WOJEWODA DOLNOŚLĄSKI

Wrocław, dnia 22 lipca 2022 r.

NK-KSE.431.2.2.2022.BJ

Pan
Roman Kowalczyk
Dolnośląski Kurator Oświaty

WYSTĄPIENIE POKONTROLNE

W dniach od 26 kwietnia 2022 r. do 28 czerwca 2022 r. na podstawie przepisu art. 28 ust. 1 pkt 1 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (tekst jedn. Dz.U. z 2022 r., poz. 135 z późn. zm.) i art. 6 ust. 4 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (tekst jedn. Dz. U. z 2020 r. poz. 224) oraz imiennych upoważnień udzielonych przez Wojewodę Dolnośląskiego w dniu 26 kwietnia 2022 r. (NK-KSE.0030.43.2022.BJ, NK-KSE.0030.44.2022.BJ, NK-KSE.0030.45.2022.BJ i NK-KSE.0030.46.2022.BJ) kontrolerzy z Wydziału Prawnego, Nadzoru i Kontroli Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu w składzie: Bartosz Jędrysiak - inspektor wojewódzki (przewodniczący zespołu kontrolnego) i Tomasz Woch - starszy inspektor wojewódzki (członek zespołu) oraz Mateusz Marć – główny specjalista z Biura Administracji i Logistyki (członek zespołu) i Tadeusz Daleczko - starszy informatyk z Biura Administracji i Logistyki (członek zespołu) przeprowadzili w Kuratorium Oświaty we Wrocławiu z siedzibą przy pl. Powstańców Warszawy 1, 50-153 Wrocław, zwanym dalej „KO we Wrocławiu", kontrolę problemową w trybie zwykłym, której tematem było bezpieczeństwo teleinformatyczne jednostki - działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań administracji rządowej na podstawie przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz. U. z 2021 r. poz. 2070, ze zm.) oraz rozporządzenia z dnia 12 kwietnia 2012 r. Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz. U. z 2017 r., poz. 2247).

Kontrola realizowana jest w oparciu o zatwierdzony w dniu 23 grudnia 2021 r. przez Wojewodę Dolnośląskiego plan kontroli na I półrocze 2022 r. (sygn. NK-KSE.430.6.2021.MK).

Kontrolę przeprowadzono w zakresie:

- Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz. U. z 2021 r. poz. 2070, z późn. zm.), zwana dalej u.i.p.r.z.p.
- Rozporządzenia z dnia 12 kwietnia 2012 r. Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz. U. z 2017 r., poz. 2247), zwane dalej r.k.r.i.

Okres objęty kontrolą obejmował czas od dnia 1 stycznia 2020 r. do dnia kontroli. Kontrola została wpisana w książce kontroli prowadzonej w KO we Wrocławiu.

Funkcję kierownika jednostki kontrolowanej w okresie objętym kontrolą pełnił Pan Roman Kowalczyk – Dolnośląski Kurator Oświaty.

W dniu 30 czerwca 2022 r. kierownikowi jednostki kontrolowanej doręczono projekt wystąpienia pokontrolnego sporządzony dnia 29 czerwca 2022 r. Do ustaleń zawartych w niniejszym dokumencie złożono, w przewidzianym do tego terminie (tj. 7 lipca 2022 r.) zastrzeżenia co do ustaleń zawartych w pkt 3.3, pkt 3.12. i pkt 3.13. projektu wystąpienia pokontrolnego. Dnia 22 lipca 2022 r. Dyrektor Wydziału Nadzoru i Kontroli Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, po rozpatrzeniu ww. zastrzeżeń, sporządził wobec nich stanowisko, które wraz z niniejszym wystąpieniem pokontrolnym, przekazano kierownikowi jednostki kontrolowanej.

Treść wystąpienia pokontrolnego, mając na uwadze powyższe oraz przepis art. 46 ust. 2 oraz ust. 3 pkt 1 i pkt 3 ustawy o kontroli w administracji rządowej, obejmuje treść projektu wystąpienia pokontrolnego z dnia 29 czerwca 2022 r., stanowiska z dnia 22 lipca 2022 r. jakie Dyrektor Wydziału Nadzoru i Kontroli Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu zajął wobec wniesionych zastrzeżeń, zalecenia dotyczące usunięcia stwierdzonych nieprawidłowości i usprawnienia funkcjonowania jednostki kontrolowanej oraz termin na poinformowanie o podjętych w związku z ww. zaleceniami działaniach lub o przyczynach ich niepodjęcia.

W związku z powyższym, zgodnie z dyspozycją art. 46 ust. 2 w zw. z art. 47 ustawy o kontroli w administracji rządowej, przekazuję niniejsze wystąpienie pokontrolne. Bezpieczeństwo teleinformatyczne jednostki - działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań administracji rządowej oceniono **pozytywnie z nieprawidłowościami.**

Powyższą ocenę uzasadniają następujące ustalenia z kontroli.

1. Świadczenie usług drogą elektroniczną.

Do jednych z podstawowych celów funkcjonowania urzędu zalicza się realizowanie usług w sposób szybki, sprawny i możliwie jak najbardziej przyjazny dla obsługiwanego podmiotu. Realizację powyższych postulatów w praktyce można uzyskać świadcząc te usługi poprzez platformę elektroniczną dostępną za pośrednictwem sieci Internet. Taki sposób realizacji umożliwia załatwianie spraw w urzędzie bez wychodzenia z domu lub z dowolnego innego miejsca, w którym klient ma dostęp do Internetu. Ma to na celu ułatwienie, jak i usprawnienie obsługi podmiotów, a także eliminowanie korespondencji papierowej na rzecz elektronicznych formularzy i dokumentacji, wypełnianych na platformie usług elektronicznych organu. Podstawową usługą elektroniczną jest Elektroniczna Skrzynka Podawcza (zwana dalej ESP) — miejsce do przyjmowania korespondencji elektronicznej. Obowiązek jej posiadania wynika z art. 16 ust. 1-1a ustawy u.i.p.r.z.p. W wyniku kontroli ustalono, iż KO we Wrocławiu udostępnia na swojej stronie internetowej zarówno adres e-mail, jak i adres skrzynki ESP na platformie ePUAP. Ponadto na stronie BIP kontrolowanego urzędu udostępniono także procedurę składania pism za pośrednictwem platformy ePUAP, jednakże link odsyłający na stronę epuap.gov.pl jest nieprawidłowy, co uniemożliwia skorzystanie z przedmiotowej strony za pośrednictwem wskazanego hiperłącza. Kontrolowany na stronie BIP zamieścił także informację o możliwości doręczania dokumentów do urzędu przy pomocy elektronicznych nośników danych. Powyższy obszar oceniono pozytywnie z nieprawidłowościami.
[dowód: akta kontroli str.: 551-554]

2. Współpraca systemów teleinformatycznych z innymi systemami (interoperacyjność).

Realizując czynności kontrolne kontrolerzy stwierdzili, iż żaden autorski system nie przesyła danych do innych systemów oraz nie pobiera danych z innych systemów, w związku z czym nie było możliwości sprawdzenia zgodności funkcjonowania programów z § 16 ust. 1 r.k.r.i.

