KANCELARIA PREZESA RADY MINISTRÓW
MINISTER – CZŁONEK RADY MINISTRÓW

*Michał Dworczyk*

DNK.WK.583.2.2020.KD Warszawa, sierpnia 2020 r.

**Pan**
**dr Wojciech Federczyk**

**Dyrektor**
**Krajowej Szkoły Administracji Publicznej**
**im. Prezydenta Rzeczypospolitej Polskiej**
**Lecha Kaczyńskiego**

# WYSTĄPIENIE POKONTROLNE

Po rozpatrzeniu zastrzeżeń[1] złożonych do *Projektu wystąpienia pokontrolnego*[2] przestawiam Panu Dyrektorowi *Wystąpienie pokontrolne* (dalej: *Wystąpienie*) z kontroli przeprowadzonej[3] przez Kancelarię Prezesa Rady Ministrów w Krajowej Szkole Administracji Publicznej[4] (dalej: *KSAP*, *Szkoła*, *Jednostka*) w zakresie *wykorzystania systemów teleinformatycznych do realizacji zadań publicznych* w okresie od 1 stycznia 2018 r. do 31 grudnia 2019 r.

Podstawa prawna:
Art. 25 ust. 1 pkt 3 lit. b) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[5] (dalej: *ustawa o informatyzacji*) oraz art. 46 i 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[6] (dalej: *ustawa o kontroli*).

Szkoła wykorzystuje 3 systemy teleinformatyczne do realizacji zadań publicznych:

- *Internetowy System Zgłoszeń Postępowanie Kwalifikacyjne w Służbie Cywilnej* (dalej: *ISPSC*) – wykorzystywany do przeprowadzenia postępowania w służbie cywilnej,
- *Internetowy System Zgłoszeń Rekrutacja KSAP* (dalej: *ISZR*) – służący do realizacji naboru do *Szkoły;*
- *Internetowy System Rejestracji na Szkolenia* (dalej: *ISRNS*) – użytkowany do organizacji szkoleń.

## OCENA KONTROLOWANEGO OBSZARU

Istotnego wzmocnienia wymagają działania *KSAP* w zakresie budowy kompleksowego i spójnego systemu zarządzania bezpieczeństwem informacji (dalej: *SZBI*) gwarantującego poufność, dostępność i integralność przetwarzanych danych. W obszarze tym stwierdzono szereg nieprawidłowości, których usunięcie wymaga podjęcia niezwłocznych czynności.

[1] Pismo z 10 lipca 2020 r., znak: PAO.090.1.2020.
[2] Z 25 czerwca 2020 r., znak: COA.WK.583.13.2019.KD.
[3] Kontrolę przeprowadzili pracownicy Kancelarii Prezesa Rady Ministrów: Magda Jarosławska, główny specjalista, kierownik zespołu kontrolującego oraz Krzysztof Dodot, główny specjalista. Czynności kontrolne przeprowadzono w okresie od 10 lutego do 12 marca 2020 r., w siedzibie Krajowej Szkoły Administracji Publicznej, ul. Wawelska 56, 00-922 Warszawa, natomiast w okresie 13-16 marca 2020 r. kontynuowano je poza siedzibą *Szkoły*. Kontrolerzy spełniają wymagania określone w art. 28 ust. 1 *ustawy o informatyzacji*, w tym posiadają jeden z certyfikatów wymienionych w załączniku do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz. U. Nr 177, poz. 1195).
[4] *KSAP* jest państwową jednostką organizacyjną, posiadającą osobowość prawną, działającą na podst. ustawy z dnia 14 czerwca 1991 r. o Krajowej Szkole Administracji Publicznej im. Prezydenta Rzeczypospolitej Polskiej Lecha Kaczyńskiego (Dz. U. z 2019 r., poz. 1388 t. j.) oraz statutu (dalej: Statut), nadanego rozporządzeniem Prezesa Rady Ministrów z dnia 7 października 1999 r. w sprawie nadania statutu Krajowej Szkole Administracji Publicznej im. Prezydenta Rzeczypospolitej Polskiej Lecha Kaczyńskiego (Dz. U. z 2017 r., poz. 1507 t. j.). Ustawowym zadaniem *KSAP* jest kształcenie i przygotowywanie do służby publicznej urzędników służby cywilnej oraz kadr wyższych urzędników administracji Rzeczypospolitej Polskiej. *Szkoła* realizuje również zadania w zakresie szkoleń dla pracowników administracji publicznej.
[5] Dz. U. z 2020 r., poz. 346, t. j. W okresie objętym kontrolą obowiązywał tekst jednolity opublikowany w Dz. U. z 2017 r., poz. 570 oraz Dz. U. z 2019 r., poz. 700.
[6] Dz. U. z 2020 r., poz. 224, t. j. W okresie objętym kontrolą obowiązywał tekst jednolity opublikowany w Dz. U. z 2011 r. Nr 185, poz. 1092.

Konieczna jest zmiana podejścia przy wdrażaniu *SZBI*. Proces ten należy rozpocząć od przeprowadzenia przeglądu i opracowania całościowej analizy ryzyka w stosunku do wszystkich aktywów *Jednostki*. Pozwoli to na identyfikację obszarów, które wymagają działań korygujących oraz proaktywne zarządzanie systemem. Niezbędne jest także zapewnienie narzędzi nadzorczych dostarczających bieżących informacji nt. poszczególnych etapów budowy *SZBI*.

**System zarządzania bezpieczeństwem informacji**

- **[SZBI]** Działania *Szkoły* w celu zapewniania odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji wykorzystywanych do realizacji zadań publicznych były nieskuteczne. Pomimo upływu blisko 8 lat od wejścia w życie *Rozporządzenia KRI*[7]*, KSAP* nie posiadała kompleksowego *SZBI*. W szczególności dotyczy to braku opracowania całościowej dokumentacji, która jest warunkiem skutecznego zarządzania bezpieczeństwem informacji. *Jednostka* nie dysponowała najważniejszym i podstawowym dokumentem *SZBI* jakim jest *Polityka Bezpieczeństwa Informacji*, ponieważ obowiązująca regulacja dotyczyła wyłącznie ochrony danych osobowych.
- **[Nadzór]** Kierownictwo *Szkoły* nie posiadało skutecznych narzędzi zarządczych i mechanizmów zapewniających nadzór i bieżącą informację w zakresie wdrażania *SZBI*. W konsekwencji postęp prac w obszarze jego budowy nie był w wystarczającym stopniu weryfikowany.
- **[Analiza ryzyka i plan postępowania z ryzykiem]** Nie przeprowadzono kompleksowej analizy ryzyka utraty integralności, dostępności i poufności informacji, która stanowi fundamentalną część procesu zarządzania ryzykiem. W rezultacie nie można stwierdzić, czy podejmowane działania były odpowiedzią na najistotniejsze, zidentyfikowane zagrożenia. Ponadto w konsekwencji braku tej analizy *KSAP* nie posiadała również planu postępowania z ryzykiem.
- **[Baza CMDB]** Pozytywnie należy ocenić wdrożenie przez *KSAP* narzędzia pozwalającego na skuteczne zarządzanie sprzętem i oprogramowaniem. Zapewniało ono szeroką informację dot. posiadanych aktywów informatycznych. Warto je jednak uzupełnić o informacje nt. przenośnych napędów CD-ROM, telefonów służbowych, pamięci przenośnej czy urządzenia dot. Internetu mobilnego. Słabością zarządzania tym obszarem był brak regulacji wewnętrznych.
- **[Audyt]** Prowadzono audyt w zakresie bezpieczeństwa informacji, jednakże narzędzie to nie było efektywnie wykorzystywane. Zrealizowany audyt nie obejmował wszystkich obszarów funkcjonowania *SZBI*, zatem nie identyfikował całościowo jego słabości i nie wspierał *Jednostki* w skutecznym doskonaleniu systemu. Nie prowadzono także efektywnych działań w zakresie monitorowania sposobu usunięcia niezgodności oraz wdrożenia rekomendacji.
- **[Uprawnienia]** W *KSAP* nie wprowadzono zasad dokumentowania nadawania, zmiany i odbierania uprawnień dla użytkowników i administratorów systemów teleinformatycznych, co jest niezbędne do przejrzystości tego procesu.
- **[Incydenty]** Istotną słabością zarządzania incydentami był brak całościowych regulacji oraz nieprowadzenie rejestru zdarzeń i incydentów bezpieczeństwa informacji. Uniemożliwiało to analizę występujących zagrożeń, a tym samym podejmowanie adekwatnych decyzji w zakresie stosowanych zabezpieczeń.
- **[Zapewnienie wiedzy pracownikom]** Czynności związane z zapewnieniem pracownikom wiedzy nt. nowych zagrożeń, adekwatnych zabezpieczeń, skutków

[7] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247 t. j.). Wejście w życie 31 maja 2012 r.

ewentualnych incydentów naruszenia bezpieczeństwa informacji, innych niż dane osobowe, nie były wystarczające. Jedyną formą podnoszącą świadomość pracowników nt. zagrożeń był kierowany do nich mailing dot. niebezpiecznych wiadomości e-mail oraz szkolenie szyfrowania plików przesyłanych pocztą elektroniczną. Obowiązująca w *KSAP* regulacja nie zawierała zasad zarządzania wiedzą w obszarze bezpieczeństwa informacji, w tym postanowień wprowadzających cykliczność różnych form szkoleń. Pozytywnie należy ocenić, organizację szkoleń dot. ochrony danych osobowych w związku z rozpoczęciem stosowania RODO[8] oraz wdrożeniem nowej regulacji wewnętrznej w Szkole.

- **[Umowy]** Za niewystarczające należy uznać działania *KSAP* w zakresie zabezpieczenia interesów *Szkoły* w umowach dot. serwisu i rozwoju systemów informatycznych i teleinformatycznych. Postanowienia umów nie gwarantowały odpowiedniego poziomu bezpieczeństwa informacji. Ponadto, obszar ten nie był wspierany przez regulacje wewnętrzne, gdyż nie ustanowiono katalogu niezbędnych postanowień dot. ochrony danych, jakie powinny być zamieszczone w umowach oraz reguł zaznajomienia wykonawców z zasadami bezpieczeństwa informacji, obowiązującymi w *Jednostce*.
- **[Praca na odległość]** Nie wdrożono całościowych regulacji dot. zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych, jak również pracy na odległość (telepracy). Mimo że od kwietnia 2019 r. wprowadzono nowe rozwiązania dot. użytkowania pakietu *Microsoft Office 365*. Brak regulacji stanowił ryzyko dla bezpieczeństwa informacji.
- **[Kopie zapasowe]** Pozytywnie należy ocenić, że *KSAP* wykonywała kopie zapasowe. Koniecznym jest jednak podjęcie działań związanych z ich testowaniem. Nie testowano kopii sporządzanych skryptem automatycznie wykonującym kopię bazy oraz skryptami umieszczonymi na maszynie danego rozwiązania. Obszar ten wymaga także wdrożenia pełnych regulacji odpowiadających faktycznie podejmowanym działaniom.
- **[Zabezpieczenia organizacyjno-techniczne dostępu do informacji]** Brak ustalonych formalnych zasad przyczyniających się do minimalizowania wystąpienia ryzyka kradzieży lub utraty informacji, środków przetwarzania informacji oraz urządzeń mobilnych, osłabiał system bezpieczeństwa informacji.
- **[Zabezpieczenia organizacyjno-techniczne systemów]** Niezasadnym było przetwarzanie danych zawartych w *ISRNS* przez okres znacznie dłuższy niż wynikający z obowiązującej *Instrukcji kancelaryjnej*[9]. Ponadto wykorzystywanie na laptopie (1) oprogramowania, dla którego producent nie zapewnia wsparcia w postaci poprawek bezpieczeństwa, stanowiło niebezpieczeństwo dla informacji przetwarzanych w *KSAP*. Zagrożenie to po okresie objętym kontrolą dotyczyło kolejnych 13 komputerów, co było skutkiem braku wymiany oprogramowania w okresie objętym kontrolą.
- **[Plan ciągłości działania]** *KSAP* nie opracowała planu ciągłości działania na wypadek wystąpienia zdarzeń o niskim prawdopodobieństwie, ale o katastrofalnych skutkach, takich jak np. pożar, katastrofa budowlana, terroryzm, powódź.
- **[Rozliczalność działań]** *Szkoła* nie posiadała dzienników systemowych, w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych. Stanowiło to naruszenie § 21 *Rozporządzenia KRI.* Ponadto nie opracowano procedur, w szczególności określających zasady ich prowadzenia i wykorzystania.

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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.
[9] Zarządzenie nr 24/2017 Dyrektora KSAP z dnia 19 grudnia 2017 r. *w sprawie instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt i instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego KSAP.*

**Zapewnienie dostępności informacji zawartych na stronie internetowej**

*KSAP* dostosowała stronę internetową do większości wymagań określonych w § 19 *Rozporządzenia KRI*, jednakże konieczne są dalsze działania dla zapewnienia pełnej dostępności treści zawartych na stronie.

**Wymiana informacji w postaci elektronicznej**

*Szkoła* powinna wzmocnić działania w zakresie wdrożenia regulacji i rozwiązań, umożliwiających świadczenie usług elektronicznych, wpływających na sprawne i szybkie załatwianie spraw z klientami.

## OCENY I USTALENIA SZCZEGÓŁOWE

### I. System zarządzania bezpieczeństwem informacji

**1. [stan *SZBI*]** Negatywnie należy ocenić, że *KSAP* nie posiadała kompleksowego i spójnego *SZBI*. *Jednostka* dysponowała *Polityką Bezpieczeństwa Informacji*, która dotyczyła wyłącznie ochrony danych osobowych i nie odnosiła się do wszystkich obszarów *SZBI*. Z tych powodów *Szkoła* nie spełniła wymogów § 20 ust. 1 *Rozporządzenia KRI*. Pełne wdrożenie kompleksowej dokumentacji zaplanowano dopiero do końca 2020 r. Brak części istotnych procedur nie zapewniał minimalnego poziomu bezpieczeństwa przetwarzanych informacji oraz nie gwarantował skutecznego zarządzania tym obszarem.

