1^2 i 2, art. 31 ust. 1, art. 41 ust. 2 i art. 53 ust. 2;
3) wspomaganie podmiotu, o którym mowa w art. 14 ust. 1, w ustalaniu właściwości ministra dla rozpatrzenia wniosku, o którym mowa w art. 14 ust. 1;
4) współpraca z ministrem koordynatorem w zakresie ustalania właściwości ministrów dla rozpatrzenia wniosków, o których mowa w art. 14 ust. 1;
5) zawiadamianie podmiotów, które uzyskały uprawnienia do certyfikowania danej kwalifikacji rynkowej, o modyfikacji danej kwalifikacji rynkowej, o której mowa w art. 27 ust. 4 pkt 2, oraz o otrzymaniu przez daną kwalifikację rynkową statusu kwalifikacji archiwalnej, o którym mowa w art. 27 ust. 4 pkt 3;
6) prowadzenie portalu Zintegrowanego Systemu Kwalifikacji w części dotyczącej Zintegrowanego Rejestru Kwalifikacji;
7) ułatwianie dialogu i współdziałania różnych interesariuszy Zintegrowanego Systemu Kwalifikacji;
8) organizowanie wymiany doświadczeń w dziedzinie kwalifikacji;
9) upowszechnianie wiedzy o Zintegrowanym Systemie Kwalifikacji, w szczególności za pośrednictwem portalu Zintegrowanego Systemu Kwalifikacji;
10) przechowywanie, przez okres dwunastu lat, raportów z ewaluacji wewnętrznej, (o których mowa w art. 64 ust. 2), raportów z zewnętrznego zapewniania jakości, (o których mowa w art. 68 ust. 1), oraz sprawozdań z działalności, (o których mowa w art. 71 ust. 1 i art. 76 ust. 1).

Zintegrowany System Kwalifikacji zapewnia m.in. dostęp do informacji o kwalifikacjach możliwych do uzyskania na terytorium Rzeczypospolitej Polskiej (art. 4 ust. 4 ustawy o ZSK). Gromadzone w ZRK informacje o kwalifikacjach są dostępne za pośrednictwem portalu internetowego Zintegrowanego Systemu Kwalifikacji.

Prowadzenie przez Instytut Badań Edukacyjnych Zintegrowanego Rejestru Kwalifikacji finansowane jest ze środków Programu Operacyjnego Wiedza Edukacja Rozwój, w ramach projektów pozakonkursowych[3]. Sposób realizacji projektu zawarty jest we wniosku o dofinansowanie projektu, gdzie określono działania przewidziane do realizacji. Realizacja działań odbywa się w ramach

[2] Podmiot prowadzący zorganizowaną działalność w obszarze gospodarki, rynku pracy, edukacji lub szkoleń może wystąpić do ministra właściwego z wnioskiem o włączenie kwalifikacji rynkowej do Zintegrowanego Systemu Kwalifikacji.

[3] Projekt POWER.02.11.00-00-0001/17 „Prowadzenie i rozwój Zintegrowanego Rejestru Kwalifikacji" od 01.01.2018 r. do 30.09.2020 r ; projekt POWER.02.11.00-00-1001/20 „Prowadzenie i rozwój Zintegrowanego Rejestru Kwalifikacji (etap 2)" od 01.10.2020 r.

„Zadań”[4], –zawierających informacje m.in. na temat zadań i obowiązków poszczególnych pracowników. Za realizację działań w ramach projektu odpowiada jego Lider. Nadzór nad realizacją projektów dotyczących Zintegrowanego Systemu Kwalifikacji (w tym projektu ZRK) sprawuje Zastępca Dyrektora ds. Zintegrowanego Systemu Kwalifikacji.

Nadzór nad podmiotem prowadzącym Zintegrowany Rejestr Kwalifikacji w zakresie wykonywania ww. zadań, o których mowa w art. 87 ust. 1 ustawy o ZSK, sprawuje minister koordynator Zintegrowanego Systemu Kwalifikacji - minister właściwy do spraw oświaty i wychowania (zgodnie z art. 88 ust. 1 ustawy o ZSK).

W art. 89 ust. 1 ustawy o ZSK określono zadania ministra koordynatora Zintegrowanego Systemu Kwalifikacji. Do zadań ministra koordynatora Zintegrowanego Systemu Kwalifikacji należy m.in. prowadzenie portalu Zintegrowanego Systemu Kwalifikacji, do którego to zadania upoważnił IBE.

Ocena ogólna kontrolowanej działalności.

Na podstawie wyników kontroli pozytywnie, pomimo stwierdzonych nieprawidłowości, oceniono obszar objęty kontrolą. Nieprawidłowości dotyczyły niezamieszczenia w BIP opisu procedur obowiązujących przy załatwianiu spraw drogą elektroniczną oraz niezgodności terminów przeglądu i aktualizacji deklaracji dostępności widniejących na stronach: https://kwalifikacje.gov.pl/; https://rejestr.kwalifikacje.gov.pl/ z terminem wskazanym w ustawie o dostępności cyfrowej.

I. Interoperacyjność – wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

Wymogi dotyczące interoperacyjności systemów teleinformatycznych zostały określone w:

- art. 16 ust. 1a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne;
- § 5 ust. 2 pkt 1-4 rozporządzenia KRI.

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

IBE udostępnił elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę. Udostępniona przez IBE elektroniczna skrzynka podawacza na platformie ePUAP umożliwia przesyłanie do IBE pism w postaci elektronicznej.

Zgodnie z § 5 ust. 2 pkt 1 rozporządzenia KRI, interoperacyjność na poziomie

[4] Np. Zadanie 1 - dokonywanie wpisów w ZRK, zakładanie kont dla użytkowników zewnętrznych, obsługa użytkowników Rejestru; Ekspert kluczowy Zadania 1 pełni rolę Administratora merytorycznego ZRK; Zadanie 3 - prowadzenie portalu kwalifikacje.gov.pl; Zadanie 4 - obsługa techniczna SI ZRK, w tym portalu kwalifikacje.gov.pl., Ekspert kluczowy Zadania 4 pełni rolę Administratora technicznego ZRK.

organizacyjnym osiągana jest poprzez 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.

IBE na stronie internetowej https://kwalifikacje.gov.pl/ zamieszcza informacje umożliwiające skuteczne zapoznanie się z usługami realizowanymi na portalu. Na portalu umieszczona jest zakładka „Materiały pomocnicze (formularze/wzory dokumentów/materiały informacyjne)", w której znajdują się m.in.: poradniki, schematy, instrukcje dla poszczególnych interesariuszy.

Zgodnie z § 5 ust. 2 pkt 4 rozporządzenia KRI podmiot realizujący zadanie publiczne powinien publikować i uaktualniać w Biuletynie Informacji Publicznej opis procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

IBE w Biuletynie Informacji Publicznej nie zamieścił opisu procedur obowiązujących przy załatwianiu spraw drogą elektroniczną.

W odpowiedzi na pytanie skierowane do IBE (pismo z 2.12.2021 r.) o wskazanie, w którym miejscu na stronie Biuletynu Informacji Publicznej Instytutu Badań Edukacyjnych (https://bip.ibe.edu.pl) opublikowany został adres skrzynki ePUAP Instytutu oraz opisy procedur obowiązujących przy załatwianiu spraw drogą elektroniczną, poinformowano, że: „*Obecnie taka informacja nie jest załączona na stronie biuletynu. Platforma ePUAP umożliwia podczas składania wniosków wybranie konkretnego rodzaju skrzynki odbiorczej instytucji. Przy okazji publikacji zamówień, każdorazowo adres elektroniczny skrzynki ePUAP zamieszczany jest w dokumentacji SIWZ".*

Zgodnie z § 15 ust. 2 rozporządzenia KRI zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczenie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

W zakresie zarządzania dostarczaniem usług realizowanych przez Zintegrowany Rejestr Kwalifikacji IBE przedstawił dokument o charakterze wewnętrznym pn. *Zasady funkcjonowania w IBE Zintegrowanego Rejestru Kwalifikacji i portalu Zintegrowanego Systemu Kwalifikacji*, który jest spisem podstawowych zasad organizacji zadań związanych z prowadzeniem ZRK i portalu udostępniającego Rejestr w IBE[5]. Po rozpoczęciu kontroli w IBE opracowany został dokument wewnętrzny pn. *Instrukcja obsługi SI ZRK dla pracowników IBE posiadających uprawnienia do pracy w systemie*.