Ponadto, w ankiecie dotyczącej działania systemów teleinformatycznych kontrolowany wskazał, że:

„Strony internetowe wytworzone w KO nie komunikują się bezpośrednio z systemami informatycznymi innych urzędów. Dane z aplikacji webowych mogą być przekazywane użytkownikom poprzez strony internetowe lub pliki pdf, excel lub word. Aplikacje umożliwiają ręczne wprowadzanie danych poprzez stronę internetową. Oprócz tego niektóre aplikacje mają możliwość wprowadzania i edycji danych poprzez interfejs ODBC i oprogramowanie Microsoft Assess. Niektóre aplikacje: info.kowroc.pl i kowroc.pl zawierają mechanizm importu danych z pliku csv do niektórych tabel. Aplikacja kowroc.pl zawiera również mechanizm importu danych z RSPO poprzez ogólnodostępne API tego systemu. Aplikacja epoczta.kuratorium.wroclaw.pl działa na tych samych tabelach.
Aplikacje kowroc.pl, info.kowroc.pl i zawody.kuratorium.wroclaw.pl mają osobne bazy i nie komunikują się z innymi aplikacjami.
Strony wykorzystują szyfrowaną transmisję danych z certyfikatem ssl. Zgodnie z zał. 2 do Krajowych Ram Interoperacyjności"
oraz
„Niektóre strony korzystają z kodowania znaków UTF-8, a niektóre są kodowane w ISO 8859-2.

Mając na uwadze powyższe wyjaśnienia należy uznać, iż systemy informatyczne udostępniają zasoby informacyjne zgodnie z § 17 ust. 1 i § 18 ust. 1 r.k.r.i.

[dowód: akta kontroli str.: 40-45, 539-550]

3. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

3.1. Dokumenty z zakresu systemu bezpieczeństwa informacji.

Mając na uwadze przepis § 20 ust. 1 r.k.r.i, podmiot realizujący zadania publiczne zobowiązany jest do opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania, a także utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji, zwanym dalej SZBI, zapewniającego poufność, dostępność oraz integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Niezbędne jest więc opracowanie kompleksowej dokumentacji SZBI, w tym również odpowiednich regulacji wewnętrznych, a także zapewnienia ich aktualizacji w zakresie dot. zmieniającego się otoczenia. Dokumentacja musi być sporządzona w sposób precyzyjny, nie może pozostawiać wątpliwości, co do stosowania zawartych w niej reguł, ponieważ dotyczy wszystkich użytkowników mających dostęp oraz przetwarzających informacje. Opracowanie wszechstronnej dokumentacji SZBI umożliwia efektywne wykonywanie zadań w jednostce, a także właściwe zarządzanie bezpieczeństwem informacji oraz zabezpieczenie interesów jednostki. Kompleksowe podejście do omawianej tematyki powinno uwzględniać rozmaite kategorie informacji, odnosząc się do ich zabezpieczenia, z uwzględnieniem właściwej klasyfikacji, zależnej od profilu działalności podmiotu, m.in. bezpieczeństwo osobowe, informatyczne, fizyczne, prawne, czy technologie

oraz tajemnice jednostki. Jednym z najważniejszych elementów, wchodzących w zakres dokumentacji SZBI jest Polityka Bezpieczeństwa Informacji, która powinna zostać zatwierdzona przez kierownictwo podmiotu, przekazana pracownikom do zapoznania, a następnie regularnie poddawana przeglądowi. Doskonalenie całego SZBI jest szczególnie istotne, ponieważ zapewnia aktualność wszystkich regulacji, co znacząco wpływa na zagwarantowanie właściwego poziomu bezpieczeństwa.

W toku przeprowadzonej kontroli ustalono, iż w Kuratorium Oświaty we Wrocławiu od dnia 25 maja 2018 r. obowiązuje Zarządzenie nr 36/2018 Dolnośląskiego Kuratora Oświaty z dnia 25 maja 2018 r. w sprawie wdrożenia nowej polityki ochrony danych osobowych i instrukcji bezpieczeństwa systemów teleinformatycznych Kuratorium Oświaty we Wrocławiu (dalej: Zarządzenie), celem ochrony danych osobowych oraz zabezpieczenia i zarządzania systemem baz danych osobowych w jednostce. W toku kontroli ustalono, że wszyscy pracownicy Kuratorium Oświaty we Wrocławiu z dniem wejścia w życie ww. przepisów otrzymali je (za pomocą poczty elektronicznej) celem zapoznania się z ich treścią.

Politykę ochrony danych osobowych w Kuratorium Oświaty we Wrocławiu, zwaną dalej Polityką ochrony danych osobowych z 2018 r., wprowadzono załącznikiem nr 1 do Zarządzenia, a zmieniono zarządzeniem nr 13/2020 z dnia 14 lutego 2020 r. (zwana dalej Polityką ochrony danych osobowych z 2020 r.) Wstęp do ww. dokumentu wskazuje, iż ma on za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych.

W kontrolowanej jednostce funkcjonuje również, wprowadzona załącznikiem nr 2 do Zarządzenia Instrukcja Zarządzania Systemem Informatycznym (zwana dalej Instrukcją z 2018 r.). Reguluje ona swoim zakresem takie kwestie jak:
- procedury nadawania i cofania uprawnień, metody i środki uwierzytelniania, wygaszacze ekranu;
- procedury rozpoczynania, zawieszania i kończenia pracy w systemie informatycznym;
- procedury użytkowania urządzeń mobilnych i elektronicznych nośników informacji, korzystanie z Internetu oraz kwestie związane z używaniem poczty elektronicznej.

Zaznaczenia wymaga, iż ww. dokument – zgodnie z § 1 Zarządzenia – ma służyć ochronie przetwarzanych w Kuratorium Oświaty we Wrocławiu danych osobowych.

Wszystkie wskazane dokumenty zostały formalnie zatwierdzone przez kierownictwo jednostki.

Jak zaznaczono powyżej aktualność oraz kompleksowość dokumentacji SZBI jest podstawą prawidłowego funkcjonowania całego systemu oraz ochrony jednostki przed potencjalnymi naruszeniami. Należy jednak negatywnie ocenić fakt, iż Polityki z 2018 r. i 2020 r., jak i Instrukcja z 2018 r., jako główne dokumenty z zakresu SZBI, odnoszą się jedynie do wąskiej kategorii bezpieczeństwa informacji, jakimi są dane osobowe. Z wyjaśnień udzielonych przez kierownika kontrolowanej jednostki w pkt 1 pisma z dnia 27 maja 2022 r.[1] wynika bowiem, iż w Kuratorium Oświaty we Wrocławiu są przetwarzane także, poza danymi osobowymi, dane związane z prowadzonym nadzorem pedagogicznym nad szkołami i placówkami oświatowymi, dane ilościowe o uczniach i nauczycielach, dane finansowo – księgowe związane z działalnością Kuratorium Oświaty we Wrocławiu oraz dane o miejscach wypoczynku organizowanego na terenie Dolnego Śląska. Skutkiem powyższego jest brak uregulowania wielu niezbędnych kwestii zapewniających poufność, dostępność oraz integralność pozostałych kategorii informacji. Dane osobowe są bardzo istotnym, ale tylko jednym z wielu obszarów informacji, które należy odpowiednio zabezpieczać i chronić. Pojęcie bezpieczeństwa informacji jest pojęciem szerszym, obejmującym różne kategorie informacji. Z tych powodów powyższy obszar oceniono pozytywnie z nieprawidłowościami.
[dowód: akta kontroli str.: 40-45, 46-80, 81-92, 93-114, 115-127, 333-335, 354-362]

[1] Znak: WO.021.10.2022, zwane dalej wyjaśnieniami z dnia 27 maja 2022 r.

