MINISTER EDUKACJI NARODOWEJ

Warszawa, 15 października 2019 r.

BO-IOD.0915.1.2018.DK

Sz. P.
Marek Charążka
Dyrektor
Centrum Informatycznego Edukacji

WYSTĄPIENIE POKONTROLNE

Zgodnie z art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092), przekazuję niniejsze Wystąpienie pokontrolne.

Na podstawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. poz. 1092) oraz art. 26 w związku z art. 31 oraz art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, z późn. zm.)[1], dalej zwanej „ustawą z 1997 r.", a także art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE z 4.5.2016, L 119/1, z późn. zm.), dalej zwanego „RODO", Ministerstwo Edukacji Narodowej[2] w okresie od 21 maja do 31 lipca 2018 r.,

---

[1] Ustawa straciła moc w odniesieniu do kontrolowanego obszaru z dniem 25 maja 2018 r.

[2] Zespół kontrolny w składzie:

1) Aleksandra Kowalik (kierownik zespołu) na podstawie upoważnienia nr 6/2018 z dnia 16 maja 2018 r. – do dnia 31 marca 2019 r., w związku z zakończeniem pracy w MEN.
2) Daniel Kołodziejski, na podstawie upoważnienia nr 7/2018 z dnia 16 maja 2018 r.
3) Rafał Wasielewski, na podstawie upoważnienia nr 8/2018 z dnia 17 maja 2018 r.
4) Natalia Piętak, na podstawie upoważnienia nr 11/2018 z dnia 21 maja 2018 r.

przeprowadziło kontrolę w Centrum Informatycznym Edukacji (dalej: „Centrum", „CIE") z siedzibą w Warszawie przy al. J. Ch. Szucha 25.

Kontrolą objęto prawidłowość wykonywania zadań w zakresie powierzonych Centrum Informatycznemu Edukacji zbiorów danych osobowych, których administratorem jest Minister Edukacji Narodowej oraz stopnia przygotowania do wdrożenia RODO.

Kontrolą objęto okres od 1 stycznia 2017 r. do 21 maja 2018 r.

Celem kontroli była:

1) ocena prawidłowości wykonywania zadań przez CIE w zakresie powierzonych zbiorów danych osobowych, których administratorem jest Minister Edukacji Narodowej;
2) ocena stopnia przygotowania CIE do wdrożenia RODO.

Na podstawie materiału zgromadzonego w trakcie kontroli, działalność CIE w zakresie objętym kontrolą została oceniona pozytywnie, pomimo stwierdzonych nieprawidłowości, które nie miały znaczącego wpływu na obszar objęty kontrolą.

Stwierdzone nieprawidłowości dotyczyły sposobu wdrożenia niektórych środków technicznych i organizacyjnych, służących zapewnieniu ochrony danych osobowych.

CIE jest jednostką organizacyjną podległą Ministrowi Edukacji Narodowej. Od dnia 1 kwietnia 2008 r. dyrektorem CIE jest Pan Marek Charążka. W okresie objętym kontrolą przedmiot działalności CIE[3], zgodnie ze Statutem nadanym zarządzeniem nr 22 Ministra Edukacji Narodowej z dnia 21 czerwca 2017 r., obejmuje:

1) Usługi informatyczne na rzecz MEN, w szczególności:
   a) projektowanie, programowanie, uruchamianie i utrzymywanie systemów informatycznych wspomagających zarządzanie i realizację zadań,
   b) zapewnienie rozwoju i rozbudowy utrzymywanych systemów informatycznych,
   c) zapewnienie bezpieczeństwa teleinformatycznego utrzymywanych systemów informatycznych,
   d) utrzymywanie oraz dbanie o wysoki standard infrastruktury informatycznej,

---

5) Michał Jurkowski, na podstawie upoważnienia nr 12/2018 z dnia 21 maja 2018 r. – do dnia 31 sierpnia 2019 r., w związku z zakończeniem pracy w MEN.
6) Małgorzata Szczupak, na podstawie upoważnienia nr 10/2018 z dnia 16 maja 2018 r. – do dnia 14 marca 2019 r., w związku z zakończeniem pracy w MEN.