IBE wyjaśnił, że zasady zarządzania systemem teleinformatycznym ZRK wynikają z:

a) ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji określającej:
   - funkcje ZRK: ewidencjonowanie kwalifikacji włączonych do Zintegrowanego Systemu Kwalifikacji oraz składanie wniosków określonych w ustawie o ZSK,
   - zadania podmiotu prowadzącego Zintegrowany Rejestr Kwalifikacji,

[5] Zasady te zostały określone wraz z przejęciem przez IBE zadań podmiotu prowadzącego ZRK w 2018 r., a następnie zostały zaktualizowane w listopadzie 2021 przez Lidera projektu „Prowadzenie i rozwój Zintegrowanego Rejestru Kwalifikacji (etap 2)".

m.in. dokonywanie wpisów w Zintegrowanym Rejestrze Kwalifikacji i ich aktualizacja, dokonywanie oceny formalnej wniosków składanych za pośrednictwem ZRK, prowadzenie portalu Zintegrowanego Systemu Kwalifikacji w części dotyczącej Zintegrowanego Rejestru Kwalifikacji;

- zakres merytoryczny wniosków składanych za pośrednictwem ZRK, znajdujący odzwierciedlenie w odpowiednich formularzach składanych za pośrednictwem systemu teleinformatycznego ZRK,
- właściwość i zadania określonych podmiotów związane np. z rozpatrywaniem wniosków określonych w ww. ustawie.

b) dokumentów projektu PO WER, w ramach którego IBE prowadzi ZRK, z których wynikają m.in. zadania i obowiązki pracowników IBE związane z obsługą Systemu Informatycznego ZRK.

Na portalu ZSK lub dla zalogowanych użytkowników ZRK dostępne są instrukcje, wyjaśnienia dotyczące korzystania z portalu.

W ramach projektu PO WER zostały opracowane procedury opisujące sposób realizacji zadań określonych w ustawie o ZSK dla ministra koordynatora ZSK oraz ministrów właściwych. Procedury te, standaryzują sposób realizacji zadań wynikających z ustawy o ZSK, w tym zadań realizowanych za pośrednictwem SI ZRK (np. *Procedura włączania kwalifikacji do ZSK, Procedura ustalania właściwości ministra*).

W wyniku kontroli ustalono, że system informatyczny ZRK umożliwia realizację zadań publicznych określonych dla ZRK w ustawie. Zarządzanie usługami świadczonymi przez Zintegrowany Rejestr Kwalifikacji realizowane jest w sposób zapewniający ich dostarczanie na poziomie dostępności wynikającym w szczególności z przepisów ustawy o Zintegrowanym Systemie Kwalifikacji oraz zapewniający ich bezpieczeństwo.

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 ustawą o ZSK Zintegrowany Rejestr Kwalifikacji to rejestr publiczny ewidencjonujący kwalifikacje włączone do Zintegrowanego Systemu Kwalifikacji. Do tych kwalifikacji należą także kwalifikacje pełne nadawane w ramach szkolnictwa wyższego – potwierdzane dyplomami ukończenia studiów pierwszego stopnia, studiów drugiego stopnia, jednolitych studiów magisterskich oraz dyplomami doktorskimi. Każdy kierunek studiów prowadzony w danej uczelni stanowi więc odrębną kwalifikację pełną, która powinna być zewidencjonowana w ZRK.

Informacje o tych kwalifikacjach pobierane są ze Zintegrowanego Systemu Informacji o Szkolnictwie Wyższym i Nauce POL-on, prowadzonego przez Ministra Edukacji i Nauki zgodnie z art. 342 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce. System Informatyczny ZRK pobiera dane o kwalifikacjach pełnych włączonych do ZSK z systemu POL-on za pomocą inteterkonektora.

System informatyczny ZRK jest zintegrowany z profilem zaufanym, dzięki temu wnioski składane przy pomocy formularzy można podpisywać elektronicznie oraz weryfikować złożony podpis.

Zgodnie z § 16 ust. 1 rozporządzenia KRI systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

System Informatyczny ZRK jest wyposażony w oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących. System ZRK udostępnia dane dotyczące kwalifikacji oraz podmiotów z nimi powiązanych poprzez API (XML) za pośrednictwem protokołu https. Dane są dostępne dla każdego, kto posiada odpowiedni link.

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

Elektroniczny obieg dokumentów funkcjonuje w IBE na podstawie zarządzenia nr 6/2020 Dyrektora IBE z dnia 3 czerwca 2020 r. w sprawie wprowadzenia regulaminu obiegu dokumentów w ramach Systemu Obiegu Informacji – SOI, do którego załącznik stanowi Regulamin obiegu dokumentów w ramach Systemu Obiegu Informacji – SOI.

Zgodnie z § 2 ww. Regulaminu „system dokumentacji SOI jest dodatkowym sposobem dokumentowania przebiegu tworzenia, załatwienia i gromadzenia dokumentów danej sprawy w stosunku do systemu tradycyjnego - nieelektronicznego.”

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

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

Zgodnie z § 18 ust. 1 rozporządzenia KRI systemy teleinformatyczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia KRI.
Na podstawie przekazanych przez IBE wyjaśnień ustalono, że zasoby Zintegrowanego Rejestru Kwalifikacji udostępniane są w formatach .csv, .xls, .pdf, .doc.

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

Z wyjaśnień przekazanych przez IBE wynika, że system teleinformatyczny ZRK umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw w formatach *.pdf, *.doc, *.docx, należących do formatów określonych w załącznikach nr 2 i 3 do rozporządzenia KRI.

Stwierdzona nieprawidłowość:

niezamieszczenie w Biuletynie Informacji Publicznej opisu procedur obowiązujących przy załatwianiu spraw drogą elektroniczną.

Ocena cząstkowa badanego obszaru: pozytywna pomimo stwierdzonej nieprawidłowości.

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

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

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

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

W okresie objętym kontrolą, tj. od 1.01.2020 r. do 20.10.2021 r. w IBE obowiązywały nw. regulacje dotyczące systemu zarządzania bezpieczeństwem informacji:

<u>Regulacje dotyczące ochrony danych osobowych:</u>

1. Zarządzenie nr 8/2011 z dnia 10 czerwca 2011 r. w sprawie wprowadzenia polityki bezpieczeństwa, do którego załączniki stanowią:

- zał. nr 1 *Polityka Bezpieczeństwa Danych Osobowych Instytutu Badań Edukacyjnych w Warszawie*;
- zał. nr 2 *Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych Instytutu Badań Edukacyjnych*, (dalej: Instrukcja Zarządzania Systemem Informatycznym), która reguluje m.in. procedury nadawania uprawnień do przetwarzania danych osobowych, stosowane metody i środki uwierzytelniania oraz procedury związane z zarządzaniem upoważnieniami i ich użytkowaniem, procedury tworzenia kopii zapasowych, a także zapisy regulujące sposób zabezpieczania systemu

informatycznego.

2. Ww. zarządzenie zostało zmienione Zarządzeniem nr 1/2012 z dnia 3 stycznia 2012 r. w sprawie wprowadzenia zmian w polityce bezpieczeństwa w zakresie załącznika nr 1.