3.2. Analiza zagrożeń związanych z przetwarzaniem informacji.

Regulacja zawarta w przepisie § 20 ust. 2 pkt. 3 r.k.r.i. wskazuje na konieczność przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzone analizy.

W pkt 2.2. ankiety dot. powyższego zagadnienia, w kol. nr 4 i nr 5 Dyrektor Wydziału Organizacyjnego Dolnośląskiego Kuratorium Oświaty (dalej: Dyrektor) wskazał odpowiednio, cyt.: *„Analiza ryzyka związanego z bezpieczeństwem informacji"* oraz *„jest"*. Ponadto wraz z ankietą przedłożono potwierdzoną za zgodność z oryginałem kopię dokumentu pn. *Analiza ryzyka związanego z bezpieczeństwem informacji* (dalej: analiza). W pkt 4 wyjaśnień z dnia 27 maja 2022 r. kierownik kontrolowanej jednostki wskazał, że ww. dokument sporządzono w grudniu 2018 r., oraz że w kolejnych latach akceptował analizy na rok 2020, 2021 i 2022[2]. Zaznaczenia wymaga, że w związku z brakiem zmiany zakresu ryzyk, od 2018 roku kierownik kontrolowanej jednostki w kolejnych latach akceptował zakres i poziomy ryzyk wówczas ustalone[3].

W pkt 5 ww. dokumentu zdefiniowano następujące zagrożenia mogące mieć niepożądany wpływ na aktywa informacyjne kontrolowanej jednostki:
- zagrożenia naturalne (16 pozycji);
- zagrożenia przypadkowe (37 pozycji);
- zagrożenia umyślne (44 pozycje).

W pkt 6 ww. dokumentu określono z kolei podatności poszczególnych zasobów na zagrożenia tj.:
- podatności dot. sprzętu/mediów (16 pozycji);
- podatności dot. oprogramowania (24 pozycje);
- podatności dot. sieci (6 pozycji);
- podatności dot. personelu (8 pozycji);
- podatności dot. siedziby (8 pozycji);
- podatności dot. organizacji pracy (29 pozycji).

W pkt 7 dla każdego z atrybutów informacji tj. dla poufności, dostępności i integralności ustalono 10-cio stopniową skalę negatywnych skutków jakie dane zagrożenie może wywrzeć na określony zasób:
- 0: brak;
- 1-2: niskie;
-3-5: średnie;
- 6-8: wysokie;
- 9-10: maksymalne.

W niniejszym punkcie analizy określono również, w skali od 0 do 1, skalę prawdopodobieństwa wystąpienia danego zagrożenia:
- 0: brak;
- 0,1-0,2: bardzo niskie;
- 0,3- 0,4: niskie;
- 0,5 - 0,6: średnie;
- 0,7 – 0,8: wysokie:
- 0,9 – 1: bardzo wysokie.

---

[2] Załącznik nr 4 do wyjaśnień z dnia 27 maja 2022 r. zawierający 4 dokumenty (z 20 grudnia 2018 r., 20 grudnia 2019 r., 21 grudnia 2019 r. i 20 grudnia 2021 r.), z których każdy został podpisany przez Dolnośląskiego Kuratora Oświaty, o treści, cyt. *Akceptuję analizę ryzyka związanego z bezpieczeństwem informacji na rok* (...) dot. lat 2019 – 2022.

[3] Patrz: wyjaśnienia zawarte w piśmie z dnia 6 czerwca 2022 r. (znak: WO.021.11.2022), będącym odpowiedzią na wezwanie z dnia 1 czerwca 2022 r.

Na podstawie danych z pkt 7 analizy w pkt 8 określono skalę ryzyk utraty poufności, dostępności i integralności (jako wynik iloczynu czynników *Skutku* oraz *Prawdopodobieństwa*):
- 0: brak;
- 1-2: niskie;
- 3-5: średnie;
- 6-8: wysokie;
-9-10: maksymalne.

Akceptowalny poziom ryzyka określono w wartości 5, powyżej którego należy podejmować działania w celu jego zmniejszenia (pkt 9 analizy).

W wyniku przeprowadzonej analizy ustalono następujące poziomy ryzyk wystąpienia niepożądanych skutków na aktywa. Na 26 aktywów zidentyfikowanych w kontrolowanej jednostce nieakceptowany poziom ryzyka utraty ich poufności wystąpił w 19 z nich, ryzyka utraty ich dostępności wystąpił w 21 z nich, natomiast ryzyka utraty ich integralności w 13 z nich (pkt 10 analizy).

Z kolei w wyniku przeprowadzenia analizy ryzyka utraty poufności, integralności i dostępności poszczególnych zasobów z uwagi na zidentyfikowane zagrożenia naturalne, przypadkowe oraz umyślne, oszacowano, że nieakceptowany poziom utraty poufności występuje w 42 przypadkach, dostępności w 48 przypadkach, a integralności w 16 przypadkach. Zaznaczenia wymaga, że poziom żadnego z ww. ryzyk nie przekraczał wartości 7,0. W wyniku powyższych działań wdrożono 104 zabezpieczenia mające na celu zmniejszenie poziomy ww. ryzyk do wartości akceptowalnych. Podzielono je na nw. grupy:
- ogóle i narzędzia;
- ochrona informacji/danych;
- bezpieczeństwo osobowe/personel;
- ochrona usług;
- ochrona oprogramowania;
- ochrona sprzętu;
- ochrona komunikacji (łączności);
- ochrona nośników danych;
- bezpieczeństwo fizyczne i środowiskowe;
- organizacja;
- procedury i polityki bezpieczeństwa.

W wyniku ich wdrożenia poziomy ryzyk wystąpienia skutków mających negatywny wpływ na aktywa został obniżony do wartości akceptowalnych dla wszystkich z nich, podobnie poziom utraty ryzyka utraty integralności, poufności i dostępności w przypadku wystąpienia zagrożeń naturalnych, przypadkowych oraz umyślnych.

Podsumowując powyższe rozważania należy wskazać, iż kontrolowana jednostka przeprowadziła wymaganą § 20 ust. 2 pkt. 3 r.k.r.i. okresową analizę ryzyka utraty integralności, dostępności lub poufności informacji oraz zidentyfikowała ryzyka utraty poufności, rozliczalności oraz integralności danych osobowych. Określono źródła zagrożeń, ryzyko ich wystąpienia oraz skutki jakie będą one wywierać na poszczególne aktywa. Jako nieprawidłowe należy ocenić, że analiza ryzyka została przeprowadzona w grudniu 2018 r. i od tamtego czasu jej nie ponawiano. Zaznaczenia przy tym wymaga, iż organ kontroli przyjąłby jako prawidłowe, iż ocena wystąpienia poszczególnych ryzyk nie zmieniała się na przestrzeni czasu, gdyby wynikało to z cyklicznie prowadzonych analiz. Brak tych analiz i zatwierdzanie poziomu ryzyk sprzed prawie czterech lat bez udokumentowanych badań tego, czy w dalszym ciągu są one aktualne nie może zostać oceniony pozytywnie. Uwaga ta jest szczególnie aktualna w kontekście tego, iż okres objęty niniejszą kontrolą obejmuje czas, w którym na obszarze całego kraju wprowadzono stan epidemii, co z kolei wymusiło m.in. zmianę sposobu świadczenia pracy w jednostkach administracji publicznej, co niewątpliwie mogło rodzić nowe zagrożenia w zakresie utraty poufności, integralności

i dostępności danych przetwarzanych w kontrolowanej jednostce, które wymagały zidentyfikowania, oceny i ujęcia w kompleksowej analizie.