[3] We wcześniejszym okresie Statut obowiązywał w brzmieniu nadanym zarządzeniem nr 30 Ministra Edukacji Narodowej z dnia 25 października 2011 r., zmienionym zarządzeniem nr 6 Ministra Edukacji Narodowej z dnia 24 marca 2014 r. oraz zarządzeniem nr 30 Ministra Edukacji Narodowej z dnia 16 lipca 2015 r.

e) zarządzanie infrastrukturą teleinformatyczną, w tym gospodarowanie powierzonymi składnikami majątku do czasu ich zwrotu,
f) przechowywanie i udostępnianie danych archiwalnych o edukacji,
g) wykonywanie kopii zapasowych administrowanych systemów i danych,
h) zapewnianie dostępu do Internetu;

2) Utrzymanie i rozwój SIO oraz udostępnianie zgromadzonych w nim danych, na wniosek komórki organizacyjnej MEN, właściwej do spraw tego systemu;
3) Obsługę informatyczną zbiorów danych osobowych, których administratorem jest Minister Edukacji Narodowej i które są przechowywane na infrastrukturze serwerowej zarządzanej przez CIE.

Powyższe zadania obejmują swoim zakresem zapewnienie właściwej ochrony danych osobowych. Do 25 maja 2018 r., wynikały one z:

a) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, z późn. zm.),
b) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. poz. 1024),
c) zarządzenia nr 22 Ministra Edukacji Narodowej z dnia 19 maja 2016 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Edukacji Narodowej, zmienionego zarządzeniem nr 46 z dnia 30 listopada 2017 r.,
d) zarządzenia nr 28 Ministra Edukacji Narodowej z dnia 2 lipca 2015 r. w sprawie ochrony danych osobowych w Ministerstwie Edukacji Narodowej, zmienionego zarządzeniem nr 36 z dnia 27 września 2017 r.

Przedmiotem kontroli było sześć obszarów działalności CIE, związanych ze zbiorami danych osobowych, dla których administratorem jest Minister Edukacji Narodowej. Do kontroli wybrano obszary, dla których ryzyko niespełnienia warunków związanych z zachowaniem bezpieczeństwa przetwarzania danych i ewentualnych skutków oceniono na duże lub bardzo duże.

Ocenę kontrolowanej działalności uzasadniają ustalenia z kontroli.

W ramach celu 1, tj. Prawidłowość wykonywania zadań przez CIE w zakresie powierzonych zbiorów danych osobowych, których administratorem jest Minister Edukacji Narodowej, zostały skontrolowane cztery niżej przedstawione obszary.

Obszar 1
Prawidłowość zapewnienia ochrony zbiorów danych osobowych powierzonych przez MEN do przetwarzania przez CIE, zarówno w zakresie środków technicznych, jak i organizacyjnych.

W ramach tego obszaru, kontrolą objęto środki techniczne i organizacyjne, o charakterze innym niż informatyczny, stosowane przez CIE w odniesieniu do powierzonych danych.

Ustalenia:

1) CIE posiadało odpowiednią dokumentację dotyczącą przetwarzania danych (w tym politykę ochrony danych osobowych oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych), która 10 lipca 2018 r. została dostosowana do RODO.
2) CIE wydawało swoim pracownikom i osobom współpracującym upoważnienia do przetwarzania danych osobowych oraz prowadziło ewidencję osób upoważnionych. Stwierdzone w tym zakresie nieprawidłowości omówiono poniżej.
3) CIE, wykonując zadania na powierzonych danych, dokonywało również ich podpowierzania innym podmiotom, na podstawie umowy powierzenia. W związku z RODO umowy te zostały aneksowane. Stwierdzone w tym zakresie nieprawidłowości zostały omówione poniżej.
4) W CIE był prawidłowo powołany ABI. W jego umiejscowieniu w strukturze organizacyjnej CIE oraz udostępnionym zakresie obowiązków nie stwierdzono nieprawidłowości.

Stwierdzone nieprawidłowości:

1) Prowadzona przez CIE ewidencja osób upoważnionych zawierała błędy i nieścisłości[4]:
   a) w prowadzonej ewidencji nie zostali ujęci wszyscy aktualni pracownicy CIE – jedna osoba, wskazana jako administrator techniczny, w ogóle nie widniała w ewidencji,
   b) w prowadzonej ewidencji występowały oczywiste błędy (np. przypisanie loginu niewłaściwej osobie, błędnie wpisane daty obowiązywania upoważnienia),
   c) w prowadzonej ewidencji nie umieszczono wszystkich udzielonych upoważnień do przetwarzania danych osobowych (załączniki do umów nr: 6/2017, 21/2017 i 7/2018),
   d) w prowadzonej ewidencji brakowało adnotacji o zakończeniu obowiązywania upoważnienia do przetwarzania danych osobowych, które wygasło wraz z zakończeniem obowiązywania umowy CIE-251/2016, czyli 31 stycznia 2018 r. (poz. 14, 22, 23, 24, 25, 26, 27, 29 ewidencji),
   e) w prowadzonej ewidencji brakowało adnotacji o wydaniu upoważnień wszystkim osobom wskazanym jako administratorzy techniczni

[4] Zgodnie z art. 39 ustawy z 1997 r. „administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania" – przepis ten określał również niezbędne elementy tej ewidencji.