   Zmiana polityki bezpieczeństwa dotyczyła dodania nowych obowiązków pracownikom IBE związanych z kontaktami z Administratorem Bezpieczeństwa Informacji w związku z przetwarzaniem danych osobowych.

3. Zarządzenie nr 10/2021 Dyrektora IBE z dnia 10 maja 2021 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w IBE oraz Procedury postępowania z naruszeniami w IBE, do którego załączniki stanowią:
   - zał. nr 1 *Polityka Bezpieczeństwa Danych Osobowych w IBE,* której celem jest zapewnienie szczególnej ochrony interesów osób, których dane osobowe przetwarzane są w IBE, a w szczególności zapewnienie, aby dane te były przetwarzane zgodnie z prawem i zbierane dla oznaczonych, zgodnych z prawem celów oraz przechowywane w sposób umożliwiający identyfikację osób, których dane dotyczą. Polityka ta ma na celu zapewnienie bezpieczeństwa procesu przetwarzania danych osobowych poprzez identyfikację potencjalnych zagrożeń oraz opracowanie, wdrożenie i stałe monitorowanie funkcjonowania mechanizmów i uregulowań umożliwiających minimalizację i eliminację tych zagrożeń;
   - zał. nr 2 *Procedury postępowania z naruszeniami w IBE*.

4. Zarządzenie Dyrektora IBE nr 28/2021 z dnia 17 sierpnia 2021 r. w sprawie wprowadzenia Procedury nadawania upoważnień do przetwarzania danych osobowych w IBE, do którego załącznik stanowi *Procedura nadawania upoważnień do przetwarzania danych osobowych w IBE.*

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

1. Zarządzenie nr 2/2020 z dnia 15 maja 2020 r. w sprawie zasad korzystania ze sprzętu komputerowego, do którego załącznik stanowią *Zasady korzystania przez pracowników IBE ze sprzętu komputerowego*.

   Ww. Zarządzenie zostało zmienione Zarządzeniem nr 19/2020 Dyrektora IBE z dnia 2 listopada 2020 r. w sprawie zmian *Zasad korzystania przez pracowników IBE ze sprzętu komputerowego*. Wprowadzona zamian dotyczy przyporządkowania zadań; zadania dotychczas przypisane Zespołowi Wsparcia Projektów zostały przyporządkowane Zespołowi Administracji.

2. Zarządzenie nr 16/2021 Dyrektora IBE z dnia 11 czerwca 2021 r. w sprawie wprowadzenia Regulaminu z korzystania ze służbowych aparatów telefonicznych, kart SIM oraz modemów mobilnego Internetu przez pracowników IBE, do którego załącznik stanowi:
   - *Regulamin korzystania ze służbowych aparatów telefonicznych, kart SIM oraz modemów mobilnego Internetu przez pracowników IBE*.

<u>Regulacje dotyczące inwentaryzacji:</u>

1. Zarządzenie wewnętrzne nr 24 p.o. Dyrektora IBE z dnia 5 listopada 2008 r. w sprawie wprowadzenia instrukcji inwentaryzacyjnej, do którego załącznik stanowi *Instrukcja inwentaryzacyjna.*

2. Zarządzenie nr 20/2019 z dnia 22 listopada 2019 r. w sprawie powołania komisji do oceny zużytych składników majątku ruchomego w IBE.
3. Zarządzenie nr 4/2020 z dnia 20 maja 2020 r. w sprawie powołania komisji do likwidacji zużytych i zbędnych składników majątku ruchomego w IBE.
4. Zarządzenie nr 23/2020 Dyrektora IBE z dnia 27 listopada 2020 r. w sprawie przeprowadzenia inwentaryzacji.

Regulacje z zakresu ochrony fizycznej:

1. Umowa monitoringu nr 29/2008 zawarta w dniu 11 lipca 2008 r. wraz z aneksem nr 1 z dnia 19 października 2010 r., aneksem nr 2 z dnia 7 czerwca 2011 r., aneksem nr 3 z dnia 2 lutego 2015 r. oraz aneksem nr 4 z dnia 3 listopada 2020 r. Aneksy nr 1, nr 2 i nr 4 dotyczyły aktualizacji listy pracowników IBE, którzy powiadamiani są o alarmie, natomiast aneks nr 3 dotyczył rozbudowy lokalnego systemu ochrony, tj. zamontowania dwóch kamer oraz rejestratora obrazu z tych kamer.
2. Zarządzenie nr 24/2021 Dyrektora IBE z dnia 23 lipca 2021 r. w sprawie wprowadzenia Regulaminu monitoringu wizyjnego w IBE, do którego załącznik stanowi *Regulamin monitoringu wizyjnego w IBE.*
3. Zarządzenie nr 25/2021 Dyrektora IBE z dnia 26 lipca 2021 r. w sprawie wprowadzenia Regulaminu korzystania z systemu kontroli dostępu oraz wydawania i użytkowania kart dostępu w IBE, do którego załącznik stanowi *Regulamin korzystania z systemu kontroli dostępu oraz wydawania i użytkowania kart dostępu w IBE*.

W IBE obowiązuje także Zarządzenie nr 6/2020 Dyrektora IBE z dnia 3 czerwca 2020 r. w sprawie wprowadzenia regulaminu obiegu dokumentów w ramach Systemu Obiegu Informacji – SOI, do którego załącznik stanowi *Regulamin obiegu dokumentów w ramach Systemu Obiegu Informacji – SOI.*

Zgodnie z wyjaśnieniami przekazanymi przez Dyrektora IBE jednostka aktualizuje i doskonali posiadaną dokumentację. W następstwie przeprowadzonej w 2019 r. i 2020 r. analizy ryzyka naruszeń ochrony danych, przedstawionej w dalszej części dokumentu, w związku z ustaleniami zawartymi w raportach, wdrażane są nowe rozwiązania, w tym przeprowadzana jest modernizacja infrastruktury teletechnicznej.

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.

Zagadnienia z powyższego zakresu zostały uregulowane w wewnętrznych dokumentach IBE, tj. w ww. *Instrukcji inwentaryzacyjnej*, która zgodnie z § 1 ma na celu w szczególności doprowadzenie danych wynikających z ksiąg rachunkowych do zgodności ze stanem rzeczywistym, a tym samym zapewnienie realności wynikających z nich informacji ekonomicznych oraz rozliczenie osób materialnie odpowiedzialnych za powierzone im mienie, również w razie zwolnienia i zmiany osoby materialnie odpowiedzialnej oraz zdarzeń losowych.

W § 17 pkt f *Regulaminu Organizacyjnego IBE* wskazano, że do zadań Zespołu Informatycznego należy w szczególności: prowadzenie dokumentacji z zakresu IT, ewidencjonowanie dokumentów, umów, licencji oraz prowadzenie zestawień posiadanego przez Instytut sprzętu i oprogramowania.

Natomiast § 8 pkt aaa *Polityki Bezpieczeństwa Danych Osobowych w IBE* wskazuje, że Kierownik Zespołu Informatycznego zobowiązany jest do: inwentaryzacji sprzętu komputerowego oraz systemów informatycznych.

W § 6 *Zasad korzystania przez pracowników Instytutu Badań Edukacyjnych ze sprzętu komputerowego* zawarto nw. zapisy:
1) Zarządzanie zasobami sprzętu komputerowego Instytutu powierza się Kierownikowi Zespołu Wsparcia Projektów.
2) Sprzęt komputerowy niewydany pracownikom składowany jest w uprzednio przygotowanym w tym celu pomieszczeniu zapewniającym odpowiednie warunki przechowywania tego sprzętu oraz uniemożliwiającym dostęp osób niepowołanych.
3) Co najmniej raz w roku, jednak nie później niż do końca grudnia każdego roku, ZWP jest zobowiązany do przeprowadzenia inwentaryzacji sprzętu komputerowego należącego do Instytutu, określając jego liczbę i stan fizyczny. Z przeprowadzonej inwentaryzacji sporządza się protokół.
4) Kopię protokołu inwentaryzacji stwierdzającego braki w sprzęcie lub jego uszkodzenia fizyczne Kierownik ZWP niezwłocznie przedkłada Zastępcy Dyrektora ds. Finansowych i Zarządzania.