Należy podkreślić, że analiza ryzyka jest istotnym elementem SZBI, umożliwia wskazanie zagrożeń związanych z przetwarzaniem informacji, a także ustalenie prawdopodobieństwa ich wystąpienia, czy stopień akceptacji ryzyka. Mając na uwadze powyższe należy wskazać, że niniejszy obszar, z uwagi na stwierdzone w nim nieprawidłowości, należy ocenić pozytywnie z nieprawidłowościami.
[dowód: akta kontroli str.: 40-45, 93-114, 128-241, 333-335, 432]

3.3. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

W toku kontroli i w okresie nią objętym stwierdzono następujące regulacje SZBI odnoszące się do obszaru opisywanego w niniejszym punkcie:

• od 1 stycznia 2020 r. do 13 lutego 2020 r.:
Procedura zgłaszania incydentów naruszenia ochrony danych osobowych organowi nadzorczemu została ujęta w pkt. 18 Polityki ochrony danych osobowych z 2018 r. (*Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu*) oraz w załączniku nr 3 do przedmiotowego dokumentu pt. *Zgłoszenie incydentu naruszenia bezpieczeństwa informacji*. Z układu przedmiotowego dokumentu wynika, że należy w nim wskazać, datę, godzinę i miejsce incydentu, aplikację, której on dotyczy, dane użytkownika systemu lub dane osoby zgłaszającej incydent i dane użytkownika sytemu, charakter naruszenia (stanowiący otwarty katalog), świadków zdarzenia oraz jego krótki opis. Ponadto procedura postępowania w przypadku naruszenia ochrony danych osobowych została opisana w załączniku nr 9 do Polityki ochrony danych osobowych z 2018 r. Z kolei w § 8 ust. 3 Instrukcji z 2018 r. zawarto nakaz, aby użytkownicy systemu w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych i systemy teleinformatycznego zgłaszali incydenty Inspektorowi Ochrony Danych, który ma podjąć stosowne działania w tym zakresie (opisane w przedmiotowym przepisie).

• od 14 lutego 2020 r. do dnia rozpoczęcia niniejszej kontroli:
Jak wskazano powyżej w dniu 14 lutego 2020 r. Kierownik kontrolowanej jednostki wydał zarządzenie nr 13/2020, którym wprowadził uaktualnioną (w stosunku do tej wprowadzonej Zarządzeniem) wersję polityki. Przepis § 3 ust. 2 ww. zarządzenia stanowi, że z dniem jego podpisania traci moc zarządzenie nr 36/2018 w zakresie Polityki ochrony danych osobowych z 2018 r. w jej pierwotnym brzmieniu. Zaznaczenia wymaga, że integralną częścią Polityki ochrony danych osobowych z 2018 r. (w jej uchylanej wersji) było 10 załączników, które straciły moc wraz z nią. W pkt 4.5.4. lit. k Polityki ochrony danych osobowych z 2020 r. wskazano, że Inspektor Ochrony Danych w Kuratorium Oświaty we Wrocławiu ma za zadanie m.in. zarządzać naruszeniami ochrony danych osobowych. Z kolei w pkt 4.6. lit. f Polityki ochrony danych osobowych z 2020 r. wskazano, że Administrator Systemu Informatycznego, w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego, ma za zadanie poinformować o tym ww. osobę oraz współdziałać z nią przy usuwaniu skutków naruszenia. Jednym z załączników do ww. dokumentu, podobnie jak do wersji Polityki ochrony danych osobowych z 2018 r. wprowadzonej Zarządzeniem, była *Procedura zarządzania ryzykiem ochrony danych osobowych* (załącznik nr 7). Niemniej jednak dokument ten nie określał (nawet w formie wzoru zgłoszenia) procedury w jaki sposób należy sygnalizować incydenty naruszenia danych. Ponadto w odniesieniu do Polityki ochrony danych osobowych z 2020 r., zaznaczenia wymaga, że w dalszym ciągu obowiązywał § 8 ust. 3 Instrukcji z 2018 r. w wersji wprowadzonej Zarządzeniem, który poza faktem wskazania komu należy zgłaszać ww. incydenty, również nie zawierał innych uregulowań o charakterze proceduralnym.

• od dnia 13 kwietnia 2022 r. do dnia rozpoczęcia niniejszej kontroli:
W dniu 13 kwietnia 2022 r. Kierownik kontrolowanej jednostki wydał zarządzenie nr 21/2022, którym uaktualniono (w stosunku do tej wprowadzonej Zarządzeniem) Instrukcję (Instrukcja z 2022 r.). W § 11 ust. 3 niniejszego dokumentu zawarto zapis, identyczny z tym zawartym w § 8 ust. 3 Instrukcji z 2018 r. w wersji obowiązującej do dnia 12 kwietnia 2022 r.

Z przedstawionego powyżej procesu zmiany przepisów Polityk z 2018 r. i 2020 r. oraz Instrukcji z 2018 r. i 2022 r. od dnia 1 stycznia 2020 r. do dnia rozpoczęcia niniejszej kontroli wynika, że obecnie obowiązujące wersje ww. dokumentów regulują kwestie zgłaszania incydentów naruszania bezpieczeństwa informacji jednie częściowo. Przepis § 11 ust. 3 Instrukcji z 2022 r. stanowi, że właściwym do przyjęcia takiego zgłoszenia jest Inspektor Ochrony Danych. Natomiast z pkt 4.5.4. lit. k i pkt 4.6. lit. f Polityki ochrony danych osobowych z 2020 r. wynika, że ww. osoba, przy usuwaniu naruszeń zabezpieczeń systemu informatycznego, współpracuje z Administratorem Systemu Informatycznego. Ponadto pierwszy z ww. przepisów stanowi, iż odpowiedzialna za przyjęcie zgłoszenia osoba podejmuje działania mające na celu powstrzymanie niepożądanych skutków zdarzenia oraz działania mające zapobiegać tego typu zdarzeniom w przyszłości. Na pozytywną ocenę (z uwagi na rodzaj incydentu) zasługuje też fakt, iż incydent naruszenia bezpieczeństwa informacji, opisany w zgłoszeniu z dnia 13 marca 2020 r. skutkował tym, iż w Instrukcji z 2022 r., wprowadzonej zarządzeniem nr 21/2022, zawarto § 5 (*Skrzynki pocztowe email*) który w pkt 3, pkt 6 i pkt 8 zobowiązuje użytkowników służbowej poczty elektronicznej do tego, aby korzystali z niej w sposób minimalizujący ryzyko naruszenia bezpieczeństwa informacji, aby dane osobowe i informacje poufne przekazywano za jej pośrednictwem w załączniku i po zabezpieczeniu hasłem, które powinno zostać udostępnione odbiorcy inną drogą oraz aby przed wysłaniem każdej wiadomości sprawdzać jej treść, załączniki oraz adresatów.