Od 25 maja 2018 r. w *KSAP* obowiązywała *Polityka Bezpieczeństwa Informacji* dot. ochrony danych osobowych (dalej: *PBI ODO* lub *Polityka*)[10]. We wcześniejszym okresie Szkoła posiadała *Politykę Bezpieczeństwa Przetwarzania Danych Osobowych* oraz *Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*[11]. Regulacje te nie stanowiły całościowych uregulowań *SZBI*. Skupiały się na ochronie danych osobowych przetwarzanych w systemach informatycznych. Nie obejmowały zatem wszystkich informacji przetwarzanych w *KSAP*, w systemach teleinformatycznych. Wyjaśniono[12], że do końca 2020 r. planowane jest dokonanie kompleksowej analizy *Polityki.* Pozwoli ona na eliminację zauważonych mankamentów oraz uregulowanie obszarów, których nie obejmowała regulacja. Wdrożona *PBI ODO* nie obejmowała zagadnień dot.:

- zarządzania ryzykiem bezpieczeństwa informacji innych niż dane osobowe, ze wskazaniem sposobu jego szacowania,
- zarządzania infrastrukturą informatyczną,
- konieczności dokumentowania czynności w zakresie nadawania, zmiany, zawieszenia, zablokowania oraz odebrania/cofnięcia uprawnień,
- realizacji szkoleń dla pracowników *Szkoły*, określających także ich cykliczność,
- kompleksowych zasad pracy na odległość i mobilnego przetwarzania danych,
- katalogu klauzul, które powinny zostać zawarte w umowach cywilnoprawnych w celu zabezpieczenia interesów *KSAP,*
- zarządzania incydentami,
- realizacji audytów wewnętrznych,
- projektowania, wdrażania, wprowadzania zmian oraz monitorowania systemów teleinformatycznych,
- całościowych zasad postępowania z kopiami zapasowymi oraz sposobu prowadzenia i wykorzystania dzienników systemowych.

Zdaniem *Szkoły*[13], mimo że *PBI ODO* literalnie odnosi się do danych osobowych, to jednak przyjęte w tym dokumencie rozwiązania miały zastosowanie do wszelkich danych przetwarzanych w *KSAP*, także w systemach teleinformatycznych. W ocenie *Jednostki* przykładowo załącznik nr 12[14] do *PBI ODO* wskazuje, że celem procedury jest zabezpieczenie właściwej pracy na stanowiskach komputerowych pod względem bezpieczeństwa przetwarzania danych osobowych i innych informacji.

[10] Wprowadzona zarządzeniem nr 8/2018 Dyrektora *KSAP* z dnia 25 maja 2018 r. w sprawie *PBI* w *KSAP*.
[11] Wprowadzone zarządzeniem nr 18 Dyrektora *KSAP* z dnia 30 października 2015 r.
[12] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 12 lutego 2020 r., znak: PAO.091.1.2020.1(1).
[13] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 12 lutego 2020 r., znak: PAO.091.1.2020.1(1).
[14] *Procedura użytkowania stanowiska komputerowego i nośników danych*.

Nie można zgodzić się z tym stanowiskiem, ponieważ w *PBI ODO*[15] wskazano, że jej zakres dotyczy zapewnienia bezpieczeństwa danych osobowych oraz wsparcia przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych. Regulacja ta wyznacza zatem granice jej stosowania i ogólnych postanowień zawartych w załącznikach nie można stosować rozszerzająco. Oznacza to, że *PBI ODO* nie zapewniała bezpieczeństwa informacji innych niż dane osobowe, którymi dysponowała *Szkoła*. Ustanowienie *SZBI,* który zapewnia poufność, dostępność i integralność informacji wymaga opracowania kompleksowych regulacji wewnętrznych gwarantujących sprawność jego działania. Dlatego prace nad ich opracowaniem powinny zostać podjęte niezwłocznie po wejściu w życie *Rozporządzenia KRI*.

**2.** *PBI ODO* nie była w pełni dostosowana do specyfiki *Szkoły*, ponieważ nie odnosiła się do funkcjonujących w niej rozwiązań, w szczególności związanych z: tworzeniem i testowaniem kopii zapasowych, pracą na odległość i mobilnym przetwarzaniem danych, prowadzeniem inwentaryzacji sprzętu i oprogramowania (bazy CMDB). Słabością działania *Jednostki* było to, że *PBI ODO* nałożyła szereg wymogów, które później w praktyce nie były przestrzegane. Tym samym wprowadzona regulacja nie wspierała *KSAP* w procesie zapewnienia bezpieczeństwa informacji.

*PBI ODO* nakładała na *Szkołę* szereg wymogów, które w praktyce nie były przestrzegane. Przykładowo nie prowadzono:

- *Ewidencji baz danych osobowych przetwarzanych w KSAP ze wskazaniem programów stosowanych do ich przetwarzania*[16],
- *Ewidencji baz danych osobowych z opisem merytorycznym pól bazy*[17],
- *Raportów zawierających oceny i wnioski wynikające z zagrożeń bezpieczeństwa przetwarzania danych osobowych i analizy stanu ochrony obszarów ich przetwarzania w KSAP*[18],
- *Szczegółowych raportów o przyczynach, przebiegu i wnioskach ze zdarzenia*[19],
- *Ewidencji budynków i pomieszczeń KSAP z wydzieleniem stref przetwarzania danych osobowych, ciągów komunikacji i przesyłania danych*[20],
- *Ewidencji odnotowującej udostępnienie danych osobowych na zewnątrz KSAP*[21],
- *Ewidencji powiązania i przepływów baz danych osobowych/systemów używanych w KSAP*[22],
- *Rejestru naruszeń danych osobowych, w tym faktów towarzyszących naruszeniom, ich skutków i podjętych działań w związku ze świadczeniem publicznie dostępnych usług telekomunikacyjnych przez KSAP*[23].

Nie opracowano także zasad: *monitorowania obszarów i systemów informatycznych*[24], *gospodarki kluczami do pomieszczeń i szaf*[25], *wyposażenia pomieszczeń, w których przetwarzane są dane osobowe we wzmocnione drzwi, odpowiednio zabezpieczone okna, meble, zamknięcia i niezbędne zabezpieczenia alarmowe*[26], *konfiguracji oraz regularnego uaktualniania oprogramowania antywirusowego zarówno na serwerach jak i komputerach użytkowników*[27]. Nie zostały wykonane analizy ryzyka do wszystkich eksploatowanych systemów informatycznych[28]. Nie przedstawiono także dokumentów potwierdzających monitorowanie 4 z 5 *Zaleceń Bezpieczeństwa*[29].

[15] Pkt. II *PBI ODO – Deklaracja intencji, cele i zakres polityki bezpieczeństwa*.
[16] § 13 ust. 1 *PBI ODO.*
[17] § 16 ust. 5 *PBI ODO.*
[18] § 12 ust. 2 *PBI ODO.*
[19] Pkt 11 załącznika nr 4 do *PBI ODO.*, tj. *Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w KSAP*.
[20] § 11 ust. 2 wdrożonej *PBI ODO.*
[21] Załącznik nr 5 do *PBI ODO*, tabela nr 2.
[22] Załącznik nr 5 do *PBI ODO*, tabela nr 6.
[23] Załącznik nr 5 do *PBI ODO*, tabela nr 9.
[24] § 23 ust. 15 *PBI ODO.*
[25] § 20 ust. 2 tabeli 1, poz. b *PBI ODO.*
[26] § 20 ust. 2 tabeli 1, poz. c *PBI ODO.*
[27] Pkt. 3.1. lit. h) załącznika nr 12 do *PBI ODO, tj. Procedury użytkowania stanowiska komputerowego i nośników danych.*
[28] § 21 *PBI ODO.*
[29] Tj. nr 1, 2, 3 i 5, natomiast zalecenie nr 4 w trakcie kontroli było dopiero przygotowywane.

Celem regulacji wewnętrznych jest usystematyzowanie obowiązujących w *Jednostce* procesów i rozwiązań oraz wsparcie ich uczestników w realizacji określonych czynności. Natomiast ustanowienie regulacji, której postanowienia nie są przestrzegane nie wspiera *Jednostki* w skutecznym zarządzaniu obszarem.

**3. [nadzór Kierownictwa i analiza *SZBI*]** Kierownictwo *Szkoły* nie dysponowało skutecznymi narzędziami zapewniającymi nadzór nad działaniami dot. bezpieczeństwa informacji. W szczególności nie wdrożono rozwiązań zarządczych pozwalających na efektywne utworzenie spójnego *SZBI*, tj. nie wyznaczono osoby albo komórki organizacyjnej odpowiedzialnej za budowę *SZBI* oraz nie przeprowadzono analizy aktualnego stanu bezpieczeństwa informacji, zwłaszcza z uwzględnieniem informacji przekazanych w piśmie Szefa KPRM[30]. Tym samym nie zapewniono identyfikacji zarówno obszarów wymagających usystematyzowania i wdrożenia nowych zasad/procedur, jak i tych, w przypadku których istnieje potrzeba podjęcia działań naprawczych. Nie opracowano również planu/strategii rozwoju *SZBI.* Zatem Kierownictwo *KSAP* nie posiadało instrumentów do weryfikacji postępu prac dot. wdrażania spójnego *SZBI*.

> Część zadań związanych z zapewnieniem bezpieczeństwa informacji przypisano do Biura Administracyjnego, a w zakresie ochrony danych osobowych do kompetencji Inspektora Ochrony Danych (dalej: *IOD*). Do Biura Administracyjnego[31] należały jedynie zadania związane z zapewnieniem bezpieczeństwa informatycznego oraz współpracą z komórkami organizacyjnymi w zakresie przestrzegania zasad bezpieczeństwa pożarowego. Nie były to wszystkie obszary *SZBI* pozwalające na skuteczne zarządzanie bezpieczeństwem.
>
> Wyjaśniono[32], że w *KSAP* nie wyznaczono jednej osoby do nadzoru nad funkcjonowaniem *SZBI*. W latach 2018-2019 skoncentrowano na bezpieczeństwie systemów informatycznych oraz ochronie danych osobowych. Poinformowano także, że nie były to wszystkie czynności, ponieważ do zadań każdego kierownika[33] należy m.in. nadzór nad przestrzeganiem przepisów o ochronie informacji niejawnych i przepisów o ochronie danych osobowych.

Przestrzeganie przepisów o ochronie informacji niejawnych i ochronie danych osobowych nie zapewnia pełnych i efektywnych działań w zakresie budowy *SZBI.* Natomiast rozproszenie nadzoru nad tym procesem nie wspierało Dyrekcji *Szkoły* we wdrażaniu systemu, ponieważ nie były przekazywane Kierownictwu zbiorcze informacje, które są kluczowe w procesie zarządzania.

> Nie przeprowadzono analizy aktualnego stanu bezpieczeństwa informacji, w szczególności po otrzymaniu pisma Szefa KPRM, w którym przestawiono najważniejsze i najczęściej powtarzające się nieprawidłowości w tym procesie. Analiza zrealizowana z uwzględnieniem tych informacji pozwoliłaby na diagnozę i wyznaczenie kierunków budowy *SZBI*. Wyjaśniono[34], że *Szkoła* na bieżąco analizuje stan bezpieczeństwa informacji, a w piśmie tym nie określono terminu na przeprowadzenie analizy. Pismo zostało potraktowane jako wytyczne, które, zdaniem *KSAP*, w praktyce są stopniowo wdrażane.
>
> W zakresie opracowania planu/strategii rozwoju *SZBI* wskazano[35], że wyznaczono kierunki rozwoju związane z: modernizacją serwerowni, sieci strukturalnej, zakupem nowych urządzeń i systemów, wprowadzeniem rozwiązań zapewniających pracę grupową na dokumencie, a także wdrożeniem rozwiązania ERP[36]. Kierunki te ustaliła Dyrekcja *Szkoły* na podstawie potrzeb zgłaszanych i konsultowanych z kierownikami komórek organizacyjnych. Działania te nie zostały jednak udokumentowane.

Skuteczne wdrażanie *SZBI* powinno rozpocząć się od diagnozy istniejących rozwiązań. *Szkoła* nie przeprowadziła takiego przeglądu nawet po otrzymaniu pisma *KPRM*. Nie opracowano także planu/strategii wdrażania *SZBI*, zawierającego w szczególności

---

[30] Pismo z 11 czerwca 2019 r., znak: COA.WK.588.1.2019.MF, *Informacja o najważniejszych i najczęściej powtarzających się nieprawidłowościach stwierdzonych w wyniku kontroli przeprowadzonych przez KPRM w zakresie wykorzystania systemów teleinformatycznych do realizacji zadań publicznych.*
[31] Zarządzenie nr 12/2018 Dyrektora KSAP z dnia 16 października 2018 r. oraz zarządzenie nr DN/12/2016 Dyrektora KSAP z 30 listopada 2016 r.
[32] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.21(1).
[33] § 11 ust. 1 lit. l) regulaminu organizacyjnego *KSAP*.
[34] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 12 marca 2020 r., znak: PAO.0910.1.2020.24(1).
[35] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 12 marca 2020 r., znak: PAO.0910.1.2020.24(1).
[36] Enterprise Resource Planning.

planowane działania, termin ich wdrożenia oraz osoby odpowiedzialne za ich realizację. Identyfikacja słabości i opracowanie pisemnego planu/strategii przyczyniłyby się do skutecznego zarządzania obszarem bezpieczeństwa informacji. Brak dokumentowania w tym zakresie utrudnia analizę i ocenę wdrażanych rozwiązań. Pozbawia również Kierownictwo *Szkoły* narzędzia zarządczego do podejmowania adekwatnych decyzji.

**4.** **[analiza ryzyka]** *KSAP* nie prowadziła systematycznej, okresowej analizy ryzyka, wskutek tego nie spełniono wymogów określonych w § 20 ust. 2 pkt 3 *Rozporządzenia KRI*. Wykonano jedynie analizy w wybranych komórkach organizacyjnych w zakresie ochrony danych osobowych, dlatego nie obejmowały one wszystkich aktywów[37] *Jednostki.* Ponadto nie przedstawiały akceptowalnych progów ryzyk. Odnosiły się do kategorii finansowej oraz wizerunku *KSAP*, podczas gdy celem analizy ryzyka bezpieczeństwa informacji powinna, być w pierwszej kolejności, ocena ryzyk związanych z utratą integralności, dostępności lub poufności. W związku z tym, że nie przeprowadzono analizy ryzyka bezpieczeństwa informacji, *Szkoła* nie posiadała także planu postępowania z ryzykiem.

> Analizy ryzyka przeprowadzono jedynie w zakresie ochrony danych osobowych w odniesieniu do wybranych 4 komórek organizacyjnych, tj. Biura Dyrektora, Biura Administracyjnego (jedynie w części Zespołu Informatyków), Kolegium *KSAP*, Ośrodka Rozwoju i Kształcenia Ustawicznego. Nie objęły one zatem ogółu informacji przetwarzanych w pozostałych komórkach oraz wszystkich aktywów *Szkoły*. Jak wskazano[38], analizy ryzyka są prowadzone w miarę możliwości organizacyjnych i finansowych *Szkoły*. Są one procesem dynamicznym i nie ograniczają się do badanego okresu. Całościowy plan postępowania z ryzykiem był w trakcie opracowania.