Zgodnie z wewnętrznymi regulacjami w okresie objętym kontrolą została przeprowadzona inwentaryzacja składników majątku ruchomego w IBE. Działania w powyższym zakresie potwierdzają następujące dokumenty przekazane w toku kontroli:
1) Zarządzenie nr 20/2019 z dnia 22 listopada 2019 r. w sprawie powołania komisji do oceny zużytych składników majątku ruchomego w IBE.
2) Zarządzenie nr 4/2020 z dnia 20 maja 2020 r. w sprawie powołania komisji do likwidacji zużytych i zbędnych składników majątku ruchomego w IBE wraz z protokołem likwidacji składników majątku ruchomego zaakceptowanym przez Dyrektora IBE.
3) Zarządzenie nr 23/2020 Dyrektora IBE z dnia 27 listopada 2020 r. w sprawie przeprowadzenia inwentaryzacji.
4) Sprawozdanie Komisji Inwentaryzacyjnej z dnia 15 stycznia 2021 r. zatwierdzone przez Dyrektora IBE.

Uwaga:
W trakcie kontroli IBE przedstawił informację na temat posiadanych aktywów informatycznych (zasobów sprzętowych, używanego oprogramowania). W ocenie kontrolerów należy rozważyć wprowadzenie w IBE bazy danych zarządzania konfiguracją - CMDB[6], zawierającej informacje o wszystkich aktywach informatycznych, w tym: szczegółowych danych o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, aktualnej konfiguracji i relacjach między elementami konfiguracji. Zgodnie z najlepszymi praktykami zarządzania usługami informatycznymi baza konfiguracji CMDB jest

[6] CMDB – z ang. *Configuration Management Database*

podstawowym narzędziem umożliwiającym skuteczne kontrolowanie, doskonalenie i zarządzanie zasobami informatycznymi organizacji.

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 IBE wprowadzono regulacje wewnętrzne dotyczące tematyki ryzyka naruszeń ochrony danych.

Zgodnie z § 5 ust. 14 pkt cc *Polityki Bezpieczeństwa Danych Osobowych w IBE* (Zarządzenie nr 10/2021 Dyrektora IBE z dnia 10 maja 2021 r.) w szczególności do zadań Inspektora należą koordynacja procesu analizy i oceny ryzyka związanego z przetwarzaniem danych osobowych z uwzględnieniem zabezpieczeń systemu informatycznego, w tym proponowanie Administratorowi mechanizmów ochrony i środków bezpieczeństwa.

Zgodnie z §17 *Polityki Bezpieczeństwa Danych Osobowych w IBE:*

- Administrator, wdrażając odpowiednie środki techniczne i organizacyjne, uwzględnia stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia po to, aby przetwarzanie odbywało się zgodnie z RODO i aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
- Analizy ryzyka należy dokonywać: a) cyklicznie; www) w razie zmiany charakteru, zakresu, kontekstu lub celu przetwarzania; xxx) w razie przetwarzania danych w nowym celu.

W przypadku, gdy analiza ryzyka wykaże umiarkowane, wysokie lub bardzo wysokie ryzyko naruszenia praw lub wolności osób fizycznych konieczne jest niezwłoczne podjęcie adekwatnych środków minimalizujących ryzyko.

W 2019 i w 2020 r. roku na zlecenie IBE wykonano szacowanie ryzyka naruszeń ochrony danych przez dwóch usługodawców zewnętrznych. Obie firmy przedstawiły raporty, w których opisane zostały zidentyfikowane ryzyka, a także plany postępowania z ryzykiem.

Zgodnie z przekazanymi przez IBE informacjami sukcesywnie podejmowane są działania minimalizujące zidentyfikowane ryzyka. Do czasu zakończenia kontroli przeprowadzono remont infrastruktury IT i rozpoczęto aktualizację procedur.

Stosownie do **§ 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.

Zgodnie z § 6 pkt mm *Polityki Bezpieczeństwa Danych Osobowych w IBE* Administrator danych osobowych powołuje Administratora Systemu Informatycznego, który: przydziela użytkownikom indywidualne identyfikatory i hasła do Systemu Informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także blokuje konta użytkowników.

W IBE obowiązuje *Procedura nadawania upoważnień do przetwarzania danych osobowych w IBE*. Zgodnie § 2 tej regulacji, celem niniejszej Procedury jest:
a) ustalenie jednolitych zasad nadawania, zmiany zakresu i odwoływania upoważnień do przetwarzania danych osobowych w Instytucie Badań Edukacyjnych,
b) wskazanie osób odpowiedzialnych za realizację postanowień niniejszej Procedury,
c) określenie procesów związanych z nadawaniem, zmianą zakresu i odwoływaniem upoważnień.

W ww. regulacji zawarto również informacje, że Procedura ma charakter uzupełniający w stosunku do ogólnych zasad nadawania upoważnień do przetwarzania danych osobowych określonych w *Polityce Bezpieczeństwa Danych Osobowych*.

W trakcie kontroli przedłożono do wglądu rejestr upoważnień do przetwarzania danych osobowych w IBE, który jest sporządzany i aktualizowany przez Inspektora Ochrony Danych.

Użytkownicy posiadający dostęp do SI ZRK to:
- użytkownicy wewnętrzni (pracownicy IBE obsługujący ZRK),
- użytkownicy zewnętrzni (np. pracownicy ministerstw, wnioskodawcy).

Użytkownikom tym w SI ZRK przypisane są określone role a każdej roli przypisany jest odpowiedni zakres uprawnień do wykonywania czynności w SI ZRK. Role i zakresy uprawnień wynikają z ustawy o ZSK oraz dokumentów projektu PO WER. Określanie zakresu uprawnień przypisanych danej roli na poziomie całego systemu pozostaje w zakresie odpowiedzialności Administratora technicznego ZRK, w porozumieniu z Administratorem merytorycznym. Z przedstawionych wyjaśnień wynika, że poziom uprawnień do pracy w SI ZRK jest adekwatny do zakresu zadań pracowników IBE.

Zasadność posiadania uprawnienia przez „wewnętrznych" użytkowników SI ZRK sprawdzana jest na bieżąco. Zasadność dalszego posiadania uprawnień przez użytkowników „zewnętrznych" jest cyklicznie weryfikowana.

Z uwagi na publiczny charakter narzędzia rejestruje ono wszystkie czynności wykonywane w systemie. Dostępne logi pozwalają na weryfikację obszarów codziennej aktywności użytkownika.

Stosownie do § 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 § 19 pkt e *Regulaminu Organizacyjnego IBE* do zadań Zespołu Kadr należy w szczególności planowanie polityki szkoleniowej dla pracowników.
Zgodnie § 39 ust. 2 pkt b tego *Regulaminu* do zadań osoby zatrudnionej na stanowisku Inspektora Ochrony Danych należy w szczególności monitorowanie zgodności organizacji ze wszystkimi przepisami prawa dotyczącego ochrony danych, w tym audyty, działania podnoszące świadomość, a także szkolenia dla personelu zajmującego się przetwarzaniem danych.
Zgodnie z § 40 ust. 2 pkt e *Regulaminu Organizacyjnego IBE* do zadań osoby zatrudnionej na stanowisku Pełnomocnika ds. Zarządzania Zasobami Ludzkimi i Współpracy ze Związkami Zawodowymi należy w szczególności koordynowanie polityki szkoleniowej, w tym planowanie szkoleń wewnętrznych dla pracowników, organizowanie szkoleń zewnętrznych i ocena ich skuteczności.