– analogiczny błąd dotyczył co najmniej dwóch osób pełniących w CIE funkcje kierownicze.

2) Brak wydanych upoważnień dla kilku osób przetwarzających dane osobowe[5]:
   a) nie wszystkie osoby fizyczne, z którymi Centrum zawarło umowy wiążące się z przetwarzaniem danych osobowych MEN, posiadały nadane upoważnienia do przetwarzania danych (dotyczy to umów nr 1/2017, nr 7/2017, nr 22/2017, nr 6/2018). Jedno upoważnienie (dotyczy umowy nr 48/2017) było udzielone „wstecz" (wydane 22 maja 2018 r., wskazując datę obowiązywania od 28 grudnia 2017 r.).
3) W kilku przypadkach brak było umów powierzenia przetwarzania danych osobowych[6]:
   a) na 60 umów, 10 umów w ocenie kontrolujących odnosi się do powierzenia przetwarzania danych osobowych, ale tylko w przypadku 4 z nich CIE podpisało odpowiednie umowy powierzenia. Natomiast w przypadku 6 umów nie zawarto umowy powierzenia przetwarzania danych (dotyczy to umów nr: 10/2017, 25/2017, 27/2017, 37/2017, 38/2017, 10/2018).

Uwaga:
W odniesieniu do umowy numer 3/2018 i 4/2018, odpowiednie umowy powierzenia przetwarzania danych osobowych, zawarte z tą samą datą co umowy główne, nieprawidłowo określały administratora danych oraz nieprecyzyjnie wskazywały przetwarzane dane osobowe. Nieścisłości te zostały jednak usunięte poprzez zawarcie nowych umów powierzenia, zawartych w związku z rozpoczęciem stosowania RODO.

Obszar nr 1 kontrolujący ocenili pozytywnie, pomimo stwierdzonych nieprawidłowości.

Obszar 2
Mechanizmy służące zapewnieniu kontroli nad wprowadzaniem danych osobowych do zbioru i nad ich przekazywaniem.

W ramach obszaru 2 kontrolą objęto 5 systemów informatycznych[7], w których zidentyfikowano największe ryzyko w zakresie przetwarzanych przez MEN danych osobowych. Sprawdzano, czy są spełnione wymogi określone w § 7

[5] Zgodnie z art. 37 ustawy z 1997 r. „do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych".
[6] Zgodnie z art. 31 ust. 1 ustawy z 1997 r. „administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych".
[7] System Informacji Oświatowej, baza RIPSDKO (Rzeczoznawcy i Podręczniki Szkolne do Kształcenia Ogólnego), baza wypoczynku, Centralny Rejestr Orzeczeń Dyscyplinarnych, system finansowo-księgowy

ust. 1 i 2 ww. rozporządzenia MSWiA, tj. czy w systemie wykorzystywanym do przetwarzania danych osobowych odnotowywane są odpowiednie informacje określone we wspomnianym przepisie.

W ramach tego obszaru sprawdzono również, czy zgodnie z § 7 ust. 1 pkt 2 Polityki bezpieczeństwa danych osobowych w Ministerstwie Edukacji Narodowej[8], realizowane było zadanie mające na celu zapewnienie w systemach informatycznych mechanizmów służących kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru danych osobowych wprowadzone oraz komu są przekazywane.

Ustalenia:

1) Wszystkie systemy zapewniają odnotowywanie, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone.
2) Wymaganie dotyczące odnotowania daty pierwszego wprowadzenia danych nie jest spełnione w bazie RIPSDKO.
3) Badane systemy nie zostały wyposażone w mechanizm, który zapewnia sporządzenie i wydrukowanie raportu, o którym mowa w § 7 ust. 3 ww. rozporządzenia MSWiA, zawierającego w powszechnie zrozumiałej formie określone informacje. Raporty takie, zgodnie z informacjami uzyskanymi od pracowników CIE, mogą zostać wykonane przy wykorzystaniu narzędzi niestandardowych.

Stwierdzona nieprawidłowość:

Zadanie określone w § 7 ust. 1 pkt 2 Polityki bezpieczeństwa danych osobowych w Ministerstwie Edukacji Narodowej dotyczące zapewnienia w systemach informatycznych mechanizmów służących kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru danych osobowych wprowadzone oraz komu są przekazywane, nie zostało w pełni wykonane. W systemach informatycznych brakuje mechanizmów służących kontroli nad tym, komu są przekazywane dane osobowe z systemów.