Niemniej jednak, poza opisanymi w powyższym akapicie okolicznościami zasługującymi na pozytywną ocenę, stwierdzono również następujące nieprawidłowości. Przede wszystkim należy stwierdzić, że w Kuratorium Oświaty we Wrocławiu brak jest kompleksowej procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji. W szczególności SZBI nie określa, w jaki sposób i w jakiej formie[4], należy dokonywać zgłoszeń, a z jego zapisów nie wynika ponadto, aby w kontrolowanej jednostce był prowadzony rejestr incydentów naruszenia bezpieczeństwa informacji. Należy zauważyć, że wraz z zastrzeżeniami do projektu wystąpienia pokontrolnego[5] kontrolowany przekazał dokument z dnia 14 lutego 2020 r. dotyczący Procedury zarządzania naruszeniem ochrony danych osobowych w Kuratorium Oświaty we Wrocławiu, jednakże nie jest to regulacja kompleksowa, obejmująca swoim zakresem wszystkie rodzaje danych przetwarzanych w Kuratorium Oświaty we Wrocławiu, a ograniczająca się jedynie do danych osobowych. Ponadto czas jaki upłynął od wystąpienia incydentu naruszenia bezpieczeństwa informacji do wprowadzenia w SZBI zmian mającymi mu zapobiegać w przyszłości był, w ocenie organu kontroli, zbyt długi (od 13 marca 2020 r. do 13 kwietnia 2022 r., tj. 25 miesięcy). Z powyższym względów niniejszy obszar oceniono pozytywnie z nieprawidłowościami.
[dowód: akta kontroli str.: 46-80, 81-92, 93-114, 115-127, 344-345]

[4] Zaznaczenia wymaga, że zgłoszenie z dnia 13 marca 2020 r., które przedłożono kontrolującym pismem z dnia 27 maja 2022 r. (patrz: pkt 3) zostało sporządzone na wzorze stanowiącym załącznik nr 3 do Polityki w wersji uchylonej w dniu 14 lutego 2020 r.
[5] Wniesionych pismem z dnia 8 lipca 2022 r. (sygn. WO.021.22.2022).

3.4. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Mając na uwadze § 20 ust. 2 pkt 14 r.k.r.i., podmiot realizujący zadania publiczne zobowiązany jest do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Audyt jest jednym z istotnych elementów wpływających na utrzymanie oraz doskonalenie całego SZBI. Pozwala na wskazanie mocnych i słabych stron przyjętych rozwiązań, a następnie ich analizę i podjęcie odpowiednich działań korygujących. Brak audytów uniemożliwia optymalne szacowanie istniejących ryzyk, jak również wyeliminowanie potencjalnych słabości, dlatego też tak ważne jest jego uregulowanie w dokumentach z zakresu bezpieczeństwa informacji.

Ponadto, audyt stanowi kluczowe narzędzie, które pozwala na regularny przegląd SZBI. Niezapewnienie przeprowadzania audytów wewnętrznych jest sprzeczne z § 20 ust. 1 r.k.r.i., który zobowiązuje podmiot realizujący zadania publiczne do monitorowania oraz przeglądania i doskonalenia SZBI. Aktualizacja regulacji wewnętrznych opiera się w znaczącym stopniu na przeprowadzanych audytach oraz realizacji zaleceń poaudytowych, a ich brak może skutkować pominięciem istotnych czynników wymagających zmiany.

W ramach przygotowań do niniejszej kontroli Dyrektor w pkt 2.4. ankiety, w odpowiedzi na pytanie *Czy przeprowadzany jest audyt wewnętrzny w zakresie BI co najmniej raz w roku* w kol. nr 4 ankiety[6] wskazał na § 11 pkt 1 Instrukcji z 2022 r. Zaznaczenia wymaga, że Instrukcja z 2018 r. zawierała analogiczne zapisy z tym, że były one ujęte nie w § 11 lecz w § 8. Brzmienie niniejszego przepisu jest następujące:

„ASI w konsultacji z IOD ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów doraźnych oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych lub wycieku danych, ASI ma obowiązek niezwłocznie powiadomić o tym fakcie IOD oraz ADO. IOD sprawuje nadzór nad wdrożeniem stosownych środków administracyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych. Nadzoruje również funkcjonowanie systemu zabezpieczeń oraz podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia lub podejrzenia naruszenia integralności systemu informatycznego".

Zaznaczenia wymaga też to, iż w kol. nr 5 i nr 6 ankiety Dyrektor nie zawarł jakichkolwiek uwag, ani też nie dokonał samooceny spełnienia powyższego wymogu. Z kolei w pkt 2 wyjaśnień z dnia 27 maja 2022 r.[7] kierownik kontrolowanej jednostki wskazał, iż w Kuratorium Oświaty we Wrocławiu przeprowadzono audyt w zakresie danych osobowych, w czynności przetwarzania „Obsługa danych osobowych". Czynności tych dokonano pomiędzy 14 a 28 listopada 2021 roku a efektem ich przeprowadzania jest raport. W dokumencie tym sformułowano niżej wymienione zalecenia:

- natychmiastowego zaprzestania praktyki udostępniania haseł dostępu do aplikacji i systemów innym użytkownikom;
- dostosować zakresy dostępu poszczególnych pracowników do danych osobowych adekwatnie do wymogów zajmowanego stanowiska pracy;
- wdrożyć stosowanie aktywnego wygaszacza ekranu.

Pierwsze zalecenie miało być wdrożone niezwłocznie, drugie do końca czerwca 2022 roku a trzecie realizowane na bieżąco. W wyniku kontroli stwierdzono realizację pierwszego oraz

[6] Mającej wskazywać dokumenty obrazujące spełnienie wymagania.
[7] W odpowiedzi na zawarte w pkt 2 pisma z dnia 19 maja 2022 r. pytanie dot. tego czy w okresie objętym niniejszą kontrolą w kuratorium były prowadzone jakiekolwiek audyty w zakresie bezpieczeństwa informacji.

trzeciego z zaleceń[8]. W związku z brakiem upływu terminu na wdrożenie drugiego z powyższych zaleceń nie weryfikowano jego faktycznego stosowania.

W toku kontroli stwierdzono ponadto, iż w pkt 13 Polityki ochrony danych osobowych z 2020 r., uregulowano kwestie związane z audytem zgodności przetwarzania danych osobowych. Przepisy te korespondują z § 20 ust. 2 pkt 14 r.k.r.i. ponieważ obligują inspektora ochrony danych w Kuratorium Oświaty we Wrocławiu do przeprowadzenia audytu według planu, który ma obejmować okres od kwartału do roku i uwzględniać co najmniej jeden audyt (pkt 13.2. i 13.3. ww. dokumentu).