Zgodnie z §20 *Polityki Bezpieczeństwa Danych Osobowych w IBE:*

- Wszystkie osoby, które mają zostać upoważnione do przetwarzania danych osobowych, oraz inne, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem i przetwarzaniem danych osobowych, odbywają szkolenie z zakresu ochrony tych danych.
- Osoby upoważnione do przetwarzania danych osobowych uczestniczą także obowiązkowo w szkoleniu przeprowadzanym okresowo przez Inspektora Ochrony Danych lub inną wyznaczoną osobę.
- Szkolenie uwzględnia aktualny stan przepisów, procedur, a także obowiązki tych osób w zakresie ochrony danych osobowych i zasady odpowiedzialności karnej za naruszenie bezpieczeństwa danych osobowych.

Prowadzona jest ewidencja osób uczestniczących w szkoleniach z zakresu ochrony danych osobowych:

- Inspektor cyklicznie, w ramach budowania świadomości pracowników, prowadzi akcje edukacyjne i informacyjne wśród pracowników.

Zgodnie z wyjaśnieniami przekazanymi w toku kontroli przez Inspektora Ochrony Danych (IOD) w okresie od 1 stycznia 2020 r. do dnia rozpoczęcia kontroli, tj. 20 października 2021 r. w IBE zatrudniano nowych pracowników. IOD wyjaśnił, iż zasadą jest, że każdy nowy pracownik odbywa obowiązkowe szkolenie wstępne z ochrony danych osobowych, podczas którego poruszane są kwestie zarówno z zakresu RODO, jak i te wchodzące w zakres bezpieczeństwa informacji, tj.: zasady bezpiecznego korzystania z urządzeń i systemów informatycznych i sieci, zasady stosowania haseł, obowiązki dotyczące stosowania polityki czystego biurka/ekranu/drukarki. Dodatkowo każda nowozatrudniona osoba otrzymuję od pracowników Zespołu Informatycznego wiadomość e-mail, w której przekazywana jest informacja o:

- założeniu hasła na komputer służbowy (wraz wymogiem jego długości),
- konieczności wylogowania się z poczty po zakończeniu dnia pracy,

- przechowywaniu kluczowych dokumentów na dedykowanym dysku Google.

Dowodem zapoznania pracowników z regulacjami wewnętrznymi dotyczącymi bezpieczeństwa danych przetwarzanych w IBE jest złożenie przez każdą z nowozatrudnionych osób oświadczenia o zapoznaniu się ww. regulacjami oraz zobowiązanie się do ich przestrzegania. Oświadczenie to dołączane jest do akt osobowych pracownika.

Na podstawie wyjaśnień IOD w badanym okresie szkolenia dla nowozatrudnionych pracowników były przeprowadzone. Nie została wytworzona dokumentacja z przeprowadzonych szkoleń (np. zaświadczenia, lista obecności).
W okresie objętym kontrolą w ww. „Ewidencji szkoleń" ujęte zostało szkolenie on-line pn. „Ochrona danych osobowych" dla nowozatrudnionego pracownika IBE przeprowadzone w dniu 03.09.2021 r. (przedstawiono dokumentację potwierdzającą udział w szkoleniu: prezentacja ze szkolenia oraz lista uczestników). W związku z tym, że formalne zasady dotyczące prowadzenia ewidencji szkoleń z obszaru ochrony danych oraz osób, które je odbyły wdrożono z początkiem września 2021 r., to w „Ewidencji szkoleń" ujmowane są wyłącznie szkolenia przeprowadzone od września 2021 r.

Dodatkowo zgodnie z zapisami ww. Regulaminu Organizacyjnego dotyczącymi prowadzenia akcji edukacyjnych i informacyjnych wśród pracowników IBE, Inspektor Ochrony Danych przesłał za pomocą poczty elektronicznej do wszystkich pracowników IBE nw. komunikaty:
- w dniu 18.10.2021 r. komunikat o nazwie „Zasady bezpiecznej komunikacji drogą e-mail", który dotyczył zasad prowadzenia korespondencji służbowej wyłącznie przy użyciu konta służbowego, zasad stosowania „kopii ukrytej", zabezpieczania wysyłanej informacji hasłem,
- w dniu 28.10.2021 r. (nawiązaniu do powyższego komunikatu) wysłano instrukcje w zakresie szyfrowania dokumentów.

Na podstawie wyjaśnień IOD, niezależnie od szkoleń wstępnych dla nowych pracowników oraz szkoleń tematycznych organizowanych na potrzeby realizowanych zadań, w I kwartale 2022 r. planowane jest:
- dołączenie modułu szkoleniowego „RODO i bezpieczeństwo informacji (1,5 h)" do cyklicznie realizowanych w IBE szkoleń z procedur wewnętrznych, kierowanych do ogółu pracowników;
- przeprowadzenie szkolenia „Bezpieczeństwo użytkowania systemów IT i sieci (hasła, zagrożenia, przykłady dobrych praktyk, incydenty, przykłady działań typu phishing)".

Powyższe szkolenia realizowane będą nie rzadziej niż dwa razy w roku.

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 IBE opracowano regulacje wewnętrzne, które określają zasady bezpieczeństwa przy przetwarzaniu mobilnym i pracy na odległość.

Zgodnie z § 2 ust. 5 pkt a *Polityki Bezpieczeństwa Danych Osobowych w IBE* ww. politykę stosuje się do danych osobowych przetwarzanych w sposób całkowicie lub częściowo zautomatyzowany, w szczególności w systemie informatycznym, poczcie elektronicznej, dyskach komputerów, dyskach sieciowych, pendrivach, telefonach oraz drukarkach.

Na podstawie § 8 pkt a *Polityki Bezpieczeństwa Danych Osobowych w IBE* Kierownik Zespołu Informatycznego zobowiązany jest do zarządzania systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji w sposób zapewniający bezpieczeństwo wymiany danych.

W § 17 pkt h *Regulaminu Organizacyjnego IBE* wskazano, że do zadań Zespołu Informatycznego należy w szczególności: zabezpieczenie dostępu do zasobów IT w IBE.

Natomiast zgodnie z § 2 ust. 4 *Zasad korzystania przez pracowników IBE ze sprzętu komputerowego* wykorzystywanie sprzętu komputerowego do wykonywania obowiązków służbowych poza siedzibą Instytutu wymaga uzyskania uprzedniej pisemnej zgody. Z wnioskiem o wyrażenie takiej zgody należy się zwracać do Zastępcy Dyrektora IBE ds. Finansowych i Zarządzania za pośrednictwem Zespołu Wsparcia Projektów.

Jednocześnie zgodnie z § 3 ust. 1 i 2 *Zasad korzystania przez pracowników IBE ze sprzętu komputerowego* pracownik nie jest uprawniony do instalowania na powierzonym mu sprzęcie komputerowym oprogramowania niezwiązanego z wykonywaniem obowiązków pracowniczych. Instalacja jakiegokolwiek oprogramowania dokonywana jest wyłącznie przez specjalistów ds. informatycznych wskazanych przez Instytut, po weryfikacji czy oprogramowanie, które ma zostać zainstalowane pochodzi z legalnego źródła i czy może być wykorzystywane przez Instytut.

Szczegółowe zasady bezpieczeństwa przy przetwarzaniu mobilnym i pracy na odległość zawiera również *Regulamin korzystania ze służbowych aparatów telefonicznych, kart SIM oraz modemów mobilnego Internetu przez pracowników IBE.* W § 5 ust. 1 tego *Regulaminu* wskazano, że pracownik odpowiedzialny jest za świadome i bezpieczne użytkowanie powierzonego aparatu telefonicznego, Karty SIM i/lub modemu Internetu mobilnego ze szczególną dbałością o bezpieczeństwo danych osobowych przetwarzanych przy użyciu środków łączności mobilnej.