CIE wyjaśniło, że w administrowanych aplikacjach i stronach MEN, wprowadza na bieżąco zmiany związane z przetwarzaniem danych osobowych, zgodnie z otrzymanymi zleceniami, a także, że pracownicy CIE, w razie konieczności, proponują opiekunom merytorycznym wprowadzanie zmian w aplikacjach. Kontrolujący stwierdzili, że przedstawione dowody nie dotyczyły propozycji wprowadzenia ww. mechanizmów.

Obszar nr 2 kontrolujący ocenili pozytywnie, pomimo stwierdzonej nieprawidłowości.

---

[8] Polityka bezpieczeństwa danych osobowych w MEN stanowi załącznik nr 1 do zarządzenia nr 28 Ministra Edukacji Narodowej z dnia 2 lipca 2015 r. w sprawie ochrony danych osobowych w Ministerstwie Edukacji Narodowej, zmienionego zarządzeniem nr 36 z dnia 27 września 2017 r.

Obszar 3

Spełnianie wymogów wynikających z zarządzenia w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w MEN, w kontekście ochrony danych osobowych.

W ramach obszaru 3, kontrolą objęto realizację zadań CIE wynikających z zarządzenia Ministra Edukacji Narodowej w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Edukacji Narodowej[9], tj.:

1) zapewnienie bezpieczeństwa teleinformatycznego systemów Ministerstwa, obsługiwanych przez CIE, w tym tworzenie barier nieuprawnionego dostępu do obsługiwanych systemów teleinformatycznych[10] (badano działania o charakterze innym niż informatyczny),
2) zarządzanie lokalną siecią teleinformatyczną Ministerstwa (badano działania o charakterze innym niż informatyczny),

a także zadania pracowników CIE wymienione w załącznikach do Polityki Bezpieczeństwa Informacji MEN.
W kontekście celów kontroli analizowano również informacje otrzymane od Pełnomocnika Ministra Edukacji Narodowej do spraw bezpieczeństwa cyberprzestrzeni.

Ustalenia:

1) W CIE jest stosowana procedura zarządzania incydentami bezpieczeństwa informacji[11].
2) Ustalenia w zakresie tworzenia barier nieuprawnionego dostępu do obsługiwanych systemów teleinformatycznych (nadawanie uprawnień, udzielanie upoważnień itp.) zostały przedstawione przy ocenie obszaru 1.
3) Ustalenia w zakresie zarządzania lokalną siecią teleinformatyczną Ministerstwa zostały przedstawione przy ocenie obszaru 4.

Uwagi:

1) W rejestrze zgłoszeń znajdowały się zgłoszenia dotyczące założenia określonej osobie nowego konta, które nie zawsze zawierały imię i nazwisko osoby.
2) W 3 zgłoszeniach kontrolujący stwierdzili nadanie uprawnień (zakończenie sprawy bez adnotacji o nienadaniu uprawnień) mimo braku upoważnienia dla wymienionych osób do przetwarzania danych osobowych.
3) W rejestrze zgłoszeń nie ma możliwości weryfikacji podstaw do nadania uprawnień do określonego systemu/domeny oraz nie jest możliwe

---

[9] Zarządzenie nr 22 Ministra Edukacji Narodowej z dnia 19 maja 2016 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Edukacji Narodowej, zmienione zarządzeniem nr 46 z dnia 30 listopada 2017 r.

[10] Należy zaznaczyć, że kontrola nie obejmowała kontroli informatycznej, więc w wystąpieniu kontrolerzy opierają się jedynie na informacjach otrzymanych od CIE w tym zakresie.

[11] Procedura zarządzania incydentami bezpieczeństwa informacji stanowi załącznik nr 1 do PBI

automatyczne generowanie odbierania uprawnień zgodnie z datą zawartą na upoważnieniu lub wniosku.

Stwierdzone nieprawidłowości:

1) Niezgłoszenie incydentu w przypadku przedłużających się problemów w dostępie do systemów przez wielu pracowników. W dniach 20-22 lutego 2018 r. w rejestrze zgłoszeń odnotowano 38 zgłoszeń dotyczących awarii konta, poczty e-mail, dostępu do serwera. W rejestrze incydentów CIE z I połowy 2018 r. nie odnotowano żadnego zgłoszenia w tym zakresie. Nie odnotowano również zgłoszenia do rejestru incydentów MEN. Zdaniem zespołu kontrolnego, odnotowana liczba zgłoszeń powinna skłonić CIE do rozważenia, czy nie doszło do incydentu bezpieczeństwa informacji (poprzez niezapewnienie dostępności informacji). Zgodnie z § 6 ust. 2 procedury zarządzania incydentami bezpieczeństwa informacji[12], CIE powinno przekazać stosowną informację do Biura Organizacyjnego MEN.
2) W rejestrze zgłoszeń zidentyfikowano przypadki nadania dostępu do określonego systemu, mimo braku upoważnienia do przetwarzania danych osobowych – zgodnie z § 13 ust. 1 i 2 oraz § 21 ust. 4 Polityki bezpieczeństwa danych osobowych w MEN[13], opiekun systemu (osoba wyznaczona przez dyrektora departamentu lub dyrektora CIE, odpowiedzialna za przydzielanie i odbieranie uprawnień do dostępu do systemu informatycznego) jest zobowiązany zweryfikować, czy nadanie dostępu do systemu jest zgodne z upoważnieniem do przetwarzania danych osobowych.