Przede wszystkim *Jednostka* powinna zadbać o rzetelną analizę ryzyka pozwalającą na opracowanie całościowego planu postępowania z ryzykiem. Analiza taka jest jednym z najistotniejszych elementów budowania *SZBI*. Pozwala na proaktywne zarządzanie bezpieczeństwem informacji, w tym przeciwdziałanie zagrożeniom oraz ograniczanie skutków w przypadku zmaterializowania się ryzyk. Z tego powodu proces ten powinien być cykliczny, a dodatkowe działania podejmowane w sytuacjach zmieniającego się otoczenia.

**5.** Opracowane analizy ryzyka, pomimo że zawierały działania naprawcze, nie były przedstawiane do zatwierdzenia Kierownictwu *Szkoły*. Czynności korygujące podejmowane były na ustne polecenie lub za zgodą Dyrekcji *KSAP*. Z tego powodu *Szkoła* nie posiadała udokumentowanych informacji o procesie postępowania z ryzykiem, do czego zobowiązują postanowienia Normy PN-ISO/IEC 27001[39].

> Analizy ryzyka zostały sporządzone przez 4 kierowników komórek organizacyjnych. Na etapie określania działań naprawczych byli oni wspierani przez *IOD*. Zgodnie z wyjaśnieniami[40], wszelkie działania zaradcze wdrażane były na polecenie i za zgodą Dyrekcji *KSAP*, która pozostaje w stałym kontakcie zarówno z kierownikami komórek organizacyjnych, jak też z *IOD*. Bardzo często kontakt polega na spotkaniach bezpośrednich i ustnych poleceniach, *stąd może powstać mylne wyobrażenie braku podjętych działań*.

Skuteczność zastosowanych zabezpieczeń wpływa na poziom zapewnienia bezpieczeństwa informacji. Z tego względu wybór odpowiednich opcji postępowania z ryzykiem ma istotne znaczenie dla organizacji. Powinien on zostać udokumentowany i podlegać akceptacji najwyższego Kierownictwa.

**6.** **[audyt]** W *KSAP* prowadzono audyty bezpieczeństwa informacji, jednak narzędzie to nie było efektywnie wykorzystywane. Nie obejmowały one wszystkich obszarów *SZBI* i nie identyfikowały wszystkich nieprawidłowości systemu, nie wspierały także *Jednostki*

---

[37] Zgodnie z normą PN-ISO/IEC 27000 aktywem jest wszystko, co ma wartość dla organizacji. Istnieje wiele typów aktywów, w tym: aktywa informacyjne, oprogramowanie, takie jak program komputerowy, fizyczne, takie jak komputer, usługi, personel i jego kwalifikacje, umiejętności i doświadczenie oraz wartości niematerialne, takie jak reputacja i wizerunek.
[38] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[39] Punkt 6.1.3 *Postępowanie z ryzykiem w bezpieczeństwie informacji*.
[40] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.

w ich eliminacji. Wymóg corocznej realizacji tego audytu, w myśl obowiązku określonego w § 20 ust. 2 pkt 14 *Rozporządzenia KRI,* nie został spełniony. Spowodowane było to przesunięciem czynności audytowych o blisko rok, tj. z 2018 r. na 2019 r.

> W okresie objętym kontrolą przeprowadzono 2 audyty w zakresie bezpieczeństwa informacji. Pierwsze czynności audytowe zrealizowano od 9 października 2017 r. do 26 stycznia 2018 r. Następny audyt odbył się dopiero w terminie od 27 listopada do 27 grudnia 2019 r., pomimo że został przewidziany w *Planie audytu na 2018 r.* Czynności audytowe przesunięto z powodu nieobecności audytora[41].
>
> Oba audyty nie objęły wszystkich obszarów *SZBI*, pomimo że *Plan audytu na 2018 r.* oraz *Program zadania audytowego*[42] nie przewidywały takiego ograniczenia. Audyty nie zawierały w szczególności informacji nt. przeglądów *SZBI*, posiadania aktualnych informacji w zakresie sprzętu i oprogramowania, zarządzania uprawnieniami, organizacji szkoleń, pracy na odległość, umów w zakresie serwisu i rozwoju systemów informatycznych /teleinformatycznych, zarządzania incydentami, tworzenia i testowania kopii zapasowych, projektowania, wdrażania, wprowadzania zmian oraz monitorowania systemów teleinformatycznych, zabezpieczeń organizacyjno-technicznych dostępu do informacji oraz systemów[43], rozliczalności działań użytkowników, strony internetowej.
>
> Wyjaśniono[44], że *z uwagi na fakt, że jednorazowe poprawne wdrożenie SZBI – tj. jednokrotne przygotowanie odpowiednich procedur, zabezpieczenie systemów, wprowadzenie odpowiednich mechanizmów monitoringu bezpieczeństwa itp. z praktycznego punktu widzenia jest trudne do zrealizowania, zdecydowano się na przeprowadzenie audytu w niepełnym zakresie*.

Audyt wewnętrzny jest narzędziem, którego celem jest wspieranie kierownika danej jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze[45]. Realizacja audytu bezpieczeństwa w niepełnym zakresie utrudnia jednak osiągnięcie tego celu, w tym nie pozwala na skuteczną identyfikację potencjalnych słabości lub zagrożeń bezpieczeństwa informacji.

**7.** Zrealizowane w 2018 r. audyty bezpieczeństwa informacji oraz *Ochrony Danych Osobowych w procesie z ODO do RODO* nie przyniosły zakładanej wartości dodanej dla *Jednostki*, ponieważ nie wdrożono ich wszystkich rekomendacji. Pomimo że analiza sposobu usunięcia niezgodności oraz wdrożenia rekomendacji wykazała brak realizacji zaleceń audytu, dalsze czynności monitorowania nie były kontynuowane.

> Audyt wewnętrzny *Ochrony Danych Osobowych w procesie z ODO do RODO*[46] przeprowadził *IOD*[47]. Stwierdzono 28 niezgodności oraz wydano 11 rekomendacji[48]. Natomiast w wyniku realizacji audytu bezpieczeństwa informacji z 2018 r. sformułowano 3 rekomendacje. W przypadku obu audytów sporządzono analizy dotyczące realizacji rekomendacji, które potwierdzają, że nie wszystkie z nich zostały wdrożone. Pomimo tego, dalsze czynności monitorowana ich wykonania nie były prowadzone. Z *Tabeli działań korygujących system bezpieczeństwa przetwarzania danych osobowych w świetle nowych przepisów prawnych*[49] wynikało, że jedynie 15 (z 28, tj. 54%) niezgodności zostało wyeliminowanych; 4 były w trakcie realizacji, a w stosunku do 9 nie wskazano żadnych informacji. Spośród rekomendacji wdrożono tylko 2 (z 11, tj. 18%), w odniesieniu do pozostałych 9 nie wskazano informacji. Natomiast notatka informacyjna[50] z czynności sprawdzających wykonanie rekomendacji audytu bezpieczeństwa informacji potwierdza, że żadna z nich nie została zrealizowana.

Sama realizacja audytu, bez analizy i wdrożenia działań naprawczych nie przyniesie dla działalności *Jednostki* wartości dodanej. Pozwala ona jedynie na uzyskanie oceny stanu

---

[41] Notatka umieszczona na *Programie zadania audytowego* z 10 grudnia 2018 r., znak; 2/AW/2018.
[42] Nr zdania audytowego: 2/AW-01/2018.
[43] W audycie nr 2/AW/2018 skupiono się jedynie na pomieszczeniu serwerowni.
[44] E-mail audytora z 10 marca 2020 r., przekazany przy piśmie Szefa Pionu Administracyjno-Organizacyjnego z 12 marca 2020 r., znak: PAO.0910.1.2020.24(1).
[45] Definicja audytu wewnętrznego zawarta w art. 272 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2019 r., poz. 869, t. j. ze zm.).
[46] Czynności audytowe zrealizowano w terminie 16 marca – 20 kwietnia 2018 r. w siedzibie *Szkoły* oraz 30 kwietnia 2018 r. w Kolegium *KSAP*.
[47] Zgodnie z art. 38 ust. 1 lit. b RODO jednym z zadań inspektora ochrony danych jest monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
[48] *Raport z audytu Ochrony Danych Osobowych w procesie z ODO do RODO w KSAP* z 4 maja 2018 r. (ze zmianą 5 maja 2018 r.).
[49] Brak daty sporządzenia.
[50] Z 23 marca 2018 r., znak zadania audytowego 1/AW/2017.

*SZBI*. To działania naprawcze mają na celu dokonanie zmian dla usprawnienia tego systemu. *Szkoła* powinna zatem monitorować ten proces oraz zapewnić szybką eliminację stwierdzonych słabości.

**8. [baza CMDB]** Pozytywnie należy ocenić wdrożenie przez *KSAP* narzędzia pozwalającego na zarządzanie sprzętem i oprogramowaniem, tj. oprogramowania *KSAP ITM – Zarządzanie infrastrukturą informatyczną, zasobami informatycznymi KSAP* (dalej: *baza CMDB*). Zapewniało ono szeroką informację nt. posiadanego sprzętu i oprogramowania, w tym jego rodzaju, konfiguracji oraz użytkownika. Rozwiązanie to należy jedynie uzupełnić o dane dot. przenośnych napędów CD-ROM, telefonów służbowych, pamięci przenośnej czy urządzeń dot. Internetu mobilnego. Słabością zarządzania tym obszarem był jednak brak regulacji wewnętrznych normujących funkcjonujące rozwiązanie.

> *Baza CMDB* prowadzona przy użyciu autorskiego oprogramowania, zawierała informacje m.in. dot. nazwy i rodzaju sprzętu, lokalizacji, oprogramowania, parametrów, aktualnej konfiguracji, stanu urządzeń[51] oraz ich użytkownika. W programie odnotowywane były także najważniejsze zmiany dotyczące sprzętu i oprogramowania. Ewidencjonowano w nim: komputery, drukarki, laptopy, monitory, tablety, AP WiFi, routery, UPS-y, switche, projektory oraz urządzenia monitorujące, zarówno podłączone, jak i niepracujące w sieci wewnętrznej.
>
> Program nie zawierał jednak informacji nt. przenośnych napędów CD-ROM, pamięci przenośnej, telefonów służbowych, czy sprzętu dot. Internetu mobilnego. Ostatnie dwie grupy urządzeń były objęte odrębną ewidencją. Nie zawierała ona informacji o przypisaniu części urządzeń Internetu mobilnego[52] do konkretnych użytkowników / lokalizacji.
>
> Wyjaśniono[53], że nie przypisano tych urządzeń do użytkownika, ponieważ są to urządzenia ruchome, używane w czasie szkoleń oraz przeznaczone są do wypożyczania pracownikom. Wypożyczenie takie jest ewidencjonowane. Wskazano także, że *KSAP* nie rejestrowała przenośnych napędów CD-ROM oraz pamięci przenośnej, co wynikało z braku potrzeby prowadzenia ewidencji w tym zakresie. Rozważane jest jednak rozbudowanie aplikacji *ITM* o brakujące elementy. *Baza CMDB* jest tworzona i prowadzona *z potrzeb praktycznych, stąd nie ma regulacji wewnętrznych dla powyższego rozwiązania.*

Posiadanie pełnej informacji o stanie aktywów informatycznych umożliwia przeprowadzenie rzetelnej analizy ryzyka i przygotowanie planu postępowania z ryzykiem. Z tych względów informacje te, zawierające dane nt. konkretnego użytkownika, powinny być gromadzone w jednym miejscu. Dotyczy to również sprzętu ruchomego, w tym przeznaczonego do wypożyczania, który powinien być przypisany do konkretnej osoby, np. pracownika nim zarządzającego. Dzięki temu *Szkoła* posiadałaby kompletną informację o wszystkich urządzeniach, w tym z podziałem na konkretnych pracowników.

**9.** Dobrą praktyką było opracowanie przez Zespół Informatyków[54] zbioru roboczych wytycznych, tj. *Bazy wiedzy IT – bazy aktywów informacyjnych (procedur i praktyk)*.

> Baza to zbiór niezatwierdzonych instrukcji wykorzystywanych przez informatyków w bieżącej pracy m.in. w zakresie konfiguracji stanowisk komputerowych, przygotowywania ich dla nowych pracowników, w tym założenia odpowiednich kont, postępowania przy zakończeniu pracy przez pracownika, przygotowania komputerów do sali szkoleniowej, przełączenia Internetu na łącze zapasowe, zasad wejścia do serwerowni.

Przygotowane wytyczne umożliwiły informatykom jednolity sposób postępowania w zakresie konfiguracji sprzętu.

**10. [uprawnienia]** Proces nadawania, zmieniania i odbierania uprawnień nie był kompletny, ponieważ rejestr zawierający te informacje prowadzony był dopiero od 29 listopada 2019 r. Nie wprowadzono także zasad nadawania, zmiany i odbierania uprawnień administratorom, a także zasad zobowiązujących do dokumentowania tych

[51] Tj. *sprawny*, *niesprawny*, *wymaga uwagi*.
[52] Urządzenia o numerach: 693231124, 725415124 oraz 726415124.
[53] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 3 marca 2020 r., znak: PAO.0910.1.2020.19(1) oraz z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[54] W ramach Biura Administracyjnego *KSAP*.

czynności w stosunku do wszystkich użytkowników systemów teleinformatycznych. Pełnienie skutecznego nadzoru nad tym obszarem utrudniało niewyznaczenie osoby odpowiedzialnej za jego realizację.