Podsumowując należy wskazać co następuje. Na pozytywną ocenę zasługuje fakt przeprowadzenia audytu, w wyniku którego zostały zidentyfikowane słabości i nieprawidłowości w funkcjonującym SZBI, a także podjęte działania w celu ich wyeliminowania, jak również fakt uregulowania kwestii audytu zgodności przetwarzania danych osobowych w dokumentacji z zakresu SZBI. Niemniej jednak negatywnie należy ocenić fakt dokonania w okresie objętym niniejszą kontrolą tylko jednego audytu. Jak bowiem zaznaczono na wstępie § 20 ust. 2 pkt 14 r.k.r.i. obliguje do przeprowadzania co najmniej jednego audytu wewnętrznego rocznie. Podobnie przepisy Polityki – nakazują, aby był przeprowadzany co najmniej jeden audyt rocznie. Wprawdzie jest jeszcze możliwe spełnienie ww. wymogu w roku 2022 r., niemniej jednak z ustaleń kontroli wynika, że w roku 2020 audytu nie przeprowadzano, co stanowi naruszenie ww. przepisu. Należy również zwrócić uwagę na fakt, iż przepis § 11 pkt 1 Instrukcji z 2022 r., na który powołał się Dyrektor wypełniając ankietę, dotyczy przede wszystkim przeglądów technicznych sprzętu. Zaznaczenia wymaga, że w dokumentacji z zakresu SZBI brak jest, w ocenie kontrolujących, przepisów, które kompleksowo regulowałyby kwestie związane z audytem bezpieczeństwa informacji w ogóle, nie ograniczając jej jedynie do danych osobowych. Z powyższych względów niniejszy obszar oceniono pozytywnie z nieprawidłowościami.
[dowód: akta kontroli str.: 40-45, 81-92, 93-114, 115-127, 333-335, 336-343]

3.5. Zarządzanie uprawnieniami do pracy w systemach informatycznych.

Istotnym elementem bezpieczeństwa informacji jest zarządzanie uprawnieniami. Proces ten ma zapewnić, że osoby zaangażowane w przetwarzanie informacji, posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, a w przypadku zmiany/nierealizowania zadań następuje również zmiana/cofnięcie tych uprawnień.

W myśl § 3 pkt 1-2 Instrukcji z 2018 r. dostęp do systemu informatycznego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona przez IOD do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie na wniosek tego pracownika w sposób określony w załączniku nr 5. Czasowego lub trwałego wyrejestrowania z systemu informatycznego dokonuje ASI na wniosek pracownika po uprzedniej akceptacji IOD. W następnych punktach opisano przesłanki czasowego i trwałego wyrejestrowania. Zauważyć należy, iż nie wskazano osoby odpowiedzialnej za zarejestrowanie użytkownika.

Zgodnie z § 3 pkt 1-2 Instrukcji z 2022 r. dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych przez Administratora danych osobowych lub osobę przez niego upoważnioną, w tym zakresie zarejestrowana jako użytkownik w tym systemie, na wniosek bezpośredniego przełożonego tego pracownika. Czasowego lub trwałego wyrejestrowania z systemu informatycznego dokonuje ASI na wniosek kierownika jednostki

[8] Obowiązek zachowania hasła dostępu do aplikacji w tajemnicy istniał już przed przeprowadzeniem audytu – nakładał go § 3 ust. 6 pkt 1 zarówno Instrukcji z 2018 r. jak i Instrukcji z 2022 r.. Faktyczne funkcjonowanie wygaszaczy ekranu zostało zweryfikowane w toczy czynności kontrolnych prowadzonych w siedzibie Kuratorium Oświaty we Wrocławiu przez kontrolerów.

organizacyjnej kuratorium. W następnych punktach opisano przesłanki czasowego i trwałego wyrejestrowania. W nowej instrukcji także nie wskazano osoby odpowiedzialnej za zarejestrowanie użytkownika.

W toku czynności kontrolnych stwierdzono, że wszystkie trzy skontrolowane konta użytkowników stacji roboczych posiadały uprawnienia lokalnego administratora systemu. Mając na uwadze powyższe należy zauważyć, iż posiadanie przez pracowników uprawnień lokalnego administratora systemu może stanowić potencjalne zagrożenie dla danych osobowych znajdujących się na stacjach roboczych tych pracowników, zatem praktykę przydzielania przedmiotowych uprawnień pracownikom, dla których ich posiadanie nie jest konieczne, należy ocenić negatywnie.

W wyniku kontroli stwierdzono, iż dostęp do systemu edu.kuratorium.wroclaw.pl posiadają dwie osoby, które nie figurują na przedstawionym kontrolerom wykazie pracowników tj. Pan Stanisław Chowaniec oraz Pani Magdalena Czukwińska, co także należy ocenić negatywnie.

Podsumowując należy wskazać, iż podmiot kontrolowany przyznał zbyt szerokie uprawnienia użytkownikom stacji roboczych oraz nie wyrejestrował z systemu edu.kuratorium.wroc.pl dwóch osób niebędących pracownikami Kuratorium Oświaty we Wrocławiu, co należy uznać za naruszenie § 20 ust. 2 pkt 4 r.k.r.i. i ocenić negatywnie.
[dowód: akta kontroli str.: 81-92, 115-127, 539-550]

3.6. Praca na odległość i mobilne przetwarzanie danych.

W wyniku kontroli ustalono, iż w Kuratorium Oświaty we Wrocławiu wykonywane były obowiązki służbowe z wykorzystaniem pracy zdalnej/urządzeń mobilnych przy przetwarzaniu informacji. Zgodnie z zapisami § 5 Instrukcji z 2018 r. i § 6 Instrukcji z 2022 r. osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe. Zakazuje się przetwarzania danych osobowych na nośnikach przenośnych bez uprzedniego ich zaszyfrowania bądź innego, odpowiedniego zabezpieczenia oraz przesyłania pocztą elektroniczną. Dodatkowo w Instrukcji z 2022 r. widnieje zapis, iż cała procedura wykorzystywania komputerów przenośnych znajduje się w oddzielnym dokumencie o nazwie „Regulamin użytkowania komputerów przenośnych w KO". W trakcie kontroli przedmiotowy regulamin nie został kontrolerom przedstawiony.

W wyniku kontroli stwierdzono, iż żaden z przedstawionych kontrolerom dokumentów nie określał zasad i warunków pracy zdalnej w Kuratorium Oświaty we Wrocławiu. Zasady przetwarzania danych osobowych w warunkach pracy zdalnej zostały wysłane przez IODO do pracowników za pośrednictwem wiadomości e-mail z dnia 21 stycznia 2022 r. i brzmiały one następująco:

„ – do przetwarzania danych osobowych w warunkach pracy zdalnej wykorzystywane mogą być urządzenia służbowe lub po uzyskaniu zgody DKO prywatne, w tym laptopy i smartfony, z których korzystać mogą wyłącznie osoby upoważnione do przetwarzania danych osobowych, w celach związanych z pracą,
- laptop przed udostępnieniem powinien zostać zweryfikowany przez użytkownika (w razie potrzeby w konsultacji z informatykiem Kuratorium), czy zastosowano w nim wymagane rozwiązania w zakresie bezpieczeństwa, tj. w szczególności zabezpieczenie hasłem, blokowanie komputera hasłowym wygaszaczem ekranu w przypadku braku aktywności użytkownika, konfiguracja programu antywirusowego umożliwiająca jego aktualizację także w miejscu pracy zdalnej,