Obszar nr 3 kontrolujący ocenili pozytywnie, pomimo stwierdzonych nieprawidłowości.

Obszar 4

Spełnianie wymogów wynikających z zarządzenia w sprawie ochrony danych osobowych w MEN.

W ramach obszaru 4, kontrolą objęto realizację obowiązków CIE określonych w zarządzeniu Ministra Edukacji Narodowej w sprawie ochrony danych osobowych[14], w tym w:

1) Polityce bezpieczeństwa danych osobowych w MEN (dalej: PBDO),

---

[12] Załącznik nr 1 do Polityki bezpieczeństwa informacji MEN

[13] Załącznik nr 1 do zarządzenia nr 28 Ministra Edukacji Narodowej z dnia 2 lipca 2015 r. w sprawie ochrony danych osobowych w Ministerstwie Edukacji Narodowej, zmienionego zarządzeniem nr 36 z dnia 27 września 2017 r.

[14] Zarządzenie nr 28 Ministra Edukacji Narodowej z dnia 2 lipca 2015 r. w sprawie ochrony danych osobowych w Ministerstwie Edukacji Narodowej, zmienione zarządzeniem nr 36 z 27 września 2017 r.

2) Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w MEN (dalej: Instrukcja).

Ustalenia:
W wyniku kontroli ustalono, że obowiązki CIE, w ww. obszarze, były realizowane prawidłowo. CIE wyznaczyło administratorów systemu informatycznego i administratorów technicznych, nadawało, zmieniało i odbierało uprawnienia w systemach teleinformatycznych służących do przetwarzania danych osobowych (w tym w domenie Active Directory i poczcie elektronicznej) oraz prowadziło dzienniki administratora technicznego.

Stwierdzone nieprawidłowości:
1) CIE nie informowało na bieżąco dyrektora BO o wynikach kontroli i audytów przeprowadzanych w CIE, ani o wnioskach wynikających ze sprawdzania zgodności z przepisami procesu przetwarzania danych osobowych, dotyczących bezpośrednio lub pośrednio bezpieczeństwa danych osobowych, w szczególności danych osobowych przetwarzanych w systemach informatycznych, dla których Minister Edukacji Narodowej jest administratorem, mimo obowiązku wynikającego z § 7 ust. 1 pkt 3 PBDO.
2) CIE nie udokumentowało prowadzenia ewidencji napraw i konserwacji sprzętu komputerowego, na którym MEN przechowuje dane osobowe. Obowiązek ten wynika z załącznika nr 3 PBDO[15].
3) Brakuje informacji pozwalających na okresową weryfikację, czy zachowany jest obowiązek instalowania wyłącznie autoryzowanego oprogramowania licencjonowanego[16].

CIE wyjaśniło, że konta domenowe dla pracowników MEN są zakładane z uprawnieniami użytkownika ograniczonego, co uniemożliwia instalowanie innego oprogramowania. Niektórym osobom, na podstawie zleceń przekazywanych do Sekcji Wsparcia Użytkownika, są jednak nadawane uprawnienia administratora lokalnego. CIE poinformowało, że nie prowadzi rejestru nadanych uprawnień tego rodzaju, gdyż nie ma takiego obowiązku. Brak takiego rejestru uniemożliwia okresową weryfikację tych uprawnień i sprawdzenie, czy użytkownicy je posiadający nie instalują nieautoryzowanego oprogramowania, narażając system teleinformatyczny MEN na dodatkowe niebezpieczeństwa.

Uwagi:
1) W przypadku 2 stanowisk komputerowych w CIE stwierdzono nieprawidłowe ustawienie ekranu komputerowego, które potencjalnie umożliwia zapoznanie się z treścią danych.