> W *Szkole* obowiązywała *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*[55]. Nie była to jednak regulacja pozwalająca na efektywne zarządzanie obszarem nadawania, zmiany i odbierania uprawnień. Nie określała zasad w odniesieniu do administratorów, jak również obowiązku dokumentowania podejmowanych czynności w zakresie uprawnień pracowników.
>
> Poinformowano[56], że nadawanie, zmiana oraz odebranie uprawnień, w tym dot. pracy na odległość i mobilnego przetwarzania danych, jest dokumentowane w poczcie elektronicznej Administratora Systemów Informatycznych (dalej: *ASI*). Pocztą, Biuro Spraw Personalnych informuje *ASI* o zatrudnieniu bądź zakończeniu stosunku pracy, natomiast kierownik komórki przesyła informację o zakresie nadania lub konieczności odebrania uprawnień. Informacje te nie były także grupowane, np. przechowywane w jednym folderze, przez co nie został zapewniony do nich łatwy i szybki dostęp.
>
> W ocenie *Jednostki* informacje przechowywane na poczcie były łatwo dostępne. Ponadto wskazano, że nadanie uprawnień administratorom 3 systemów teleinformatycznych nastąpiło na podstawie *mailowej lub telefonicznej zgody Kierownictwa Szkoły oraz decyzji nr 72/2019*. Decyzja ta dotycząca powołania zespołu sprawdzającego do przeprowadzenia postępowania kwalifikacyjnego, nie była zatem dokumentem stanowiącym podstawę do nadania uprawnień administratora. Inne dokumenty nie zostały w toku kontroli przekazane.
>
> Od 29 listopada 2019 r. prowadzony jest rejestr nadanych, zmienionych i odebranych uprawnień zapewniający przejrzystość procesu.

Przechowywanie informacji o nadanych uprawnieniach wśród wszystkich informacji mailowych *ASI* nie zapewnia przejrzystości procesu i łatwego dostępu do nich, w szczególności w przypadku urlopu *ASI,* bądź zmiany systemu pocztowego, co miało miejsce w okresie kontrolowanym. Niewdrożenie całościowych zasad zarządzania uprawnieniami wpływa na obniżenie poziomu ochrony i bezpieczeństwa informacji.

**11.** Zarządzanie hasłami oraz identyfikacją i uwierzytelnianiem użytkowników w przypadku 2 z 3 systemów teleinformatycznych przebiegało prawidłowo. Trzeci system, tj. *ISRNS*[57]*,* nie spełniał istotnych wymogów w tym zakresie.

> W przypadku 2[58] z 3 eksploatowanych w *KSAP* systemów teleinformatycznych, funkcjonujących jedynie w sieci wewnętrznej *Szkoły*, zabezpieczenia w zakresie uwierzytelnienia użytkowników zapewniono na etapie dostępu do systemu Windows. System ten wymuszał konieczność ustanowienia hasła dobrej jakości, nie wyświetlał znaków przy logowaniu, zapewniał okresową zmianę hasła, zapamiętywał kilka ostatnich z nich, w celu uniemożliwienia wykorzystania jednego z ostatnich, gwarantował blokowanie systemu po kilku nieudanych próbach oraz jego odłączenie po określonym czasie nieaktywności. Wszystkich tych wymogów nie spełniał *ISRNS* funkcjonujący w oparciu o przeglądarkę internetową.

**12.** **[incydenty]** Ustanowione w *KSAP* zasady zarządzania zdarzeniami dotyczyły jedynie naruszeń ochrony danych osobowych, tym samym nie został spełniony obowiązek wskazany w § 20 ust. 2 pkt 13 *Rozporządzenia KRI*. Wdrożona *PBI ODO* nie regulowała takich zagadnień jak np.: monitorowanie, wykrywanie, analizowanie, zgłaszanie zdarzeń i incydentów związanych z bezpieczeństwem informacji w ustalony sposób, postępowanie z dowodami procesowymi, nadawanie priorytetów, zasady kontroli oraz sposób reakcji na incydenty przez wyznaczone osoby w celu szybkiego podjęcia działań naprawczych

[55] Załącznik nr 1 do *PBI ODO*.
[56] Pisma Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 3 marca 2020 r., znak: PAO.0910.1.2020.8(1), 30 marca 2020 r., znak: PAO.0910.1.2020.26(1) oraz 30 kwietnia 2020 r., znak: PAO.0910.1.2020.21(1).
[57] Internetowego Systemu Rejestracji na Szkolenia.
[58] *ISPSC* oraz *ISZR*.

i korygujących, a także określenie procesu dyscyplinarnego pracowników, którzy naruszyli zasady bezpieczeństwa informacji.

> W *PBI ODO* ustalone zostały jedynie procedury dotyczące naruszenia ochrony danych osobowych, tj. *Rodzaje naruszenia ochrony danych osobowych i sposoby postępowania w przypadkach ich zaistnienia*[59] oraz *Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych*[60]*.* W ocenie *KSAP*[61]*,* zasady te pozwoliłyby na podjęcie działań w zakresie potencjalnych zdarzeń. W *Szkole* zapewniony jest przepływ informacji od pracownika, przez kierownika, do Dyrekcji, co wynika z niewielkiego rozmiaru *Jednostki* oraz stopienia rozbudowania struktury organizacyjnej.

Wielkość *Jednostki* nie powinna mieć wpływu na konieczność ustanowienia i wdrożenia prawidłowej procedury zarządzania incydentami, uwzględniającej podział zadań i odpowiedzialność, ponieważ to przejrzyste zasady postępowania w sytuacjach wystąpienia zagrożeń pozwalają na szybkie podjęcie działań korygujących. *PBI ODO* nie regulowała sposobu postępowania z zagrożeniami innymi niż dane osobowe, dlatego podjęcie właściwych działań wobec takich zagrożeń nie byłoby możliwe. Wielkość *Jednostki*, sposób jej organizacji i zadań ma natomiast istotny wpływ na sposób uregulowania tego obszaru.

**13.** Istotną słabością zarządzania incydentami był brak obowiązku prowadzenia rejestru zdarzeń i incydentów bezpieczeństwa informacji. W konsekwencji nie było możliwe przeprowadzenie analizy występujących zagrożeń i ustalenie słabości *SZBI*, a następnie wprowadzenie niezbędnych zmian. Rejestr ten nie był prowadzony, pomimo że w *Raporcie dotyczącym wykrytych wirusów* odnotowano zdarzenia tego typu.

> Zgodnie z *PBI ODO Szkoła* była zobowiązana do prowadzenia *Rejestru zdarzeń*, jednak tylko w dziedzinie przetwarzania danych osobowych. Zatem *Jednostka* nie dysponowała całościowym rejestrem zdarzeń i incydentów bezpieczeństwa informacji, w szczególności zawierającym informacje dotyczące daty i godziny zgłoszenia incydentu, daty i godziny zamknięcia jego obsługi, opisu podjętych działań naprawczych, imienia i nazwiska pracownika zgłaszającego, imienia i nazwiska osoby obsługującej incydent oraz wskazania kategorii priorytetu incydentu.
>
> Wyjaśniono[62], że *w badanym okresie nie odnotowano incydentów naruszenia bezpieczeństwa informacji*. Jednakże *Raport dotyczący wykrytych wirusów* zawiera takie zdarzenia. Podano[63], że *spora część wirusów dotyczy laptopów używanych w salach wykładowych i salach komputerowych*, które nie są podłączone do sieci wewnętrznej *KSAP*.

Szybki postęp technologiczny w środowisku informatycznym powoduje pojawianie się szeregu coraz to nowszych ryzyk dla bezpieczeństwa informacji. Wystąpienie zagrożeń potwierdza *Raport dotyczący wykrytych wirusów*, dlatego rejestr zdarzeń i incydentów powinien być wdrożony.

**14.** W *KSAP* nie prowadzono miesięcznych analiz *Raportów dotyczących wykrytych wirusów*, co było niezgodne z postanowieniami *PBI ODO* i nie wspierało *Jednostki* w doborze adekwatnych zabezpieczeń do występujących zagrożeń.

> Zgodnie z postanowieniami pkt 3.1. lit. o) załącznika nr 12 do *PBI ODO*[64] *Raporty dotyczące wykrytych wirusów* powinny być analizowane z częstotliwością nie mniejszą niż raz na miesiąc. A wszystkie wykryte anomalie zgłaszane osobie na stanowisku ds. bezpieczeństwa teleinformatycznego lub osobie wyznaczonej. W *KSAP* jednak nie prowadzono miesięcznych analiz. Wyjaśniono[65], że analiza prowadzona była w odniesieniu do każdego incydentu na miejscu u danego pracownika *KSAP*, a jej wynik przekazywany był temu pracownikowi.

---

[59] Załącznik nr 2 do *PBI ODO*.
[60] Załącznik nr 3 do *PBI ODO*.
[61] Wyjaśnienia Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.12(1).
[62] Wyjaśnienia Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.12(1).
[63] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 10 marca 2020 r., znak: PAO.0910.1.2020.14(1).
[64] *Procedura użytkowania stanowiska komputerowego i nośników danych.*
[65] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 10 marca 2020 r., znak: PAO.0910.1.2020.14(1).

Rozwiązanie problemu związanego z zaistniałym incydentem i przedstawienie go wyłącznie pracownikowi, pozbawia *Jednostkę* informacji nt. podjętych działań. W konsekwencji nie wspiera *Szkoły* w doskonaleniu systemowych działań naprawczych, gdyż w przypadku wystąpienia tożsamej sytuacji nie posiada ona informacji nt. działań, które okazały się nieskuteczne.

**15. [szkolenia]** *Szkoła* w niewystarczający sposób zapewniała wiedzę pracownikom nt. nowych zagrożeń, adekwatnych zabezpieczeń, skutków ewentualnych incydentów naruszenia bezpieczeństwa informacji, innych niż dane osobowe. Jedyną formą podnoszącą świadomość pracowników nt. zagrożeń był kierowany do nich mailing dotyczący niebezpiecznych wiadomości e-mail oraz szkolenie szyfrowania plików przesyłanych pocztą elektroniczną. Wdrożona *PBI ODO* nie zawierała zasad zapewnienia wiedzy pracownikom w zakresie bezpieczeństwa informacji innych niż dane osobowe, w tym postanowień wprowadzających cykliczność szkoleń. Właściwym działaniem było natomiast zorganizowanie szkoleń dotyczących nowych wymogów wprowadzonych przepisami RODO[66] oraz *PBI ODO*. W szkoleniach tych uczestniczyła większość pracowników *Szkoły* (tj. 68 z 75[67], 91%), a pozostałym osobom zapewniono indywidualne szkolenia z *IOD*.

> Zorganizowano specjalistyczne szkolenia w zw. z rozpoczęciem stosowania przepisów RODO oraz wdrożeniem *PBI ODO*, a dla kierowników komórek organizacyjnych dodatkowo szkolenie z szacowania ryzyka. Ponadto wraz z wdrażaniem nowych rozwiązań, tj. poczty elektronicznej oraz *SharePoint* przeprowadzono szkolenie z szyfrowania plików oraz użytkowania platformy.
>
> Wyjaśniono[68], że szkolenia z ochrony danych osobowych faktycznie obejmowały szerszy zakres niż dane osobowe i dotyczyły szeroko rozumianego bezpieczeństwa informacji. Program szkolenia *Z ODO do RODO ochrona danych osobowych w praktyce* nie obejmował jednak innych zagadnień niż ochrona danych osobowych i nie można uznać, że dotyczył szeroko rozumianego bezpieczeństwa informacji.
>
> *KSAP* przesyłała do pracowników e-maile o niebezpiecznych wiadomościach, tym samym ostrzegała o zagrożeniach. Jednakże działań w zakresie konkretnej sytuacji nie można uznać za zapewnienie wiedzy pracownikom nt. szeregu występujących zagrożeń, adekwatnych zabezpieczeń oraz skutków ewentualnych incydentów.
>
> Wdrożona *PBI ODO* zawężała zakres szkoleń do ochrony danych osobowych oraz systemu informatycznego. Nie zawierała postanowień w zakresie zasad przeprowadzania szkoleń, w szczególności ich cykliczności, możliwości zgłaszania potrzeb szkoleniowych przez pracowników, ich analizy, ustalania priorytetów i celów szkoleniowych, sporządzania okresowego planu szkoleń oraz oceny skuteczności procesu szkolenia. Zdaniem *Jednostki*[69], procedura w tym zakresie nie była niezbędna, bowiem podnoszenie świadomości użytkowników zaangażowanych w proces przetwarzania informacji odbywa się przez faktyczne działania, tj. szkolenia, mailing.

Podnoszenie świadomości pracowników zmniejsza ryzyko popełnienia przez nich błędów i jest istotnym elementem *SZBI*. Dlatego tak ważne jest opracowanie zasad dotyczących zapewniania im wiedzy, w tym gwarantujących cykliczność i dostępność różnych form szkoleń dla wszystkich pracowników. Przedmiot szkoleń powinien dotyczyć w szczególności zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji.

**16.** Zrealizowano obowiązek zapoznania się przez pracowników z *PBI ODO,* jednakże 17 z 20 osób nie posiadało aktualnych (5) lub zgodnych z *Polityką* upoważnień do przetwarzania danych osobowych (12).

---

[66] Rozporządzenie 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.
[67] Zatrudnionych na dzień 31 grudnia 2019 r.
[68] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.26(1).
[69] Wyjaśnienia Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.26(1).

*PBI ODO* została przekazana do wszystkich pracowników pocztą elektroniczną i dodatkowo od 16 października 2018 r. zamieszczona na stronie intranetowej *KSAP*.

Kontroli w zakresie wydawania upoważnień do przetwarzania danych osobowych poddano 25[70] z 75 (33%) pracowników zatrudnionych na 31 grudnia 2019 r. oraz 1 osoby wykonującej czynności na podstawie umowy cywilnoprawnej. Spośród tej grupy posiadanie upoważnień było wymagane dla 20 osób. Aktualnych upoważnień nie posiadało 5 osób (z 20, tj. 25%). Kolejnych 12 osób (z 20, tj. 60%) posiadało upoważnienie, które nie było w pełni zgodne z wzorem[71] określonym w załączniku nr 6 do *PBI ODO,* w tym w przypadku 3 osób przekazano kontrolującym upoważnienie wydane pod koniec 2019 r. lub na początku 2020 r., mimo że byli to długoletni pracownicy *Szkoły*.

Wyjaśniono[72], że wszystkie upoważnienia znajdują się w aktach osobowych oraz w rejestrze prowadzonym przez *IOD*. Jednakże w toku czynności kontrolnych[73] nie zostały one przedstawione.

**17. [umowy]** Postanowienia w umowach serwisu i rozwoju systemów informatycznych/teleinformatycznych nie gwarantowały odpowiedniego poziomu bezpieczeństwa informacji i należytego zabezpieczenia interesów *KSAP*, w tym możliwości skutecznego dochodzenia odpowiedzialności usługodawcy w przypadku wystąpienia sytuacji naruszenia bezpieczeństwa informacji. Tym samym nie został spełniony obowiązek wskazany w § 20 ust. 2 pkt 10 *Rozporządzenia KRI*.