- za bezpieczeństwo danych osobowych na urządzeniach przenośnych – laptopy, pendrivy, smartfony odpowiedzialny jest pracownik,
- elektroniczne nośniki danych, w tym laptop zawierający dane osobowe, wykorzystywane do pracy poza siedzibą Kuratorium, muszą zostać zabezpieczone hasłem lub poprzez szyfrowanie co najmniej tej części nośnika, która zawiera dane osobowe (np. za pomocą programu kompresującego z opcją szyfrowania),
- zaleca się unikanie połączeń z siecią Internet z wykorzystaniem publicznie dostępnych hotspotów,
- wszelkie wydruki zawierające dane osobowe powinny po zakończeniu pracy zdalnej zostać przetransportowane do siedziby Kuratorium Oświaty we Wrocławiu,
- do realizacji obowiązków służbowych wykorzystywana może być wyłącznie służbowa poczta elektroniczna,
- dane osobowe przekazywane za pośrednictwem poczty elektronicznej powinny zostać zapisane w osobnym pliku, który został uprzednio zaszyfrowany. Hasło do odszyfrowania przesłanego pliku przekazuje się innym kanałem komunikacji (np. telefonicznie),
- w razie braku możliwości zapewnienia bezpieczeństwa danych osobowych przez osobę upoważnioną do przetwarzania danych osobowych, nie jest możliwe korzystanie z systemów teleinformatycznych w ramach wykonywanej pracy zdalnej,
- warunkiem umożliwienia pracy zdalnej wiążącej się z przetwarzaniem danych osobowych jest zastosowanie się do treści powyższego dokumentu.
- w przypadku wystąpienia podejrzenia zagrożenia bezpieczeństwa informacji osobowa upoważniona do przetwarzania danych osobowych zobowiązana jest bezzwłocznie skontaktować się z Inspektorem Ochrony Danych (...)".

Ponadto, w ankiecie dotyczącej działania systemów teleinformatycznych kontrolowany wskazał, że:

„Dodatkowo każde urządzenie mobilne jest nadzorowane poprzez platformę chmurową eset protect cloud pod względem zabezpieczeń antywirusowych oraz szyfrowania dysków wewnętrznych".

W wyniku kontroli stwierdzono, iż jeden z poddanych sprawdzeniu programów (R2Płatnik) działa jedynie lokalnie i nie ma możliwości pracy zdalnej na tym programie.

Mając na uwadze powyższe dokumenty oraz wyjaśnienia należy pozytywnie ocenić spełnienie wymogów z § 20 ust. 2 pkt 8 r.k.r.i. tj. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, jednakże winny być one uregulowane w drodze stosownego dokumentu wewnętrznego stanowiącego część Systemu Zarządzania Bezpieczeństwem Informacji, nie zaś być jedynie przesłane do pracowników za pośrednictwem wiadomości e-mail.
[dowód: akta kontroli str.: 81-92, 115-127, 295-330]

3.7. Zabezpieczenia techniczno - organizacyjne dostępu do informacji.

Budynek, w którym mieści się siedziba kontrolowanej jednostki jest własnością Skarbu Państwa[9] w trwałym zarządzie Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu. W dniu 1 kwietnia 2020 r. ww. jednostka oraz kontrolowana jednostka zawarły porozumienie nr 4/2010/W, na mocy którego Kuratorium Oświaty we Wrocławiu korzysta z pomieszczeń biurowych oraz magazynowych znajdujących się z budynku położonym we Wrocławiu przy pl. Powstańców Warszawy 1[10]. Jednym z obowiązków jakie Użyczający

[9] Zgodnie z informacjami dostępnymi w Systemie Informacji Przestrzennej Wrocławia pod adresem https://gis.um.wroc.pl/imap/?gpmap=gp16.
[10] Patrz: § 1 porozumienia w sprawie użyczenia nr 4/2010/W (dalej: porozumienie).

(tj. Dolnośląski Urząd Wojewódzki we Wrocławiu) ma wobec Biorącego do używania (tj. wobec kontrolowanej jednostki) jest m.in. zapewnienie dozoru obiektu[11], w których to kosztach eksploatacji Biorący w użyczenie partycypuje[12]. Użyczający zobowiązał się zabezpieczyć ww. budynek (i udostępnione pomieszczenia) poprzez zapewnienie całodobowej ochrony[13]. Z kolei pracownicy kontrolowanej jednostki zobowiązali się do przestrzegania zasad pobierania kluczy do udostępnionych im pomieszczeń[14]. Ponadto od dnia 1 stycznia 2015 r. kontrolowana jednostka partycypuje także w kosztach utrzymania systemu gaszenia serwerowni[15].

W toku kontroli ustalono, iż w okresie nią objętym zostały zawarte dwie umowy dot. ochrony osób i mienia znajdującego się w ww. budynku tj. umowa nr AL/2019/425 zawarta w dniu 16 grudnia 2019 r.[16], oraz umowa nr AL./2021/7 zawarta w dniu 18 stycznia 2021 r.[17]. Z ich zapisów wynika m.in. to, że wykonawca zobowiązuje się do świadczenia usługi ochrony osób oraz mienia polegającej w szczególności na całodobowej ochronie mienia i budynku oraz osób się w nim znajdujących, obsłudze portierni oraz do natychmiastowego podejmowania, w razie zagrożenia mienia w budynku, czynności zmierzających do zapobieżenia powstania szkody, a w razie ich powstania do maksymalnego ograniczenia jej rozmiarów, a także do powiadamiania przedstawicieli Zamawiającego i Policji, a w razie potrzeby także Pogotowania Ratunkowego, Straży Pożarnej oraz innych stosownych służb i straży[18]. Ponadto do zadań podmiotu świadczącego ww. usługi należy też m.in. nadzorowanie ruchu osobowego pracowników i klientów, weryfikacja uprawnień do przebywania na obiekcie, niedopuszczanie nieuprawnionych osób do przebywania w pomieszczeniach biurowych i magazynowych i obsługa systemu monitoringu przemysłowego[19]. Zgodnie z § 8 ww. umów osobą upoważnioną w sprawach realizacji ww. umów jest wyznaczony pracownik podmiotu kontrolującego.

Wypełniając ankietę Dyrektor w zakresie niniejszego punktu (pkt 2.7. ankiety) wskazał na § 3 aktualnej instrukcji oraz zaznaczył, iż Kuratorium Oświaty we Wrocławiu korzysta z sieci Internet Dolnośląskiego Urzędu Wojewódzkiego (co wynika wprost z umowy użyczenia, o której mowa powyżej). Zabezpieczenia typu Firewall, monitorowanie ruchu sieciowego oraz zagrożeń jest realizowane przez pracowników jednostki kontrolującej. Dyrektor zaznaczył ponadto, że wszystkie komputery stacjonarne oraz przenośne są monitorowane platformą chmurową ESET PROTECT CLOUD i jednocześnie zaznaczył, że brak jest narzędzi do monitorowania jednostek względem oprogramowania i działań administratorów i użytkowników w systemach teleinformatycznych.