---

[15] Załącznik nr 3 do PBDO w części Środki techniczne, tabela „Zabezpieczenie sprzętu"
[16] Załącznik nr 3 do PBDO w części Środki techniczne, tabela „Środki ochrony systemów informatycznych i narzędzi baz danych"

2) Na stanowisku komputerowym udostępnionym w recepcji[17] ekran nie wygasza się automatycznie.
3) Stwierdzono jeden przypadek nadania uprawnień do dysku sieciowego, mimo, że z wniosku nie wynikało, że był przekazany z upoważnienia dyrektora właściwego merytorycznie departamentu (mail nie był też przesłany do jego wiadomości). Zgodnie z § 18 Instrukcji, uprawnienia do dysków sieciowych przydziela CIE na wniosek (lub z upoważnienia) dyrektora departamentu właściwego merytorycznie dla danego dysku sieciowego.

Obszar nr 4 kontrolujący ocenili pozytywnie, pomimo stwierdzonych nieprawidłowości.

W ramach celu 2, tj. Ocena stopnia przygotowania CIE do wdrożenia RODO, zostały skontrolowane dwa niżej przedstawione obszary.

Obszar 5
Spełnianie wymogów wynikających z art. 28 RODO[18].

Art. 28 RODO formułuje wymagania dotyczące podmiotu przetwarzającego, tj. podmiotu, który przetwarza dane osobowe w imieniu administratora. W kontrolowanym przypadku Minister Edukacji Narodowej jest administratorem, a CIE pełni funkcję podmiotu przetwarzającego.

W ramach obszaru 5, kontrolą objęto realizację zadań i obowiązków podmiotu przetwarzającego w odniesieniu do danych osobowych powierzonych CIE przez MEN. Powierzenie przetwarzania danych zostało uregulowane zarządzeniem nr 17 Ministra Edukacji Narodowej z dnia 28 maja 2018 r. w sprawie powierzenia Centrum Informatycznemu Edukacji przetwarzania danych osobowych, których administratorem lub podmiotem przetwarzającym jest Minister Edukacji Narodowej.

Niżej przedstawione regulacje wprowadzone przez Dyrektora Centrum Informatycznego Edukacji związane były z przygotowaniem CIE do wdrożenia RODO. Zgodnie z art. 37 ust. 1 RODO, CIE, jako podmiot publiczny obligatoryjnie wyznacza inspektora ochrony danych. 25 maja 2018 r. na inspektora został wyznaczony specjalista w Zakładzie Administracyjnym. Zostało to potwierdzone i dookreślone zarządzeniem nr 8/2018 Dyrektora Centrum Informatycznego Edukacji z dnia 10 lipca 2018 r. w sprawie wdrożenia w Centrum Informatycznym Edukacji dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych

[17] Punkt 6 w tabeli „Zasady pracy z danymi osobowymi" w części „Środki organizacyjne" PBDO
[18] RODO jest stosowane od 25 maja 2018 r.

danych osobowych. Na mocy zarządzenia nr 8/2018 Dyrektora Centrum Informatycznego Edukacji, CIE dostosowało do RODO dokumentację dotyczącą przetwarzania danych osobowych, którą stanowi obecnie Polityka Ochrony Danych Osobowych w CIE (dalej: Polityka CIE) w Warszawie. Stanowi to realizację zarówno art. 24 ust. 2 RODO, jak i art. 28 ust. 3 lit. c RODO.

Uwagi dotyczące Polityki CIE:

1) Osoba wyznaczona do pełnienia funkcji inspektora ochrony danych obecnie pełni obowiązki Kierownika Zakładu Administracyjnego, co, w opinii kontrolujących, może być powodem wystąpienia konfliktu interesów. Zgodnie z art. 38 ust. 6 RODO, inspektor ochrony danych może wykonywać inne zadania i obowiązki, pod warunkiem, że administrator lub podmiot przetwarzający zapewnia, że takie zadania i obowiązki nie prowadzą do konfliktu interesów. Zgodnie z obowiązującymi Wytycznymi dotyczącymi inspektorów ochrony danych[19] „Co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (...), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych.".
2) Rola inspektora ochrony danych w procesie przygotowywania upoważnień do przetwarzania danych osobowych, w nadawaniu i odbieraniu upoważnień, choć nie ma charakteru decyzyjnego, stoi w sprzeczności z jego obowiązkiem monitorowania przestrzegania RODO (występuje tu konflikt interesów, gdyż inspektor w zakresie wydawania upoważnień, zgodnie z zaprojektowanym procesem, musiałby kontrolować samego siebie).
3) Brakuje doprecyzowania, czy Polityka CIE odnosi się zarówno do danych osobowych przetwarzanych przez CIE jako administratora danych, jak i do danych, które przetwarza jako podmiot przetwarzający. Brak takiego dookreślenia może budzić w pracownikach CIE wątpliwości co do zakresu obowiązywania tej regulacji.
4) W katalogu obowiązków osoby upoważnionej[20] brak jest doprecyzowania, że osoba upoważniona jest zobowiązana do zachowania w poufności przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia, również po rozwiązaniu stosunku prawnego z CIE (zgodnie z brzmieniem wzoru oświadczenia o zachowaniu danych osobowych w poufności[21]).
5) Na podstawie Polityki CIE, prowadzony jest m.in. rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. Analiza treści dokumentu wykazała, że wymaga on uzupełnienia, gdyż nie uwzględnia wszystkich czynności (procesów) przetwarzania danych

[19] Wytyczne dotyczące inspektorów ochrony danych („DPO") przyjęte przez Grupę Roboczą art. 29 ds. Ochrony Danych w dniu 13 grudnia 2016 r., zmienione i przyjęte w dn. 5 kwietnia 2017 r. (nadal obowiązujące).