Od 1 stycznia 2018 r. do 31 grudnia 2019 r. obowiązywały 4[74] umowy dot. serwisu i rozwoju systemów informatycznych/teleinformatycznych[75]. W żadnej z nich nie sformułowano obowiązku przestrzegania zasad bezpieczeństwa informacji obowiązujących w *KSAP*, nie zawarto klauzul w zakresie zapewnienia bezstronności przez wykonawców oraz klauzul o odszkodowaniu ze strony wykonawcy w przypadku niezastosowania się do procedur, czy świadomego działania, wpływającego na osłabienie systemu bezpieczeństwa.

Ponadto w 1[76] umowie nie określono postanowień dot. poufności i możliwości nałożenia kary umownej. Wyjaśniono[77], że umowy z wykonawcami takimi jak Asseco Business Solutions S.A. (wcześniej Macrologic S.A.) oraz home.pl sp.j. zawierane są na podstawie wzorów umów przedstawionych przez wykonawców i nie ma możliwości negocjowania tych wzorów.

Pomimo stosowanego przez wykonawcę wzoru umowy, *KSAP* powinna skutecznie działać w celu zawarcia w umowie postanowień dot. bezpieczeństwa informacji zabezpieczających jej interesy.

**18.** Proces zawierania umów serwisu i rozwoju systemów informatycznych /teleinformatycznych nie był wspierany przez regulacje wewnętrzne, ponieważ nie opracowano katalogu niezbędnych postanowień dotyczących ochrony informacji, które powinny być zamieszczone w tych umowach oraz reguł zaznajomienia wykonawców z zasadami bezpieczeństwa informacji obowiązującymi w *Szkole*.

W *KSAP* nie obowiązywały regulacje wewnętrzne dot. zawierania umów cywilnoprawnych, określające zasady współpracy z wykonawcami zewnętrznymi w zakresie serwisu i rozwoju systemów informatycznych. Nie opracowano także katalogu klauzul, które powinny zostać zawarte w umowie w celu zabezpieczenia interesów *Szkoły*, w szczególności w zakresie zapewnienia poufności, bezstronności i przestrzegania zasad bezpieczeństwa informacji, w tym zaznajomienia z nimi wykonawców.

Wyjaśniono[78], że każdorazowo wprowadzane są w umowach postanowienia zabezpieczające interesy *KSAP*. Potwierdzono[79], że nie wdrożono procedur zawierania umów

[70] Doboru próby dokonano na podstawie *Zestawienia zatrudnionych osób wg stanu na dzień 31 grudnia 2019 r.* metodą wyboru losowego, ze stałym odstępem.
[71] Tj. brak oświadczenia o znajomości przepisów i zobowiązania się do ochrony danych osobowych.
[72] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[73] Tj. w okresie od 10 lutego do 16 marca 2020 r.
[74] Dot. umowy: nr 77/2008/KSAP z 12 sierpnia 2008 r. z home.pl sp.j., nr 301/KSAP/2017 z 27 września 2017 r. z Macrologic S.A., nr 476/KSAP/2019 z 28 sierpnia 2019 r. z Asseco Business Solutions S.A. oraz nr 245/KSAP/2019 z 15 kwietnia 2019 r. z Arstech [redacted] (ze zm.).
[75] Pozostałe 3 umowy przedstawione do kontroli zawarto na dostarczenie usługi Internetu – 2 ( nr 539/KSAP/2017 z 11 grudnia 2017 r. oraz z nr 590/KSAP/2018 z 5 grudnia 2018 r. z NASK S.A.) oraz powierzenia przetwarzania danych osobowych – 1 (nr 286/KSAP/2018 z 1 czerwca 2018 r. z Asseco Business Solutions S.A.).
[76] Dot. umowy: nr 77/2008/KSAP z 12 sierpnia 2008 r. z home.pl sp.j.
[77] Pismo Szefa Pionu Organizacyjno-Administracyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.27(1).
[78] Pismo Szefa Pionu Organizacyjno-Administracyjnego *KSAP* z 2 marca 2020 r., znak: PAO.0910.1.2020.7(1).
[79] Pisma Szefa Pionu Organizacyjno-Administracyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.27(1) oraz PAO.0910.1.2020.28.

cywilnoprawnych i nie określono zasad współpracy z wykonawcami zewnętrznymi. Odpowiedni stopnień zabezpieczenia miały zapewnić działania polegające na bieżącej współpracy pracownika merytorycznie odpowiadającego za treść umowy, radcy prawnego oraz *IOD*.

Należy zauważyć, że w 2016 r. KSAP otrzymała od Szefa KPRM *Rekomendacje dotyczące zawierania umów cywilnoprawnych w jednostkach administracji rządowej*[80], w których zwrócono uwagę na kwestię regulacji wewnętrznych.

Sformułowanie przez *Szkołę* zasad ochrony przetwarzanych informacji i należytego zabezpieczenia interesów *Jednostki* umożliwi stosowanie przez świadczących usługi tych samych standardów i zachowanie wymaganego poziomu bezpieczeństwa. Ułatwi to również dochodzenie praw przez *KSAP* w przypadku ewentualnych sporów.

**19.** W procedurach wewnętrznych nie określono także zasad udzielania dostępu osobom trzecim do zasobów i pomieszczeń *KSAP*, w tym miejsc szczególnie wrażliwych.

*PBI ODO* nie precyzowała zasad udzielania dostępu osobom trzecim do zasobów *Szkoły*. Nie wskazano w niej kategorii/rodzajów miejsc szczególnie wrażliwych[81], z określeniem zasad przebywania w nich osób trzecich i obowiązku uczestnictwa w wykonywanych czynnościach wyznaczonych pracowników *KSAP*. Regulacja[82] ta zawierała ogólne zasady przebywania w *Szkol*e osób trzecich, jednak dotyczyły one wyłącznie kwestii dostępu i prac w obszarze związanym z przetwarzaniem danych osobowych.

Wyjaśniono[83], że udzielanie dostępu osobom trzecim do zasobów *Szkoły* odbywa się na zasadach nie mniej rygorystycznych niż przewidziane w *PBI ODO*. Osoby trzecie *nigdy nie przebywają w miejscach szczególnie wrażliwych bez obecności uprawnionego pracownika KSAP*.

Zasady dostępu do zasobów *KSAP* przez osoby trzecie powinny zostać określone, aby dostęp ten odbywał się wg jasnych i znanych pracownikom Szkoły reguł, a ingerencja osób trzecich była ograniczona do niezbędnego minimum. Stanowiłyby one także wsparcie w zapewnieniu bezpieczeństwa informacji.

**20.** **[praca na odległość]** *KSAP* nie wdrożyła kompleksowych regulacji dotyczących zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych, jak również pracy na odległość (telepracy). Wprowadzone ogólne postanowienia, zawarte w załączniku[84] do *PBI ODO – Procedurze użytkowania stanowiska komputerowego i nośników danych,* nie gwarantowały bezpieczeństwa informacji przetwarzanych na odległość, ponieważ nie odnosiły się do zasad funkcjonujących w *Szkole*.

W *KSAP* istniała możliwość pracy na odległość (co uregulowano w umowach o pracę – 5 pracowników) oraz zdalnego przetwarzania danych (wszyscy pracownicy *KSAP*). Zdalny dostęp do zasobów *Szkoły* możliwy był w przypadku 8 z 21 systemów/aplikacji, tj.: *Internetowego Systemu Rejestracji na Szkolenia*, *Argo*[85], *Akademii Zarządzania*, *eKSAP – platformy e-learning*, *eusługi – platformy e-learning* (*Elektroniczna Platforma Szkoleniowa*), *Legis*[86]*, BIP*, *Microsoft Office 365*[87], w tym poczty elektronicznej *Microsoft Outlook* i usługi *SharePoint*[88].

Dostęp taki do wszystkich systemów *Szkoły*[89] posiadał *ASI* przez połączenie tunelowe *VPN* oraz osoba administrująca częścią systemów, tj. *Lokalnym Systemem Rejestracji, Wydatki, Magazyn i Amortyzacja* (zestawione połączenie RDP między komputerem tej osoby

[80] Pismo Szefa KPRM z 29 sierpnia 2016 r., znak: COA.WN.580.13.2016.MW.
[81] Np. ogólnego dostępu, ograniczonego dostępu, zastrzeżonego dostępu.
[82] Zgodnie z § 23 ust. 1 *PBI ODO*: pomieszczenia, w których przetwarza się dane osobowe są zamykane po zakończeniu pracy. Niedopuszczalne jest przebywanie w tych pomieszczeniach osób nieposiadających pisemnego pozwolenia Administratora na przetwarzanie danych osobowych bez obecności osób upoważnionych. Z kolei zgodnie z § 23 ust. 2 *PBI ODO* wszystkie prace montażowe, remontowe i budowlane w obszarze przetwarzania danych osobowych powinny być nadzorowane przez upoważnionego przez IOD pracownika KSAP w celu wyeliminowania zagrożenia poufności,, integralności, rozliczalności i ciągłości w przetwarzaniu danych.
[83] Pismo Szefa Pionu Organizacyjno-Administracyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.27(1).
[84] Nr 12.
[85] Program zakończony z końcem 2019 r.
[86] Program zakończony z końcem 2019 r.
[87] *Microsoft Office 365* – to zbiór aplikacji i usług dostępnych z serwerów Microsoft. W skład produktów *Microsoft Office 365* wchodzi m.in. pakiet *Microsoft Office*, *Microsoft Outlook*, usługa *SharePoint*. Usługi dostępne są z dowolnego urządzenia przez sieć Internet. Logowanie do *Microsoft Office 365* następuje przez przeglądarkę internetową pod adresem: portal.office.com.
[88] *SharePoint* – usługa ta umożliwia m.in. jednoczesną pracę nad dokumentami (w tym ich edycję) przez wiele osób.
[89] Z wyłączeniem możliwości zdalnego połączenia się z pulpitem dowolnego użytkownika *Szkoły* (w tym Kolegium *KSAP*) dzięki aplikacji *AnyDesk*.

a komputerem wewnętrznym *KSAP*). Ponadto dostęp do dysków sieciowych, systemu do fakturowania *Finka FK* i *Finka Faktura*, ewidencji czasu pracy posiadał kierownik Kolegium *KSAP* (przez szyfrowane połączenie tunelowe *VPN*).

W *PBI ODO*[90] sformułowano tylko ogólne postanowienia dot. korzystania z komputerów przenośnych i zdalnego dostępu do przetwarzania danych osobowych. Regulacja ta nie odnosiła się do możliwości i zasad obowiązujących w *KSAP*, w tym związanych z wdrożeniem pakietu *Microsoft Office 365* w kwietniu 2019 r. W procedurze nie określono także m.in.: charakteru zadań ze wskazaniem systemów, w przypadku których dopuszcza się możliwość pracy na odległość, sposobu postępowania, zasad bezpieczeństwa i obowiązków osób wykonujących pracę na odległość i zdalnie przetwarzających informacje, odpowiedzialności pracowników za nieprzestrzeganie wymogów bezpieczeństwa, zasad uzyskiwania, odbioru praw dostępu, zasad dostępu administratorów do zasobów, opisu zabezpieczeń stosowanych na urządzeniach przenośnych, np. mechanizmów szyfrujących zawartość dysków twardych i nośników danych, sposobów i częstotliwości archiwizowania danych (tworzenia kopii zapasowych), możliwości bądź zakazu korzystania z prywatnego sprzętu do pracy na odległość i mobilnego przetwarzania danych.

Wskazano[91], że do *PBI ODO* prowadzone są prace uzupełniające, które obejmą pozostałe zakresy związane z przetwarzaniem informacji w *KSAP*. Ponadto *zasady bezpieczeństwa oraz odpowiedzialności pracowników określają Kodeks pracy*[92] *z przepisami wykonawczymi oraz Polityka Bezpieczeństwa Informacji*. Poinformowano, że bieżące monitorowanie ryzyk w zakresie bezpieczeństwa sprawia, że kompleksowe rozwiązania w tym zakresie są w trakcie nieustannego tworzenia i doskonalenia w ramach możliwości organizacyjnych i finansowych *Szkoły*.

Możliwość podłączenia się z dowolnego urządzenia z dostępem do Internetu do zasobów *Szkoły*, w tym możliwość pobierania i załączania dowolnych załączników, niesie za sobą szereg ryzyk związanych z bezpieczeństwem informacji. Z tych względów niezbędne jest opracowanie przejrzystych procedur i zasad przeciwdziałających tym zagrożeniom, w szczególności określających zasady pracy oraz odpowiedzialność. Nie można zgodzić się, że zasady w tym zakresie określa *Kodeks pracy* oraz obowiązująca *PBI ODO*. Akty prawa rangi ustawowej nie regulują indywidualnych rozwiązań w zakresie bezpieczeństwa informacji, które powinny być dostosowane do potrzeb *Jednostki* i określone w *Polityce Bezpieczeństwa Informacji*. Obowiązująca w *Szkole Polityka* odnosiła się jedynie do przetwarzania danych osobowych i nie regulowała całościowo wszystkich obszarów w zakresie pracy na odległość i zdalnego dostępu do przetwarzania danych. Nie jest możliwe skuteczne dochodzenie odpowiedzialności pracowników za nieprzestrzeganie zasad bezpieczeństwa, jeśli nie zostały one określone i przedstawione im do zapoznania i stosowania.

**21.** Aktywność użytkowników korzystających z usług *Microsoft Office 365,* tj. służbowej poczty elektronicznej *Microsoft Outlook* oraz platformy *SharePoint*, a także systemów pozwalających na zdalny dostęp, nie była na bieżąco analizowana i monitorowana. Brak systematycznych analiz utrudniał zidentyfikowanie ewentualnych, niedozwolonych działań pracowników. *Nie przedstawiono* powodów braku takich analiz za pomocą oprogramowania *Microsoft Office 365* (*Dziennik inspekcji*), mimo że zgodnie z dokumentacją producenta, oprogramowanie to posiadało taką funkcjonalność.

Wyjaśniono[93], że działania dotyczące wykorzystania poczty elektronicznej oraz platformy *SharePoint* były analizowane i monitorowane jedynie w konkretnych sytuacjach, np. sprawdzenia czy mail został wysłany na zewnątrz, do kogo został wysłany z danego adresu, sprawdzenia kto usunął plik z platformy *SharePoint* itp. Wskazano również, że Platforma *Office 365* posiada możliwość zaimplementowania mechanizmu DLP, który automatycznie będzie chronić przed wyciekiem danych. W związku z tym analizowana jest możliwość uruchomienia tego mechanizmu.