Dokument ten reguluje obowiązki pracownika związane z korzystaniem z powierzonego mu sprzętu oraz wskazuje niepożądane działania, których nie należy podejmować z uwagi na bezpieczeństwo danych i ochronę danych przed nieuprawnionym udostępnieniem.

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 umowie nr 456/2019 zawartej z wykonawcą w dniu 16.12.2019 r., której przedmiotem było wykonanie głębokiej modernizacji nowego Systemu Informatycznego Zintegrowanego Rejestru Kwalifikacji zawarto zapisy, zgodnie z którymi SI ZRK, musi przejść zewnętrzne testy m.in. pod względem bezpieczeństwa oraz wymagań interoperacyjności, w tym WCAG.

Zgodnie z zapisami § 1 ust. 4 i 5 umowy, wykonawca zobowiązał się do świadczenia w terminie do dnia 30.06.2020 r. usług w ramach asysty technicznej w wymiarze 40 godzin miesięcznie. W ramach tej usługi zobowiązał się do naprawy błędów SI ZRK. Ze względu na bezpieczeństwo funkcjonowania SI ZRK w umowie określone zostały maksymalne czasy naprawy określonego rodzaju błędu. W przypadku błędów krytycznych czas naprawy wynosi do 8 godzin, w przypadku błędu zwykłego do 24 godzin.

Ponadto wykonawca oświadczył, że posiada niezbędne kwalifikacje i środki techniczno-organizacyjne związane z realizacją umowy (§ 4 ust. 1 pkt 1 umowy). Jednym z warunków odbioru pracy związanej z modernizacją SI ZRK był warunek dotyczący obowiązku przeprowadzenia testów zewnętrznych pod względem bezpieczeństwa, doświadczenia użytkownika (UX) podczas korzystania z produktu, a także wymagań interoperacyjności w tym WCAG. Dodatkowym zapisem umowy było zabezpieczenie Zamawiającego w postaci możliwości przeprowadzenia testu weryfikacyjnego w celu sprawdzenia czy wszystkie zgłoszone problemy zostały przez Wykonawcę usunięte (§ 7 ust. 5 umowy).

Umowa zawiera również zapisy dotyczące ochrony danych osobowych (§ 12 ust. 3 umowy), zgodnie z którymi, strony oświadczyły, że stosują środki bezpieczeństwa w szczególności środki techniczne i organizacyjne zapewniające adekwatny stopień bezpieczeństwa odpowiadającemu ryzyku związanym z przetwarzaniem danych osobowych.

Także w umowie nr 166/2020 zawartej z innym wykonawcą w dniu 01.07.2020 r. na dostarczenie usług hostingowych w oparciu o chmurę obowiązującej do 31 grudnia 2022 r., zawarto zapisy dotyczące bezpieczeństwa informacji gwarantujące, że infrastruktura udostępniona jako chmura będzie spełniała liczne wymogi bezpieczeństwa, w tym dotyczące szyfrowania informacji oraz ich zabezpieczenia przed nieuprawnionym dostępem.

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.

W IBE obowiązuje *Procedura postępowania z naruszeniami w IBE* (ww. Zarządzenie nr 10/2021 Dyrektora IBE z dnia 10 maja 2021 r.), która zawiera zasady postępowania w przypadku zidentyfikowania zdarzenia, którego skutkiem jest lub może być naruszenie bezpieczeństwa danych osobowych przetwarzanych w IBE. Procedura ta określa również zasady postępowania podczas obsługi zdarzeń związanych z bezpieczeństwem informacji, które mogą

doprowadzić do naruszenia bezpieczeństwa systemów informatycznych, w szczególności związanych z przetwarzaniem danych osobowych.

Przyjęte w ww. procedurze zasady mają na celu ograniczenie skutków wystąpienia zdarzeń godzących w bezpieczeństwo przetwarzania danych osobowych oraz zmniejszenie ryzyka ich powstania w przyszłości.

Zgodnie z ww. Procedurą w IBE prowadzony jest rejestr naruszeń bezpieczeństwa informacji (udostępniony w toku kontroli). Rejestr ten obejmuje szczegółowy opis naruszenia (w tym określenie osób, których naruszenie dotyczy, rozmiaru naruszenia, wskazania źródła oraz przyczyny powstania naruszenia), w rejestrze wskazane są również środki podjęte w związku ze zidentyfikowanym naruszeniem oraz zastosowane środki i wdrożone zalecenia.

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

Zgodnie ze *Wspólnym stanowiskiem Departamentu Informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji*[7] 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 (Dz. U. z 2013 r. poz. 885, z późn. zm.). Jak wyżej wskazano, ustawodawca nie określił sposobu, trybu, rodzaju audytu, ani też osób czy komórek organizacyjnych, którym należałoby powierzyć prowadzenie ww. audytu. Zatem decyzja co do tego, komu zostanie powierzone prowadzenie omawianego audytu, spoczywa na kierownictwie podmiotu.

W ramach realizacji obowiązków wynikających z § 20 ust. 2 pkt 14 KRI, IBE zlecił 25.05.2020 r. firmie zewnętrznej przygotowanie ekspertyzy zawierającej analizę i rekomendacje zgodności Zintegrowanego Rejestru Kwalifikacji z rozporządzaniem KRI i RODO oraz przygotowanie metodyki analizy ryzyka i polityki zarządzania ryzykiem w obszarze bezpieczeństwa informacji.

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

W ramach realizacji ww. umowy przekazany został „Raport z procesu szacowania ryzyka naruszeń ochrony danych” (ww. ekspertyza) oraz „Plan postępowania z ryzykiem” (ww. metodyka).

W Polityce Bezpieczeństwa Danych Osobowych w IBE stanowiącej załącznik nr 1 do Zarządzenia nr 10/2021 z dnia 10 maja 2021 r. wprowadzone zostały regulacje dotyczące audytów wewnętrznych w zakresie ochrony danych osobowych. Zgodnie z § 21 ust. 62 monitorowanie ochrony danych osobowych prowadzone jest:

- na bieżąco przez Inspektora Ochrony Danych;
- na bieżąco przez Kierowników Zespołów, w których przetwarzane są dane osobowe;
- poprzez audyty okresowe i doraźne (w sytuacji wystąpienia incydentów naruszenia ochrony danych) wykonywane przez Inspektora;
- podczas audytów wewnętrznych przeprowadzanych przez upoważnione podmioty.

W toku kontroli przekazano wyjaśnienia IOD w kwestii realizacji obowiązków wynikających z zapisów § 20 ust. 2 pkt 14 rozporządzenia KRI, w których zawarto, że plany, a także wstępne działania w zakresie ww. obowiązku zostały już podjęte, i tak:

- ustalono, że audyt bezpieczeństwa informacji będzie realizowany przez Zespół ds. interoperacyjności, bezpieczeństwa informacji i RODO,
- Zespół będzie wspierany w tym zadaniu przez Inspektora Ochrony Danych, który posiada Certyfikat Audytora Wewnętrznego SZBI zgodnego z normą PN-ISO/IEC 27001, wydany przez Polski Komitet Normalizacyjny,
- Dyrekcja IBE podjęła działania by zapewnić członkom zespołu szkolenia podnoszące kwalifikacje w związku z realizacją zadań związanych z wdrożeniem SZBI w IBE.

IOD poinformował również, że niezależnie od wewnętrznych audytów bezpieczeństwa informacji realizowanych przez ww. Zespół, w IBE planowany jest audyt bezpieczeństwa informacji przetwarzanych w ramach Zintegrowanego Rejestru Kwalifikacji, który zostanie przeprowadzony przez wyspecjalizowany podmiot zewnętrzny.