[20] str. 12/90

[21] załącznik nr 4, str. 66/90

osobowych, dla których CIE jest podmiotem przetwarzającym. Zostały w nim umieszczone tylko te czynności, które wiążą się z dalszym powierzeniem przetwarzania danych osobowych, a powinien on obejmować wszystkie procesy przetwarzania danych, dla których CIE jest podmiotem przetwarzającym – niezależnie od tego, czy następuje dalsze powierzenie przetwarzania, a także niezależnie od tego, czy to MEN jest administratorem danych, czy inny podmiot.

6) W Procedurze udostępniania danych występują sprzeczności zapisów dotyczących uprawnień inspektora ochrony danych. Zgodnie z RODO, Inspektor opiniuje, doradza i monitoruje, ale nie podejmuje decyzji za administratora. W punkcie 4 Procedury jest zapisane, że inspektor podejmuje decyzję, w punkcie 6 i 7 Procedury są zapisy dotyczące uzyskania pozytywnej lub negatywnej opinii inspektora (opinia w sensie prawnym nie ma mocy wiążącej).
7) W Procedurze zgłaszania incydentów, rola inspektora ochrony danych obejmuje otrzymywanie przez niego informacji o zaistniałym incydencie oraz o podjętych działaniach. Nie przewiduje się udziału inspektora w wyjaśnieniu incydentu, ani w ocenie, czy incydent kwalifikuje się do zgłoszenia do organu nadzorczego oraz czy należy o nim informować osobę, której dane dotyczą.

Uwagi dotyczące załącznika nr 2 do Polityki CIE - wzór informacji podawanej w przypadku zbierania danych od użytkowników SIO[22].

1) Załączona klauzula informacyjna, umieszczona w arkuszu kontaktowym, w zakresie informacji o administratorze danych osobowych, jest niewłaściwa, bowiem zawiera informację, że administratorem danych jest CIE. Formularz kontaktowy jest ściśle powiązany z SIO, za który odpowiada Minister Edukacji Narodowej. Przetwarzanie danych osobowych dotyczących SIO zostało powierzone CIE. W związku z tym, administratorem danych przekazywanych w formularzu SIO, jest Minister Edukacji Narodowej.
2) W klauzuli nie są również zawarte precyzyjne informacje dotyczące skutków podania lub niepodania danych w formularzu kontaktowym.

Wzór informacji podawanej w przypadku zbierania danych od wykonawców lub zleceniobiorców nie uwzględnia sytuacji, kiedy administratorem danych jest MEN lub inny podmiot, a CIE jest podmiotem przetwarzającym.

Uwaga dotycząca załącznika nr 5 do Polityki CIE:
W treści wzoru upoważnienia do przetwarzania danych osobowych nie ma określonego zakresu danych, do których jest upoważniana dana osoba.

---

[22] str. 52/90

Uwaga dotyczące załącznika nr 8 do Polityki CIE:
We wzorach umów powierzenia zawieranych przez CIE, trudno rozgraniczyć role, w jakich CIE w tych umowach występuje, tzn. czy występuje w roli administratora danych, czy w roli podmiotu przetwarzającego dane powierzone przez MEN. W odniesieniu do „podpowierzania" przetwarzania danych osobowych powierzonych CIE przez MEN, umowy powierzenia zostały zaktualizowane i dostosowane do wymogów RODO. Nieprawidłowości zostały wskazane w ramach omówienia obszaru 1.

Obszar nr 5 kontrolujący ocenili pozytywnie. W obszarze tym nie stwierdzono nieprawidłowości.

Obszar 6
Wdrożenie zasady Privacy by design (ochrony danych w fazie projektowania) oraz Privacy by default (domyślnej ochrony danych).

Zgodnie z motywem 78 RODO, ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie stosowania RODO. Aby wykazać spełnienie RODO, konieczne jest stosowanie zasady ochrony danych w fazie projektowania – czyli wprowadzanie rozwiązań mających na celu ochronę danych od samego początku pracy nad określonym projektem, czy systemem. Druga wskazana zasada oznacza, iż, domyślnie, przetwarzane są wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Kontrolą objęto stosowanie ww. zasad w ramach działań prowadzonych na rzecz Ministerstwa.