[90] W pkt. 3.6 *zał. 12 do PBI ODO – Procedura użytkowania stanowiska komputerowego i nośników danych.*
[91] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 2 marca 2020 r., znak: PAO.0910.1.2020.6(1) oraz 30 marca 2020 r., znak: PAO.0910.1.2020.25(1).
[92] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2019 r., poz. 1040, t.j. ze zm.).
[93] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.25(1).

Oprogramowanie *Microsoft Office 365* (*Dziennik inspekcji*), zgodnie z dokumentacją producenta, posiada możliwość odnotowywania działań użytkowników w ramach dostępu do służbowej poczty elektronicznej. Jednakże w czasie oględzin przeprowadzonych 27 lutego 2020 r.[94] ta funkcjonalność nie była dostępna. Kontrolującym przedstawiono przykładowe zestawienie logów poczty sporządzone w oparciu o serwery Exchange Online, którego opracowanie wymagało podjęcia dodatkowych czynności przez informatyków. Wskazano[95], że *KSAP* nie podejmowała jeszcze kroków związanych z wyjaśnieniem braku wyświetlania działań dotyczących poczty w *Dzienniku inspekcji*. Jednakże działania wykonywane przez użytkowników poczty odnotowywane są na serwerach Exchange Online, co pozwala na pobranie logów tych działań wykorzystując skrypt PowerShell.

W sytuacji możliwości zdalnego dostępu do zasobów *KSAP,* działania użytkowników powinny podlegać okresowym przeglądom w celu wykrycia działań niepożądanych. Oferowane rozwiązania w *Dzienniku inspekcji* umożliwiają sprawniejszą i mniej czasochłonną analizę niż serwery Exchange Online. Z tego powodu *KSAP* powinna podjąć działania pozwalające na przywrócenie pełnej funkcjonalności *Dziennika inspekcji*.

**22.** Istotne ryzyko dla bezpieczeństwa informacji stanowiło wykorzystywanie komputerów prywatnych do celów służbowych w ramach dostępu zdalnego przez pracowników wykonujących pracę na odległość oraz administratorów systemów (łącznie 6 osób). Sytuacja ta miała charakter stały i nie wynikała z nadzwyczajnych okoliczności uzasadniających taki sposób wykonywania obowiązków pracowniczych. W konsekwencji *Szkoła* miała ograniczony wpływ na konfigurację urządzeń prywatnych w celu odpowiedniego zabezpieczenia tego sprzętu. Wpływało to również na ograniczenie możliwości weryfikacji działań pracowników.

Z komputerów prywatnych do pracy na odległość korzystało 4 pracowników (telepraca). Ponadto sprzęt prywatny w ramach zdalnego dostępu wykorzystywał *ASI* oraz osoba administrująca częścią systemów (*Lokalnym Systemem Rejestracji, Wydatki, Magazyn i Amortyzacja)*. *KSAP* nie zapewniła tym pracownikom sprzętu służbowego, ponieważ, jak wskazano[96], *wymienione osoby wyraziły zgodę na pracę na sprzęcie prywatnym.*

Ponadto w celu odpowiedniego zabezpieczenia sprzętu prywatnego pracownicy zostali poproszeni o posiadanie zabezpieczenia antywirusowego, niezapamiętywanie haseł dostępu do systemów w przeglądarce internetowej oraz zwracanie uwagi, aby nawiązywane połączenie z systemem w przeglądarce internetowej było szyfrowane. Powyższe zobowiązania nie miały jednak charakteru formalnego.

Wyjaśniono[97] również, że sama praca administratorów nie odbywa się na komputerze prywatnym, a na komputerze zdalnym będącym w *KSAP,* do którego podłączają się administratorzy i który posiada zainstalowane aplikacje niezbędne do wykonania pracy. Komputer prywatny wykorzystywany jest tylko i wyłącznie do nawiązania połączenia z komputerem zdalnym.

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji, *KSAP* powinna zapewnić sprzęt służbowy do wykonywania obowiązków pracowniczych (zwłaszcza w sytuacji, w której liczba pracowników wykonujących pracę na odległość oraz administratorów systemów nie była znaczna) albo wprowadzić szczegółowe zasady wykorzystania sprzętu prywatnego do realizacja zadań służbowych. Jest to szczególnie ważne dla osób pełniących istotne role w bezpieczeństwie informacji, jakimi są administratorzy. Wskazane jest, aby praca z wykorzystaniem urządzeń prywatnych odbywała się zgodnie z ustalonymi zasadami, a zobowiązanie się pracowników do ich przestrzegania miało charakter jednoznaczny i formalny.

**23.** W *KSAP* nie wydawano pracownikom pisemnych zgód na zdalny dostęp do zasobów *Szkoły*, co stanowiło naruszenie obowiązującej *PBI ODO*.

[94] Protokół oględzin oraz przyjęcia ustnych wyjaśnień dot. zdalnego dostępu do zasobów *KSAP*, pracy na odległość i mobilnego przetwarzania informacji.
[95] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.25(1).
[96] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.25(1).
[97] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.25(1).

> Zgodnie z *PBI ODO*[98], *korzystanie z oprogramowania pozwalającego na zdalny dostęp i zarządzanie komputerem jest ściśle zakazane bez pisemnej zgody Administratora Danych Osobowych (dalej: ADO) lub osoby wyznaczonej.* Wyjaśniono[99], że zgoda Dyrektora *Szkoły* na wykonywanie pracy zdalnej oznacza jednocześnie zgodę na wszelkie związane z tym konsekwencje, w tym dostęp do systemów i zarządzenie komputerem w sposób umożliwiający świadczenie pracy zdalnej.

Wyjaśnienia *Jednostki* odnoszą się jedynie do pracowników wykonujących telepracę, w przypadku których zgoda na zdalny dostęp do zasobów wynikała z umów o pracę podpisanych przez Dyrekcję *KSAP*. Nie dotyczą one pozostałych osób mających możliwości mobilnego dostępu do zasobów *KSAP*. Nadawanie uprawnień tej grupie pracowników odbywało się pomiędzy kierownikiem komórki organizacyjnej (wskazującym zakres uprawnień) a *ASI* (nadającym dostęp). W tych przypadkach dodatkowa, pisemna zgoda *ADO* lub osoby wyznaczonej nie była wydawana, gdyż nie uczestniczyli oni w procesie nadawania uprawnień. Tym samym postanowienia przywołanej regulacji w zakresie wydawania zgód na zdalny dostęp nie były przestrzegane.

**24. [kopie zapasowe]** *PBI ODO* częściowo regulowała kwestie tworzenia kopii zapasowych, ponieważ odnosiła się wyłącznie do sporządzania kopii w celu zapewnienia bezpieczeństwa danych osobowych. *Polityka* nie precyzowała działań związanych z tworzeniem i zarządzaniem kopiami zapasowymi, w tym nie wskazywała systemów, z których sporządza się kopie z określeniem sposobu i częstotliwości ich sporządzania dla danego systemu/rodzaju danych oraz sformułowania procedur w zakresie ich odtwarzania i testowania. Postanowienia tej regulacji nie odpowiadały faktycznie podejmowanym działaniom w zakresie częstotliwości tworzenia kopii, okresu ich przechowywania oraz odtworzenia danych. Natomiast opracowana przez *ASI* dokumentacja zawierająca wspomniane elementy[100], nie podlegała zatwierdzeniu przez Dyrekcję *KSAP*. Kopie zapasowe stanowią element ciągłości działania *Jednostki*, zatem w tak istotnym obszarze zasadnym było przekazanie tej dokumentacji do akceptacji Kierownictwa *Szkoły*.

> Regulacje *PBI ODO* w zakresie tworzenia, przechowywania i testowania kopii zapasowych nie odpowiadały faktycznie podejmowanym działaniom w *KSAP*, w szczególności częstotliwość tworzenia kopii zapasowych i okres ich przechowywania nie były zgodne z postanowieniami *PBI ODO*[101]. Ponadto nie dokonywano sprawdzenia odtworzenia danych z kopii zapasowych z udziałem *IOD*, co stanowiło naruszenie § 14 ust. 6 zał. nr 1 do *Polityki*.
>
> Odnosząc się do innego sposobu tworzenia kopii, niż wynikający z *PBI ODO* wyjaśniono[102], że *Polityka* została przygotowana przed zakupem oprogramowania zapewniającego automatyczne tworzenie kopii. W związku z jego wdrożeniem (w grudniu 2018 r.) *Szkoła* wprowadziła zmiany w tym obszarze. Natomiast sama regulacja nie została zmieniona.
>
> *ASI* opracował dokumentację tworzenia kopii zapasowych, która została przekazana e-mailem jedynie do *IOD*. Określała ona m.in. z jakich systemów, z jaką częstotliwością są tworzone kopie zapasowe oraz przez jaki okres są przechowywane. Ponadto wskazywała jaką metodą wykonywane są kopie zapasowe w odniesieniu do poszczególnych systemów. Dokumentacja ta nie została zatwierdzona przez Dyrekcję *KSAP* oraz Szefa Pionu Administracyjno-Organizacyjnego. Wyjaśniono[103], że przygotowana przez *ASI* dokumentacja *zastała wysłana mailem do Kierownictwa KSAP i IDO oraz zaakceptowana milczącą zgodą. IOD oraz Kierownictwo nie wniosło uwag do przygotowanej dokumentacji*.

Tworzenie kopii zapasowych powinno być uregulowane w aktualnych procedurach, dostosowanych do potrzeb *Jednostki* i zmieniającego się otoczenia. Ponadto w tak istotnym obszarze regulacje powinny podlegać formalnemu zatwierdzeniu przez Dyrekcję *Szkoły*, nie zaś akceptacji przez *milczącą zgodę*.

---

[98] Pkt 3.6. lit b zał. 12 do *PBI ODO – Procedura użytkowania stanowiska komputerowego i nośników danych.*
[99] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.25(1).
[100] Dokumentacja przygotowana 24 lipca 2019 r.
[101] Odpowiednio z postanowieniami § 13 ust. 3 oraz § 14 ust. 5 załącznika nr 1 do *PBI ODO*, tj. *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*.
[102] Protokół oględzin oraz przyjęcia ustnych wyjaśnień w zakresie funkcjonowania systemu tworzenia, przechowywania i testowania kopii zapasowych z 27 lutego 2020 r.
[103] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.23(1).

**25.** Pozytywnie należy ocenić, że *KSAP* wykonywała kopie zapasowe danych przetwarzanych w ramach posiadanych systemów. Jednakże *Szkoła* powinna podjąć dodatkowe działania w zakresie ich testowania, ponieważ czynności te nie były wykonywane w stosunku do kopii sporządzanych skryptem automatycznie wykonującym kopię bazy oraz skryptami umieszczonymi na maszynie danego rozwiązania.

> W *KSAP* tworzono kopie zapasowe na kilka sposobów, w zależności od możliwości technicznych urządzeń i systemów. Kopie były tworzone: automatycznie przez oprogramowanie *Veritas Backup Exec*, przy zastosowaniu skryptu automatycznie wykonującego kopię bazy, skryptu umieszczonego na maszynie danego rozwiązania, przez ręczne tworzenie kopii, a także przez zewnętrzną firmę. *Szkoła* nie sporządzała jedynie kopii zapasowych dot. informacji przetwarzanych przy wykorzystaniu usług *Microsoft Office 365*, w szczególności plików umieszczanych w module *Biblioteka Dokumentów* usługi *SharePoint*.
>
> Wyjaśniono[104], że *KSAP* nie wykonywała tych kopii we własnym zakresie, gdyż były one realizowane przez producenta usługi (firmę *Microsoft*). Producent ten gwarantował dostępność, ciągłość działania platformy *Microsoft Office 365* oraz jej odporność na awarie. *KSAP* planuje wykonywanie własnej kopii zapasowej plików zawartych w module *Biblioteka Dokumentów* usługi *SharePoint*.
>
> *Szkoła* testowała również utworzone kopie, z wyjątkiem tych sporządzanych przez skrypt automatycznie wykonujący kopię bazy oraz skrypty umieszczone na maszynie danego rozwiązania.
>
> Poinformowano[105], że kopie zapasowe sporządzane przy wykorzystaniu skryptów są wykonywane narzędziem dostarczanym przez producenta bazy danych, które były sprawdzone przy produkcyjnym odtwarzaniu danych we wcześniejszym okresie. Kopie zapasowe przechowywane były w serwerowni. Od grudnia 2018 r. prowadzono także rejestr procesów/testów odtwarzania kopii zapasowych. Zawierał on informacje o odtworzeniach kopii sporządzonych zarówno ręcznie, jak i przez oprogramowanie *Veritas Backup Exec*.

Przetestowanie narzędzi jedynie przy produkcyjnym odtworzeniu danych nie zapewnia prawidłowości ich funkcjonowania przez dłuższy okres użytkowania. Dlatego testowanie kopii zapasowych sporządzanych skryptem automatycznie wykonującym kopię bazy oraz skryptami umieszczonymi na maszynie danego rozwiązania powinno być kontynuowane.

**26. [projektowanie i eksploatacja systemów teleinformatycznych]** Podejmowano prawidłowe działania związane z monitorowaniem systemów i środowiska ich pracy pod kątem wydajności i pojemności. Jednakże nie wprowadzono zasad w zakresie projektowania, wdrażania oraz wprowadzania zmian w systemach teleinformatycznych.

> Wyjaśniono[106], że w okresie objętym kontrolą wdrożono nowe serwery wraz z oprogramowaniem serwerowym *Vmware.* Rozwiązanie hypernadzorcy *VMware* monitoruje w czasie rzeczywistym serwery pod kątem wydajności i pojemności. Poinformowano, że mając na uwadze, iż *KSAP* jest małą instytucją, nie identyfikowano potrzeby wprowadzenia dodatkowych procedur dot. projektowania i eksploatacji systemów teleinformatycznych.

W celu świadczenia usług elektronicznych *KSAP,* w szczególności powinna wprowadzić zasady dot. projektowania systemu teleinformatycznego umożliwiającego realizację tych usług. Pozwolą one wdrożenie efektywnego systemu wpierającego działalność *Szkoły*.

**27. [zabezpieczenia techniczno-organizacyjne dostępu do informacji]** W *Szkole* nie obowiązywały regulacje wewnętrzne dotyczące minimalizowania wystąpienia ryzyka kradzieży lub utraty informacji, środków przetwarzania informacji oraz urządzeń mobilnych. Brakowało zasad ochrony fizycznej budynków[107] i pomieszczeń *KSAP*, zasad dostępu do pomieszczeń, w tym z ograniczonym dostępem, zasad związanych z monitorowaniem

[104] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.23(1).
[105] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.23(1).
[106] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.11(1).
[107] Tj. budynku *Szkoły* oraz Kolegium *KSAP*.

ruchu osobowego, zarządzania kluczami. Nie spełniono zatem wymogów określonych w § 20 ust. 2 pkt 11 *Rozporządzenia KRI*.