W listopadzie 2020 r. IOD w IBE przeprowadził analizę zgodności z RODO w IBE, która stanowi element audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, tj. minimalizowaniu ryzyka utraty informacji w wyniku awarii.

Zgodnie z § 6 pkt pp *Polityki Bezpieczeństwa Danych Osobowych w IBE* (Zarządzenie nr 10/2021 Dyrektora IBE z dnia 10 maja 2021 r.) Administrator danych osobowych powołuje Administratora Systemu Informatycznego, który: nadzoruje wykonywanie kopii zapasowych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu informatycznego.

W ww. *Polityce* w Rozdziale V zostały określone środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzania danych. Jednym ze środków ochrony technicznej jest tworzenie kopii zapasowych danych. Kopie te przechowywane są w szafie pancernej w pomieszczeniu do którego mają dostęp upoważnieni pracownicy.

Zgodnie z informacją przekazaną przez Administratora Systemu Informatycznego, za tworzenie kopii zapasowych odpowiadają administratorzy serwera oraz administratorzy sieci.

Wykonanie kopii zapasowej odbywa się zgodnie z przyjętymi przez IBE ścieżkami postępowania, które zostały zróżnicowane pod względem rodzaju kopii zapasowej, miejsca jej przechowywania, a także okresu czasowego w którym kopia jest wykonywana (kopie przechowywane są na dyskach serwera backupowego i macierzy backupowej oraz taśmach i kasetach RDX). Cały proces podlega monitorowaniu logów i ewentualnych alertów. Taśmy z backupem krytycznych systemów przechowywane są w bezpiecznej lokalizacji.

Ważnym elementem tworzenia kopii zapasowych wdrożonym w IBE jest system monitorowania sieci w tym system alertów, który przekazuje informację o niewykonanym backupie, a ta z kolei przesyłana jest do administratorów.

Poprawność działania kopii na dyskach serwera backupowego jest sprawdzana przy konfigurowaniu procesu, w przypadku reakcji na awarię oraz przy migracji serwera wirtualnego na innego hosta. Taśmy testowane są z losowej próby natomiast kasety RDX testowane są kilkukrotnie przy migracji serwera wirtualnego na innego hosta.

Uwaga:
Ustalono, że kopie na dyskach serwera backupowego nie były na bieżąco testowane, co w opinii kontrolerów mogło nie w pełni minimalizować ryzyko utraty informacji w wyniku awarii. Dobrą praktyką w tym zakresie jest testowanie kopii zapasowych danych zaraz po ich wykonaniu, co w znaczny sposób ogranicza ryzyko wystąpienia błędów związanych z tworzeniem kopii zapasowych, które mogą skutkować utratą informacji.

Zgodnie z § 15 ust. 1 rozporządzenia KRI 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.

System informatyczny ZRK składa się z dwóch części: ZRK1 pod adresem https://rejestr.kwalifikacje.gov.pl oraz ZRK2 (zmodernizowany ZRK) pod adresem https://kwalifikacje.gov.pl.

ZRK 1 służący do składania wniosków, o których mowa w ustawie o ZSK, został wykonany na podstawie umowy zawartej 22 lipca 2015 r. Umowa zobowiązywała Wykonawcę do przekazania razem z Systemem ZRK Zamawiającemu jego aktualnych kodów źródłowych. Zgodnie z opisem przedmiotu zamówienia realizacja zamówienia obejmowała testy wymagań funkcjonalnych a w ich ramach pokrycie przypadkami testowymi pełnej funkcjonalności systemu, jak również testy wymagań niefunkcjonalnych w zakresie obciążenia, wydajności, bezpieczeństwa. Moduły Systemu ZRK (Moduł obsługi formularzy, portal ZRK)

musiały zostać tak zaprojektowane, by priorytetem była ich użyteczność dla osób obsługujących (zrozumiałość, prostota obsługi, kompletność informacji).
Wykonawca zobowiązany był do dokonania analizy projektowanej architektury i późniejszych warunków eksploatacji celem wprowadzenia rozwiązań technicznych i mechanizmów techniczno- organizacyjnych zapewniających bezpieczeństwo danych zgodnie z Ustawą o ochronie danych osobowych oraz bezpieczeństwo systemu wymagane dla rejestrów publicznych dostępnych przez Internet.

Wykonawca zobowiązany był do zapewnienia w szczególności:

- zachowania przez system i dane: poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności; rozumianych zgodnie z normą ISO/IEC 27001:2005,
- identyfikacji i uwierzytelnienia użytkownika opartego także o e-PUAP lub alternatywnie poprzez: zapewnienie odrębnego identyfikatora dla każdego użytkownika, znanego tylko temu użytkownikowi hasła,
- odnotowanie przez moduł, który odpowiedzialny jest za zarządzanie użytkownikiem daty pierwszego wprowadzenia danych, a w szczególności danych osobowych,
- odnotowanie przez system modyfikacji i usunięcia danych, a w szczególności danych osobowych, identyfikatora użytkownika wprowadzającego, modyfikującego i usuwającego dane, a w szczególności dane osobowe do systemu.

Na podstawie umowy z 16 grudnia 2019 r. została wykonana modernizacja Zintegrowanego Rejestru Kwalifikacji poprzez stworzenie ZRK2 udostępniającego publicznie informacje o kwalifikacjach na stronie internetowej ZRK. Zgodnie z umową ZRK2 musiał przejść zewnętrzne testy m.in. pod względem: bezpieczeństwa; wymagań interoperacyjności, w tym WCAG. System miał zapewniać udostępnianie danych o podmiotach i kwalifikacjach poprzez API, szyfrowaną komunikację sieciową (SSL, https) oraz miał być odporny na popularne próby ataków. Z uwagi na publiczny charakter narzędzia rejestruje ono czynności wykonywane w systemie (system logów skonstruowany tak, aby informacje nie były usuwane).

W 2020 r. IBE zlecił dokonanie zewnętrznych testów bezpieczeństwa dla SI ZRK, obejmujących m.in. testy całościowe zmodernizowanego systemu ZRK. Testy dokonywane były w środowisku testowym, ujawnione podatności zostały usunięte zgodnie z dobrymi praktykami IT.

Zgodnie z § 20 ust. 2 pkt 7, pkt 9 i pkt 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:
  a) monitorowanie dostępu do informacji,
  b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
  c) 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 8);
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych (pkt 11).

W okresie objętym kontrolą, tj. od 1.01.2020 r. do 20.10.2021 r. w IBE obowiązywały regulacje dotyczące systemu zarządzania bezpieczeństwem informacji w tym: regulacje dotyczące ochrony danych osobowych, regulacje dotyczące ochrony i bezpiecznego korzystania ze sprzętu, regulacje dotyczące inwentaryzacji oraz regulacje z zakresu ochrony fizycznej.

Administrator Systemu Informatycznego wyjaśnił, że zgodnie z wewnętrznymi regulacjami, każdy komputer kliencki zabezpieczony zostaje stosownym hasłem dostępowym. Natomiast podczas konfiguracji nowego sprzętu dla pracowników wydzielane zostają konta administratorskie z dostępem dla działu IT.

Dostęp administratora do serwerów (systemów operacyjnych) realizowany jest za pomocą haseł generowanych w zewnętrznym programie przy zachowaniu odpowiednich dobrych praktyk w kontekście jego długości oraz złożoności.

W celu ochrony komputerów użytkowników wykorzystywana jest ochrona dostarczana wraz z oprogramowaniem Windows10. Funkcjonują filtry antyspamowe oraz bramy firewall.

W IBE funkcjonuje system kontroli dostępu do budynku oraz monitoring wizyjny.

Zgodnie z § 20 ust. 2 pkt 12 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.

IBE wyjaśnił, że urządzenia oraz ich oprogramowanie o znaczeniu krytycznym oraz ich bazy aktualizowane są automatycznie po dostarczeniu przez producenta oficjalnej aktualizacji.