Ustalenia:
W wyniku kontroli, na podstawie przekazanych informacji ustalono, że CIE stosuje obie zasady. CIE przed przystąpieniem do projektu przeprowadza ocenę i analizę zagrożeń, identyfikację ryzyk oraz wpisuje ochronę prywatności w każde rozwiązanie i w każdy system, od momentu zebrania danych do momentu ich trwałego i ostatecznego usunięcia. Środki, jakie CIE w szczególności stosuje to:

1) minimalizacja danych,
2) ukrywanie danych i powiązań między danymi – tam gdzie jest to możliwe,
3) separowanie danych,
4) agregowanie danych.

Obszar nr 6 kontrolujący ocenili pozytywnie. W obszarze tym nie stwierdzono nieprawidłowości.

CIE prawidłowo realizowało zadania w zakresie powierzonych zbiorów danych osobowych, których administratorem jest Minister Edukacji Narodowej, mimo

uwag i nieprawidłowości, które wskazują na potrzebę poprawy i uporządkowania niektórych obszarów. Rozwiązania systemowe zastosowane w CIE zostały dostosowane do RODO, ale wymagają przeglądu i wprowadzenia odpowiednich korekt.

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

1) Udzielić brakujących upoważnień do przetwarzania danych osobowych oraz poprawić błędy i nieścisłości w ewidencji osób upoważnionych (obszar 1).
2) W przypadkach zawartych przez CIE umów odnoszących się do powierzenia danych osobowych, należy zgodnie z art. 28 ust. 3 RODO zawrzeć również umowy powierzenia przetwarzania danych osobowych (obszar 1).
3) W nowo projektowanych systemach informatycznych wdrożyć odpowiednie środki techniczne i organizacyjne, służące również kontroli nad tym, komu są przekazywane dane osobowe z systemów (obszar 2).
4) W przypadku podejrzenia zaistnienia incydentu bezpieczeństwa informacji, przekazywać informacje o tym fakcie do administratora bezpieczeństwa fizycznego lub sekretariatu Biura Organizacyjnego zgodnie z § 6 ust. 2 Procedury zarządzania incydentami bezpieczeństwa informacji[23] (obszar 3).
5) Weryfikować posiadane przez pracowników MEN oraz inne osoby współpracujące z MEN (osoby zatrudnione na umowie cywilnoprawnej, praktykanci, stażyści, wolontariusze) upoważnienia do przetwarzania danych osobowych przed nadaniem dostępu do danego systemu informatycznego (obszar 3).
6) Informować na bieżąco administratora o wszelkich planowanych lub realizowanych w CIE kontrolach i audytach dotyczących powierzonych danych osobowych, zgodnie z zarządzeniem w sprawie powierzenia przetwarzania danych osobowych, których administratorem lub podmiotem przetwarzającym jest Minister Edukacji Narodowej[24] (obszar 4).
7) Dokonywać okresowych sprawdzeń oprogramowania wykorzystywanego przez użytkowników, w celu zapewnienia bezpieczeństwa informatycznego

[23] Załącznik nr 1 do Polityki bezpieczeństwa informacji MEN.

[24] Zarządzenie nr 17 Ministra Edukacji Narodowej z dnia 28 maja 2018 r. w sprawie powierzenia Centrum Informatycznemu Edukacji przetwarzania danych osobowych, których administratorem lub podmiotem przetwarzającym jest Minister Edukacji Narodowej.

Ministerstwa zgodnie z § 3 ust. 3 Zasad bezpieczeństwa w systemach informatycznych[25] (obszar 4).

8) W Procedurze udostępniania danych w Polityce Ochrony Danych Osobowych w CIE zadaniom inspektora ochrony danych nadać charakter opiniujący, a nie decyzyjny (obszar 5).
9) We wzorze informacji podawanej w przypadku zbierania danych od użytkowników SIO (klauzula informacyjna) wskazać faktycznego administratora danych osobowych (obszar 5).

Na podstawie art. 49 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, przedstawiając powyższe wystąpienie pokontrolne, proszę o złożenie w terminie 30 dni od daty otrzymania niniejszego wystąpienia informacji o sposobie wykonania zaleceń.

Od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Wystąpienie sporządzono w dwóch jednobrzmiących egzemplarzach.

Z upoważnienia Ministra Edukacji Narodowej

Sławomir Adamiec
Dyrektor Generalny

[25] Zasady bezpieczeństwa w systemach teleinformatycznych stanowią załącznik nr 3 do PBI.