> Wyjaśniono[108], że ogólne zasady bezpieczeństwa, w tym stosowanie fizycznych środków ochrony, wdrożenie *PBI ODO* oraz posługiwanie się przez *Szkołę* profesjonalną obsługą ochrony fizycznej przez wyspecjalizowane firmy, było wystarczające do zapewnienia bezpieczeństwa informacji. Bieżące monitorowanie i analizowanie zagrożeń nie wyklucza rozszerzenia obowiązujących regulacji w zakresie ochrony fizycznej.

*PBI ODO* nie określała zasad ochrony fizycznej, tym samym firma wykonująca usługę ochrony nie zapoznała się z wymogami w zakresie bezpieczeństwa informacji akceptowanymi przez *KSAP*. *Szkoła* nie zapewniała zatem wymaganej minimalizacji potencjalnych zagrożeń.

**28.** Pozytywnie należy ocenić prowadzenie ewidencji ruchu osobowego po terenie *Szkoły* oraz wyposażenie pomieszczeń o podwyższonym poziomie bezpieczeństwa w system alarmowy sygnalizacji włamania. Nie były prowadzone jednak analizy wejść i wyjść na teren *Szkoły* w celu wykrycia nieautoryzowanych działań, w tym również do pomieszczeń z ograniczonym dostępem (z wyjątkiem serwerowni). Należy także ujednolicić praktykę wydawania kart magnetycznych dla *Gości*[109] oraz wzmocnić mechanizmy nadzorcze nad dostępem osób korzystających z *Kafeterii KSAP*.

> Dostęp do budynku *Szkoły* dla pracowników, słuchaczy, absolwentów oraz osób korzystających ze szkoleń organizowanych przez *Szkołę* odbywał się na podstawie wydanych kart magnetycznych. W przypadku zaproszonych *Gości* praktyka ta była niejednolita. Osoby te mogły nie otrzymać karty, gdy wyszedł po nich pracownik *KSAP.* Obligatoryjnie była ona wydawana w przypadku wprowadzenia określonego stopnia alarmowego przez Prezesa Rady Ministrów oraz w sytuacji braku obecności pracownika *KSAP*. Wyjaśniono[110], że *Gość*, któremu nie została wydana karta, przebywa pod nadzorem pracownika, zaś brak wydania karty stanowi wyjątek.
>
> Ewidencję ruchu osobowego osób korzystających z karty magnetycznej zapewniał system informatyczny *UniRCP – rozliczenie czasu pracy*, który gromadził informacje kto i o której godzinie wszedł i wyszedł z terenu *KSAP*. W przypadku uczestników szkoleń i *Gości* widoczny był jej numer, pozwalający na identyfikację uczestnika. System ten pozwalał na wygenerowanie raportu (np. plik xls, pdf, xml) osób, które w danym dniu weszły i wyszły z *KSAP*. Dodatkowo w przypadku *Gości* prowadzona była ewidencja papierowa – *Lista osób wchodzących do budynku KSAP*. Analiza tych informacji w celu wykrycia nieautoryzowanych działań nie była jednak prowadzona. Zapewniono[111], że wszelkie nieautoryzowane wejście do pomieszczeń z ograniczonym dostępem byłoby na bieżąco wykryte.
>
> W przypadku osób wchodzących do *Kafeterii KSAP* z zewnątrz, pracownik recepcji w *Liście osób wchodzących do Kafeterii KSAP*, odnotowywał jedynie dane osobowe danej osoby oraz godzinę wejścia. W ewidencji tej nie było informacji nt. godziny wyjścia, pomimo że osoby te nie otrzymywały karty magnetycznej. Wskazano[112], że osoby poruszające się bez identyfikatorów lub co do których identyfikacja wykaże brak uprawnień do przebywania na terenie budynku, są z niego wypraszane. Pracownicy są regularnie informowani o konieczności zwracania uwagi na osoby obce przebywające na terenie *Szkoły*.

Nieodnotowywanie godziny wyjścia uniemożliwia pracownikowi recepcji prowadzenie bieżącej kontroli ruchu osobowego. Istnieje zatem ryzyko, że wyproszenie osoby przebywającej, mimo braku uprawnień, na terenie *KSAP* nastąpi po dłuższym czasie, który może pozwolić jej na nieuprawniony dostęp do informacji.

**29.** Brak formalnych zasad wydawania i zdawania kluczy do pomieszczeń stwarzał dodatkowe ryzyka nieuprawnionego dostępu i osłabiał system bezpieczeństwa informacji. Pracownik recepcji nie posiadał pełnych informacji kto jest uprawniony do pobrania kluczy

[108] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[109] Osoby umówione na spotkanie z Kierownictwem lub pracownikiem *Szkoły*.
[110] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[111] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[112] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.

i do jakich konkretnie pomieszczeń, ponieważ dokument, którym dysponował nie zawierał informacji odnośnie do pokoi technicznych. Ponadto jednorazowe wjazdy samochodem prywatnym na teren *Szkoły* nie były ewidencjonowane, co uniemożliwiało sprawdzenie, czy nie doszło do nieuprawnionego wjazdu.

> Wydawanie i zdawanie kluczy do pomieszczeń odbywało się na podstawie przyjętej praktyki. Klucze wydawane i przyjmowane były przez pracownika recepcji[113]. Pracownik recepcji posiadał *Spis telefonów KSAP* z informacją, który pracownik pracuje w jakim pokoju, tym samym do którego pokoju posiada uprawnienia w zakresie pobrania kluczy. Jednakże nie była to pełna informacja, ponieważ *Spisie* brak było informacji kto ma dostęp do pokoi technicznych. Pracownikowi recepcji ustnie zostały przekazane informacje, że administrator budynku posiada możliwość pobierania kluczy do wszystkich pomieszczeń[114]. Wskazano[115], że problem ten wymaga analizy i wdrożenia odpowiednich środków.
>
> Dodatkowe klucze do pomieszczeń posiadały również osoby sprzątające, każda do swojej, wyznaczonej strefy budynku. Klucze przechowywane były w ich wspólnym pokoju przez co *de facto* każda osoba miała dostęp do kluczy wszystkich pomieszczeń. Ponadto osoby sprzątające posiadały klucze również do pomieszczeń biurowych, pomimo że miały obowiązek wykonywania swoich czynności w tych pomieszczeniach jedynie w obecności pracowników *Szkoły*. Poinformowano[116], że osoby sprzątające mają świadomość obowiązku sprzątania w obecności pracownika. Natomiast sposób przechowywania przez nie kluczy wymaga analizy i wdrożenia odpowiednich środków.

**30.** *Jednostka* nie posiadała procedur utylizacji dokumentacji, sprzętu i nośników danych, z wyjątkiem tych przetwarzających dane osobowe.

> Wyjaśniono[117], że w okresie objętym kontrolą nie dochodziło do utylizacji sprzętu informatycznego i nośników danych. Podano, że utylizacja odbywa się w *KSAP* w oparciu o rozporządzenie w sprawie szczegółowego sposobu gospodarowania składnikami rzeczowymi majątku ruchomego Skarbu Państwa[118].

Regulacje zawarte w przywołanym rozporządzeniu mają charakter generalny i nie są wystarczające z punktu widzenia bezpieczeństwa informacji, ponieważ nie określają w szczególności zasad kwalifikacji sprzętu do utylizacji, przebiegu procedury utylizacji, częstotliwości i osoby odpowiedzialnej za jej przeprowadzenie.

**31. [zabezpieczenia organizacyjno-techniczne systemów]** Pozytywnie należy ocenić, że przeprowadzono remont i zakupiono dodatkowe wyposażenie do serwerowni. Działania te przyczyniły się do poprawy bezpieczeństwa informacji. Jednakże część z planowanych czynności, w tym związanych z koniecznością uzyskania zgody właściwych organów[119], nie została zrealizowana. Wejście do serwerowni było zabezpieczone i objęte monitoringiem wizyjnym. *Jednostka* prowadziła również ewidencję osób wchodzących, która była analizowana w celu wykrycia nieautoryzowanych działań.

> Wejście do serwerowni zostało wyposażone w systemy zapewniające bezpieczeństwo pomieszczenia i dostęp jedynie upoważnionym pracownikom. Potrzebne są jednak dodatkowe prace remontowe oraz wyposażenie tego pomieszczenia w system pomiaru wilgotności. Wyjaśniono[120], że prace w tym zakresie będą prowadzone, a obecnie przygotowywana jest procedura przetargowa w celu wyboru wykonawcy projektu przebudowy. *Szkoła* nie potrafiła wskazać terminu, kiedy będzie możliwe wszczęcie tej procedury, ponieważ nastąpi ona dopiero po otrzymaniu dotacji na ten cel.
>
> *Szkoła* posiadała również zabezpieczenia na wypadek przerw w zasilaniu, zapewniające ciągłość działania.

---

[113] Pracownik firmy zew. realizującej usługi recepcyjne oraz ochrony na podst. umowy nr 46/KSAP/2019 z 11 lutego 2019 r. oraz nr 35/KSAP/2017 z 8 lutego 2016 r.

[114] Z wyjątkiem kasy, archiwum oraz pokoi: 108, 109, 127 i 133.

[115] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.

[116] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.

[117] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 12 marca 2020 r., znak: PAO.0910.1.2020.16(1).

[118] Rozporządzenie Rady Ministrów z dnia 21 października 2019 r. w sprawie szczegółowego sposobu gospodarowania składnikami rzeczowymi majątku ruchomego Skarbu Państwa (Dz. U. z 2019 r., poz. 2004).

[119] Zgodę otrzymano po okresie objętym kontrolą, tj. 17 lutego 2020 r.

[120] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 27 lutego 2020 r., znak AO.0910.1.2020.18(1).

Pomieszczenie serwerowni stanowi kluczowe miejsce w zakresie bezpieczeństwa informacji, w związku z czym *KSAP* powinna kontynuować czynności związane z poprawą stanu jego bezpieczeństwa i wyposażenia.

**32.** Zagrożenie dla bezpieczeństwa informacji przetwarzanych w *KSAP* stanowi wykorzystywanie oprogramowania, dla którego producent nie zapewniał wsparcia w postaci poprawek bezpieczeństwa (*Windows 7* i starsze).

> W *KSAP* wykorzystywano 1 laptop z oprogramowaniem, dla którego w okresie kontrolowanym producent nie zapewniał wsparcia w postaci poprawek bezpieczeństwa. W marcu br. trwała wymiana komputerów po przetargu i planowana była aktualizacja systemu. Jednakże *Szkoła* nie określiła, kiedy zakończy te działania. Po okresie objętym kontrolą wsparcie nie było zapewnione dodatkowo dla 13 komputerów (w tym laptopów) z systemem Windows 7. Wyjaśniono[121], że w okresie objętym kontrolą sprzęt z oprogramowaniem Windows 7 był w pełni wspierany przez producenta oprogramowania.

Brak możliwości aktualizacji oprogramowania prowadzi do znacznego wzrostu ryzyka wszelkiego rodzaju ataków, a tym samym zagraża bezpieczeństwu informacji gromadzonych i przetwarzanych w *KSAP*.

**33.** Niezasadne było przetwarzanie danych osobowych uczestników szkoleń w ramach *ISRNS* przez okres znacznie dłuższy niż wynikający z *Instrukcji kancelaryjnej*. Informacje przetwarzane w ramach tego systemu przechowywane były ponad 10 lat (czyli o 8 lat dłużej niż przewidywała *Instrukcja*) i nie podlegały pseudonimizacji albo likwidacji w sytuacji, gdy ich przetwarzanie nie było już konieczne z uwagi na prowadzoną przez *Szkołę* działalność. Usuwanie tych danych następowało jedynie na wniosek urzędu zgłaszającego danego pracownika na szkolenie, co było rozwiązaniem niewystarczającym. Sytuacja ta stwarzała ryzyko poniesienia dodatkowych konsekwencji przez *KSAP* w sytuacji nieuprawnionego dostępu do tych danych.

> W *ISRNS* przechowywano informacje[122] od września 2008 r. (tj. najwcześniejszego szkolenia odnotowywanego w tym systemie)[123]. Dane podlegały usunięciu jedynie na prośbę instytucji kierującej danego pracownika na szkolenie[124]. Stanowiło to naruszenie *Instrukcji kancelaryjnej*[125], zgodnie z którą okres przechowywania dokumentacji w zakresie rekrutacji uczestników, bazy szkoleniowej oraz oceny szkolenia wynosił – 2 lata. Wyjaśniono[126], że nie było decyzji dotyczącej likwidacji danych zawartych w *ISRNS* od działu obsługującego system. Art. 6 ust. 1 lit. a (pomocniczo także lit. b) RODO stanowi podstawę prawną umożliwiającą przetwarzanie danych przez okres nawet do 6 lat z uwagi na konieczność zachowania dokumentacji pozwalającej na rozliczenie szkoleń.

Przepisy RODO stanowią podstawę do przetwarzania danych osobowych, nie określają jednak okresu ich przetwarzania. Zgodnie z zasadą ograniczenia przechowywania[127] i motywem 39 preambuły RODO, administrator powinien ustalić okres retencji danych. W myśl *Instrukcji kancelaryjnej* okres przechowywania dokumentacji wynosił 2 lata, zatem po tym czasie dane powinny podlegać usunięciu bądź pseudonimizacji[128].