Wszystkie maszyny serwerowe świadczące usługi zewnętrzne posiadają system redundantnego zasilania (2 oddzielne zasilacze UPS). Serwerownia wyposażona jest w dwie niezależne jednostki klimatyzacji oraz posiada moduł monitorowania parametrów fizycznych (temperatura, wilgotność, dym). W korytarzach prowadzących do pomieszczeń serwerowni funkcjonuje system monitoringu wizyjnego (kamery).

W IBE wykonywane są kopie zapasowe na różne nośniki i przechowywane są w bezpiecznej lokalizacji. Zasoby teleinformatyczne są odpowiednio monitorowane.

Zgodnie z § 20 ust. 2 pkt 12 g 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 niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa.

Z ustaleń kontroli wynika, że w lutym 2020 r. doszło do naruszenia ochrony danych osobowych polegającego na uzyskaniu nieuprawnionego dostępu do danych osobowych przetwarzanych w IBE. Okoliczności naruszenia zostały zbadane przez powołany w tym celu w IBE Zespół ds. Incydentu. Podjęte działania wyjaśniające doprowadziły do ustalenia przyczyn naruszenia. IBE dokonał szczegółowej oceny zdarzenia, przeprowadzona została analiza skuteczności środków organizacyjnych i technicznych mających zapewnić bezpieczeństwo danych osobowych w systemach informatycznych objętych naruszeniem.

W IBE przystąpiono do wdrożenia rozwiązań mających zapewnić bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w szczególności w celu zminimalizowania ryzyka ponownego wystąpienia podobnych naruszeń.

Ocena cząstkowa badanego obszaru: pozytywna.

III. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów 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 obwiązuje wersja 2.1 tych wytycznych. Wymogi określone w ww. dokumencie zostały wprowadzone w § 19 i załączniku nr 4 do rozporządzenia KRI.

Podczas kontroli IBE przekazał wykonane przez podmioty zewnętrzne raporty:

- z audytu dostępności serwisu https://rejestr.kwalifikacje.gov.pl/ z dnia 31 stycznia 2019 r.;
- z audytu dostępności wybranych podstron serwisu http://serwertest.ibe.edu.pl/ z 30 września 2019 r.;
- z audytu dostępności wybranych podstron serwisu https://www.nurte.com/ibe/portalv2/index.php/pl/ z dnia 8 czerwca 2020 r.;
- z badania dostępności strony internetowej dla osób niepełnosprawnych, starszych i innych narażonych na wykluczenie cyfrowe w oparciu o WCAG 2.0 z rozszerzeniem o aktualizację WCAG 2.1. wykonanego w dniach 10-20 sierpnia 2021 r.

Strona *rejestr.kwalifikacje.gov.pl* spełnia wytyczne WCAG 2.0, zgodnie z raportem z audytu[8] wiele reguł z wytycznych 2.1 zostało spełnionych.

Strona Zintegrowanego Systemu Kwalifikacji (https://*kwalifikacje.gov.pl*), zgodnie z raportem z audytu[9] spełnia wymagania WCAG 2.1. na poziomie AA

[8] Audyt przeprowadzony był w dniach 10-20 sierpnia 2021 r.
[9] Audyt przeprowadzony był w dniach 1-8 czerwca 2020 r.

w 48% [10].

IBE nie przedstawiło dokumentów potwierdzających spełniania wytycznych WCAG dla strony Biuletynu Informacji Publicznej IBE (https://bip.ibe.edu.pl/).

Podmiot publiczny publikuje deklarację dostępności strony internetowej – na tej stronie internetowej (art. 10 ust. 7 pkt 1 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 (art. 11 ustawy o dostępności cyfrowej).

Deklaracja dostępności została zamieszczona na stronie Zintegrowanego Systemu Kwalifikacji (https://kwalifikacje.gov.pl/) i zawiera informacje na temat poziomu dostępności tej strony internetowej. IBE udzieliło informacji, że: *W ramach realizowanych działań związanych z prowadzeniem Zintegrowanego Rejestru Kwalifikacji stale monitorowana jest kwestia dostępności cyfrowej portalu (…). Na portalu nie zostały jednak na czas zaktualizowane informacje dotyczące przeglądu deklaracji dostępności cyfrowej strony internetowej*. Widniejąca obecnie data dokonania ostatniego przeglądu deklaracji to 2.02.2022 r.

Deklaracja dostępności została zamieszczona na stronie Biuletynu Informacji Publicznej IBE (https://bip.ibe.edu.pl.) i zawiera informacje na temat poziomu dostępności tej strony internetowej. Widniejąca data dokonania ostatniego przeglądu deklaracji to 2.03.2021 r.

Deklaracja dostępności została zamieszczona na stronie Zintegrowanego Rejestru Kwalifikacji (https://rejestr.kwalifikacje.gov.pl/) i zawiera informacje na temat poziomu dostępności tej strony internetowej. Widniejąca data dokonania ostatniego przeglądu deklaracji to 31.01.2019 r.

Stwierdzona nieprawidłowość:

terminy przeglądu i aktualizacji deklaracji dostępności widniejące na stronach: https://kwalifikacje.gov.pl/, https://rejestr.kwalifikacje.gov.pl/ nie były zgodne z terminem wskazanym w ustawie o dostępności cyfrowej na ich dokonanie, tj. do dnia 31 marca każdego roku.

Ocena cząstkowa badanego obszaru: pozytywna, pomimo stwierdzonej nieprawidłowości.

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

Zalecenia:

1) Zamieszczenie w Biuletynie Informacji Publicznej Instytutu Badań Edukacyjnych opisu procedur obowiązujących przy załatwianiu spraw drogą elektroniczną;

[10] Zgodnie z informacjami zawartymi w raporcie ilość kryteriów sukcesu na poziomie A wynosiła 30, ilość kryteriów sukcesu na poziomie AA wynosiła 20, ilość przebadanych kryteriów sukcesów na poziomie A i AA wynosiła 45.

2) Dokonywanie przeglądu i aktualizacji deklaracji dostępności do dnia 31 marca każdego roku oraz niezwłocznie w każdym przypadku, gdy strona internetowa lub aplikacja mobilna podlega zmianom mogącym mieć wpływ na jej dostępność cyfrową (zgodnie z art. 11 ustawy z dnia 4 kwietnia 2019 r. *o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych*).

Wnioski:

1) W trakcie kontroli IBE przedstawił informację na temat posiadanych aktywów informatycznych (zasobów sprzętowych, używanego oprogramowania). Należy rozważyć wprowadzenie w IBE bazy danych zarządzania konfiguracją – CMDB[11], zawierającej informacje o wszystkich aktywach informatycznych, w tym: szczegółowych danych o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, aktualnej konfiguracji i relacjach między elementami konfiguracji. Zgodnie z najlepszymi praktykami zarządzania usługami informatycznymi baza konfiguracji CMDB jest podstawowym narzędziem umożliwiającym skuteczne kontrolowanie, doskonalenie i zarządzanie zasobami informatycznymi organizacji;
2) W trakcie kontroli ustalono, że kopie na dyskach serwera backupowego nie były na bieżąco testowane, co mogło nie w pełni minimalizować ryzyko utraty informacji w wyniku awarii. Należy rozważyć wprowadzenie praktyki w tym zakresie, tj. testowania kopii zapasowych danych zaraz po ich wykonaniu, co w znaczny sposób ogranicza ryzyko wystąpienia błędów związanych z tworzeniem kopii zapasowych, które mogą skutkować utratą informacji.

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 zaleceń i wykorzystaniu wniosków.

Od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z upoważnienia

MINISTRA EDUKACJI I NAUKI

Włodzimierz Bernacki

Sekretarz Stanu

/ – podpisano cyfrowo/

[11] CMDB – z ang. *Configuration Management Database*