**34.** Nie zapewniono skutecznego systemu zastępstwa osoby pełniącej funkcję administratora *ISRNS*. Stwarzało to dodatkowe ryzyka zakłóceń i mogło prowadzić do przerwania ciągłości działania systemu, w przypadku awarii lub nieobecności osoby pełniącej tę funkcję. Sytuacja ta zagrażała także bezpieczeństwu danych przetwarzanych w *ISRNS.*

---

[121] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 3 marca 2020 r., znak: PAO.0910.1.2020.19(1) oraz z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[122] W zakresie: szkoleń centralnych, e-learningowych, ofertowych, na zlecenie oraz językowych.
[123] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.21(1).
[124] Protokół oględzin oraz przyjęcia ustnych wyjaśnień w zakresie dostępu do sieci wewnętrznej oraz systemów teleinformatycznych *KSAP* z 25 lutego 2020 r.
[125] Sym. klasyfikacyjne 510, 511, 512 – kategoria archiwalna B2.
[126] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[127] Art. 5 ust. 1 lit. e) RODO.
[128] Zgodnie z komentarzem *Ogólne rozporządzenie o ochronie danych osobowych*, red. dr Marlena Sakowska-Baryła, wyd. 1 z 2018 r. – *ograniczenie czasowe dotyczy przechowywania danych w sposób umożliwiający identyfikację osób, nie zaś przechowywania danych w ogóle. W konsekwencji po upływie określonego czasu administrator, zamiast usunąć dane, mógł je przetwarzać w taki sposób, aby nie było możliwe zidentyfikowanie tożsamości osób, których dane dotyczą, wykorzystując np. pseudonimizację.*

Uprawnienia administratora wszystkich systemów teleinformatycznych w *KSAP* posiadał *ASI*. Pomimo że w przypadku 2 pozostałych systemów teleinformatycznych pełne uprawnienia administracyjne posiadał również Szef Pionu Administracyjno-Organizacyjnego *KSAP*, to w ramach *ISRNS* nie ustalono zasad zastępstwa *ASI* w sytuacji jego nieobecności. Wyjaśniono[129], że system ten jest tak skonstruowany, że pracownik *Szkoły* posiadający uprawnienia do modułu (szkoleń lub języków) może wykonywać każdą operację w ramach tego modułu. Oznacza to, że *zastępstwo administratora jest niepotrzebne i przez lata działania ISRNS nie było takiej konieczności*.

Posiadanie dostępu do wykonywania pełnych operacji w ramach poszczególnych modułów *ISRNS* przez pracowników *Szkoły* nie zapewnia skutecznego zastępstwa dla administratora systemu. Osoby te nie posiadają tożsamych uprawnień jak administrator, umożliwiających całościowe zarządzanie systemem i gwarantujących ciągłość jego działania, choćby w przypadku wystąpienia zakłóceń spowodowanych, np. złośliwym oprogramowaniem.

**35.** Logowanie do *ISRNS* możliwe było przez połączenie nieszyfrowane, co stwarzało ryzyko przejęcia wprowadzanych danych przez osoby nieuprawnione.

Użytkownik *ISRNS* posiadał możliwość zalogowania się do tego systemu zarówno przy wykorzystaniu połączenia szyfrowanego, jak i nieszyfrowanego. *Jednostka* wyjaśniła[130], że jest to etap przejściowy, w którym *ISRNS* domyślnie otwiera się w wersji normalnej (nieszyfrowanej), a użytkownik jest informowany o zaleceniu przejścia na wersję szyfrowaną *ISRNS*. Stan ten wynika ze znajomości adresu nieszyfrowanego przez urzędy oraz podawaniu go w broszurach informacyjnych np. ofercie szkoleń.

Połączenia szyfrowane umożliwiają bezpieczne przesyłanie i pobieranie plików z/do serwera. Użytkownik systemu nie powinien posiadać możliwości wprowadzania danych drogą nieszyfrowaną, gdyż stwarza to dodatkowe ryzyko dla bezpieczeństwa informacji.

**36.** Zagrożeniem dla bezpieczeństwa informacji było przetwarzanie w poczcie elektronicznej niezaszyfrowanych wiadomości e-mail otrzymywanych w ramach usługi *Pekao Collect* o dokonanych wpłatach od kandydatów przystępujących do postępowania kwalifikacyjnego w służbie cywilnej. Szyfrowania takiego nie stosowano, mimo że w *PBI ODO* dostrzeżono, że poczta elektroniczna nie gwarantuje dostatecznej ochrony informacji. Ponadto w *KSAP* obowiązek szyfrowania danych przesyłanych e-mailem nie podlegał monitorowaniu.

System teleinformatyczny – *ISPSC* współpracuje z aplikacją *Pekao Collect*. Dzięki tej usłudze otrzymuje informacje nt. osób dokonujących wpłat za przystąpienie do postępowania kwalifikacyjnego w służbie cywilnej. Z tych informacji generuje się również automatyczny raport zawierający dane osobowe tych osób[131], który otrzymują e-mailem wybrani pracownicy *KSAP*. Informacje na poczcie elektronicznej przetwarzane były w postaci nieszyfrowanej, pomimo że w *PBI ODO*[132] zauważono, że *poczta elektroniczna nie gwarantuje dostatecznej ochrony przesyłanych informacji.* Zatem raporty te nie powinny być przechowywane na poczcie w formie niezaszyfrowanej. W sytuacji braku możliwości szyfrowania takich e-maili, raport powinien być możliwy do pobrania jedynie za pośrednictwem *ISPSC.*

*PBI ODO* zawierała także obowiązek szyfrowania danych osobowych i informacji wrażliwych przed ich wysłaniem. Obowiązek ten nie był monitorowany. *Szkoła* nie wyjaśniła, jakie działania podejmuje dla zapewnienia bezpieczeństwa informacji przesyłanych pocztą elektroniczną i przestrzegania obowiązku szyfrowania danych.

Brak stosowania rozwiązań zapewniających szyfrowanie wiadomości e-mail stwarza ryzyko w zakresie bezpieczeństwa informacji przetwarzanych tą drogą. Nabiera to szczególnego znaczenia w sytuacji możliwości dostępu do elektronicznej poczty służbowej *KSAP* z dowolnego urządzenia posiadającego dostęp do sieci Internet.

[129] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.21(1).
[130] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[131] Raport zawiera informacje nt. imienia i nazwiska kandydata przystępującego do postępowania, jego numer nadany przez system, adres zamieszkania (o ile został podany w przelewie), kwotę wpłaty oraz dane identyfikacyjne dot. przelewu.
[132] Pkt. 3.5. lit. n) załącznika nr 12 do *PBI ODO*, tj. *Procedury użytkowania stanowiska komputerowego i nośników danych.*

**37.** Istotnym ryzykiem w zakresie bezpieczeństwa informacji było wyznaczenie granicy możliwych prób zalogowania do systemu Windows na poziomie 10, tj. system blokował dostęp dopiero po 10 nieudanych próbach.

> W *KSAP* wyznaczono próg 10 nieudanych logowań do systemu operacyjnego Windows na stanowisku roboczym pracownika *Szkoły*, po których możliwość zalogowania się do niego była blokowana na okres 30 min. Wyjaśniono[133], że wynika on z wieloletniego doświadczenia *Jednostki*, dotyczącego efektywnej pracy z użytkownikami. Zdaniem *Szkoły* użytkownicy po 9 nieudanych próbach zalogowania się potrafią samodzielnie przypomnieć sobie hasło. Sytuacja ta dot. głównie użytkowników, którzy nie pracują codziennie w *KSAP*.

Tak duży limit logowań nie jest uzasadniony, ponieważ ma on stanowić zabezpieczenie przed działaniami użytkownika lub programu usiłującego włamać się do systemu przez podawanie kolejno różnych haseł. W przypadku ustalenia limitu logowań na poziomie 10, skuteczność tego zabezpieczenia znacznie maleje.

**38.** **[plan ciągłości działania]** W *KSAP* nie opracowano planu ciągłości działania na wypadek wystąpienia zdarzeń o niskim prawdopodobieństwie, ale o katastrofalnych skutkach, takich jak np. pożar, katastrofa budowlana, terroryzm, powódź. Wyjaśniono[134], że *plany są w trakcie opracowywania.* Brak planu ciągłości działania, który uwzględnia szerokie spektrum ryzyk sprawia, że *Jednostka* narażona była w szczególności na wysokie ryzyko braku kontynuacji działalności w przypadku wystąpienia zdarzeń nadzwyczajnych.

**39.** **[rozliczalność]** *Szkoła* nie posiadała dzienników systemowych 3 eksploatowanych systemów teleinformatycznych, w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych. Stanowiło to naruszenie wymogów § 21 *Rozporządzenia KRI.* Ponadto nie opracowano procedur, w szczególności określających zasady prowadzenia i wykorzystania tych dzienników.

> Wyjaśniono[135], że systemy teleinformatyczne nie odnotowują działań w dziennikach systemowych z uwagi na nieposiadanie przez nie takiej funkcjonalności.

Bezpieczeństwo informacji przetwarzanych w systemach wymaga zapewnienia rozliczalności podejmowanych działań, ponieważ to ona pozwala przypisać określone działania do konkretnej osoby lub procesu oraz umiejscowić je w czasie. Dla zapewnienia pełnej zgodności tego obszaru ważne jest także opracowanie odpowiednich zasad.

## II. Zapewnienie dostępności informacji zawartych na stronie internetowej

**40.** *KSAP* dostosowała stronę internetową[136] do większości wymagań określonych w § 19 *Rozporządzenia KRI*. Należy kontynuować te działania dla osiągnięcia pełnej dostępności treści zawartych na stronie, przez zapewnienie napisów bądź transkrypcji tekstowej do wszystkich materiałów wideo.

> Umowa[137] na utworzenie strony internetowej *Szkoły*, dotyczyła także dostosowania jej do wymagań określonych w § 19 *Rozporządzenia KRI*, tj. *Web Content Accessibility Guidelines* 2.0 (dalej: *WCAG 2.0*). Strona ta była przedmiotem audytu prowadzonego w ramach monitoringu wdrażania postanowień *Konwencji Organizacji Narodów Zjednoczonych o prawach osób niepełnosprawnych*, który dotyczył również innych aspektów związanych z dostępnością, w tym w aspekcie architektonicznym. Jak wynika z *raportu* z 31 stycznia 2019 r. wszystkie rekomendacje dotyczące strony internetowej zostały wdrożone. Wyjaśniono[138], że po terminie przeprowadzenia audytu strona internetowa *KSAP* nie była przebudowywana i nie zmieniała się jej funkcjonalność, układ treści bądź sposób redagowania informacji. Natomiast transkrypcja do materiałów wideo wykonywana jest w ramach możliwości.

[133] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.21(1).
[134] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 10 marca 2020 r., znak:PAO.0910.1.2020.14(1).
[135] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.
[136] Pod adresem: http://ksap.gov.pl/.
[137] Umowa z 1 kwietnia 2014 r., znak: 150/KSAP/2014, zawarta z wykonawcą Direktpoint sp.j.
[138] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 kwietnia 2020 r., znak: PAO.0910.1.2020.28.

## III. Wymiana informacji w postaci elektronicznej

**41.** *KSAP* nie świadczyła usług w formie elektronicznej, jednakże zapewniła komunikację elektroniczną przez skrzynkę podawczą na platformie ePUAP[139]. Spełniono zatem wymogi określone w art. 16 ust. 1a *ustawy o informatyzacji*.

> Wyjaśniono[140], że *KSAP* nie świadczy usług w formie elektronicznej, zatem nie było konieczności opracowania procedur określających deklarowany poziom dostępności usług elektronicznych oraz opracowania wzorów dokumentów elektronicznych i przekazania ich do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych. Planowane są jednak działania związane z wdrożeniem ERP.

Jednym z celów działalności każdej jednostki administracji publicznej jest świadczenie usług dla klientów w sposób jak najbardziej sprawny, szybki i przyjazny. Cel ten można osiągnąć przez świadczenie usług elektronicznych. *Szkoła* powinna zatem rozważyć wdrożenia takich rozwiązań, a wraz z nimi dostosować procedury zarządzania usługami i świadczyć je na deklarowanym poziomie dostępności.

**42.** Obowiązujący w *KSAP* sposób zarządzania dokumentacją uregulowany został w *Instrukcji kancelaryjnej*. Nie wprowadzono elektronicznego systemu zarządzania dokumentacją[141].

Biorąc pod uwagę ustalenia i oceny przedstawione w *Wystąpieniu*, zalecam Panu Dyrektorowi:

1. Opracowanie i wdrożenie kompleksowego, spójnego systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność, integralność gromadzonych i przetwarzanych informacji, w tym:
   - przeprowadzenie przeglądu procedur i regulacji wewnętrznych dotyczących *SZBI,* w tym dokonanie oceny zasadności wdrożonych wymogów, które w praktyce nie były realizowane,
   - ustanowienie systemu zarządzania ryzkiem zapewniającego cykliczną identyfikację ryzyk oraz opracowanie planu postępowania z ryzykiem,
   - wprowadzenie zasad zarządzania incydentami, w tym utworzenie i prowadzenie rejestru zdarzeń i incydentów,
   - opracowanie planów ciągłości działania na wypadek wystąpienia zdarzeń zagrażających realizacji zadań,
   - wprowadzenie systemowych rozwiązań zapewniających prowadzenie audytu wewnętrznego pozwalającego na identyfikację wszystkich słabości *SZBI* oraz niezwłoczne wdrażanie jego rekomendacji.
2. Wdrożenie narzędzi i mechanizmów zarządczych zapewniających Kierownictwu *KSAP* efektywny nadzór nad podejmowanymi działaniami w procesie tworzenia *SZBI* oraz dokonywanie okresowej ewaluacji tego procesu.
3. Prawidłowe zabezpieczenie interesów *KSAP* w zawieranych umowach, w tym wprowadzenie postanowień gwarantujących odpowiedni poziom ochrony i bezpieczeństwa informacji.
4. Modyfikację zabezpieczeń *ISRNS* w celu zapewnienia bezpieczeństwa informacji oraz ograniczenie okresu przetwarzania danych w tym systemie do niezbędnego minimum potrzebnego z uwagi na prowadzoną przez *Szkołę* działalność, a także ustanowienie zastępstwa dla administratora tego systemu.
5. Podjęcie skutecznych działań zapewniających świadczenie usług elektronicznych.

---

[139] http://bip.ksap.gov.pl/index.php?id=752, dostęp 19 lutego 2020 r.
[140] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 25 lutego 2020 r., znak; PAO.0910.1.2020.2(1) oraz 30 marca 2020 r., znak: PAO.0910.1.2020.15(1).
[141] Pismo Szefa Pionu Administracyjno-Organizacyjnego *KSAP* z 30 marca 2020 r., znak: PAO.0910.1.2020.15(1).

6. Podnoszenie świadomości pracowników poprzez podejmowanie cyklicznych działań pozwalających na zwiększanie wiedzy z wykorzystaniem różnych form szkoleń z zakresu bezpieczeństwa informacji.
7. Wyeliminowanie pozostałych nieprawidłowości wskazanych w *Wystąpieniu*.

Proszę Pana Dyrektora o przedstawienie, w terminie 60 dni od daty otrzymania *Wystąpienia*, informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub o przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

Informuję, że od *Wystąpienia* nie przysługują środki odwoławcze.

Podstawa prawna:
Art. 46 ust. 3, art. 47, 48 i 49 *ustawy o kontroli.*

*Z poważaniem*

Michał Dworczyk

Minister-Członek Rady Ministrów

*/-podpisano kwalifikowanym podpisem elektronicznym-/*