Analiza zapisów § 3 Instrukcji z 2022 r. wskazuje, że jest on podzielony na 6 ustępów obejmujących kolejno:
- nadawanie uprawnień do użytkownika systemu w systemie informatycznym;
- odbieranie uprawnień w systemie teleinformatycznym;
- rozpoczęcie pracy w systemie informatycznym;
- zawieszenie pracy w systemie informatycznym;
- zakończenie pracy w systemie informatycznym;
- informacje ogólne.

Powyższy przepis Instrukcji z 2022 r. opisuje m.in. powinności pracowników Kuratorium Oświaty we Wrocławiu, takie jak np. oględziny miejsca pracy oraz procedura uruchamiania sprzętu, zawieszania pracy na tym sprzęcie oraz zadania do wykonania przed trwałym

---

[11] Patrz: § 3 pkt 4 porozumienia.
[12] Patrz: § 6 ust. 3 pkt 5 porozumienia.
[13] Patrz: § 13 ust. 1 porozumienia.
[14] Patrz: § 13 ust. 3 – ust. 7 porozumienia.
[15] Patrz: § 1 aneksu nr 12 z dnia 17 grudnia 2014 r. do porozumienia, którym dokonano zmiany § 6 ust. .3
[16] Obowiązująca w okresie od 19 stycznia 2020 r. do 19 stycznia 2021 r. (patrz: § 3 przedmiotowej umowy).
[17] Obowiązuje w okresie od 19 stycznia 2021 r. do 19 stycznia 2023 r. (patrz: § 3 przedmiotowej umowy).
[18] Patrz: § 1 ust. 2 lit. a i lit. b i § 2 ust. 2 lit. e zawartych umów
[19] Patrz: § 2 ust. 1 zawartych umów w zw. z częścią I pkt. 1 ppkt 1.5., 1.6., 1.10., 1.15. i 1.17. opisu przedmiotu zamówienia zakończonego podpisaniem umowy nr AL/2019/425.

opuszczeniem miejsca pracy w danym dniu, związane z rozpoczynaniem, zawieszaniem i zakańczaniem pracy w kontekście bezpieczeństwa przetwarzanych informacji. W przepisie tym opisano też zasady nadawania i odbierania uprawnień do pracy w systemie oraz politykę haseł. Zaznaczenia wymaga też fakt, iż w § 5 Instrukcji z 2022 r. opisano zasady bezpiecznego użytkowania poczty elektronicznej, w § 6 zasady dot. komputerów przenośnych, w § 7 zasady dokonywania napraw i utylizacji nośników danych oraz zasady ich zabezpieczania, natomiast w § 8 zasady korzystania z sieci wi-fi. W Instrukcji z 2018 r. obowiązywały § 5 i § 6 odpowiadające treści § 6 i § 7 aktualnie obowiązującej instrukcji. W poprzednio obowiązującej instrukcji brak było przepisu odpowiadającego obecnie obwiązującemu przepisowi § 5 (zasady użytkowania poczty elektronicznej). Niemniej jednak poprzednia instrukcja zawierała w § 7 zapisy dot. monitorowania stacji roboczej pracownika (zasady oraz zakres), których to przepisów obecna instrukcja nie zawiera (na co wskazano powyżej opisując informacje zawarte przez dyrektora w ankiecie).

W toku kontroli ustalono także, iż Kuratorium Oświaty we Wrocławiu korzysta z serwera udostępnianego przez podmiot zewnętrzny, na podstawie zawartej z nim umowy.

Ponadto w pkt 6 wyjaśnień z dnia 27 maja 2022 r. kierownik kontrolowanej jednostki udzielił następujących informacji w zakresie stosowanych w Kuratorium Oświaty we Wrocławiu zabezpieczeń fizycznych, środowiskowych oraz organizacyjnych:
- za ochronę fizyczną obiektu odpowiada Dolnośląski Urząd Wojewódzki (co szczegółowo opisano na wstępie);
- pomieszczenia użytkowane przez Kuratorium Oświaty we Wrocławiu posiadają zabezpieczenia w postaci zamków w drzwiach, zamków w szafach i metalowych szafach pancernych, w których przechowywane są dane kadrowe, księgowe, archiwalne oraz dane Inspektora Ochrony Danych Osobowych;
- pomieszczenia Kuratorium Oświaty we Wrocławiu są wyposażone w czujki przeciwpożarowe oraz w gaśnice natomiast sam budynek posiada instalację odgromową (za ich konserwację i prawidłowe działanie odpowiada Dolnośląski Urząd Wojewódzki);
- sprzęt komputerowy jest chroniony za pomocą listew przeciwprzepięciowych;
- w Kuratorium Oświaty we Wrocławiu został wdrożony i jest stosowany rejestr wydawanych kluczy oraz ewidencja wejść i wyjść.

Odnosząc się do ustalonego powyżej stanu faktycznego należy generalnie pozytywnie ocenić środki zabezpieczenia technicznego dostępu do pomieszczeń Kuratorium Oświaty we Wrocławiu, co wskazuje, że podjęto odpowiednie działania mające zapewnić ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez monitorowanie dostępu do informacji. Powyższe świadczy o tym, że podjęto działania mające na celu wypełnienie wymogów opisanych w § 20 ust. 2 pkt 7 lit. a oraz § 20 ust. 2 pkt 11 r.k.r.i. Niemniej jednak nie można uznać za prawidłowe sytuacji, w której spośród pracowników Kuratorium Oświaty we Wrocławiu nie wyznaczono osoby/osób które należy zawiadomić w przypadku wystąpienia sytuacji nadzwyczajnej (np. pożar, zalanie, włamanie) niosącej za sobą ryzyko utraty danych, ich dostępności lub integralności. Za właściwe nie można również uznać tego, że aktualnie obowiązująca dokumentacja SZBI nie zawiera regulacji dot. monitorowania aktywności poszczególnych użytkowników systemu. Z tego powodu niniejszy obszar oceniono pozytywnie z nieprawidłowościami.
[dowód: akta kontroli str.: 40-45, 81-92, 115-127, 333-335, 458-536, 539-550]

3.8. Zabezpieczenia techniczno – organizacyjne systemów informatycznych.

Kontrola wykazała, iż w zakresie zabezpieczeń technicznych w obszarze dostępu do sieci Internet, Kuratorium Oświaty we Wrocławiu posiada umowę z dnia 18 lutego 2021 r. zawartą z podmiotem zewnętrznym na świadczenie usług hostingowych. W ramach przedmiotowej umowy programy autorskie Kuratorium (edu.kuratorium.wroclaw.pl oraz

kowro.pl) są uruchomione na serwerze firmy zewnętrznej. Wskazany serwer posiada ochronę zapobiegania atakom DDoS, a jego system operacyjny i oprogramowanie jest aktualizowane na bieżąco. Przedsiębiorca zapewnia także zapasową kopię serwera, która jest przetrzymywana przez 28 dni na zewnętrznym urządzeniu oraz całodobowo monitoruje działanie serwera. Brak jednak systemu ochrony aplikacji webowych typu WAF (Web Application Firewall), który zwiększyłby bezpieczeństwo systemów zewnętrznych poprzez automatyczną kontrolę treści wchodzących do aplikacji.

W ocenie kontrolerów stosownym byłoby zawrzeć w przedmiotowej umowie (albo w innym dokumencie) zapis umożliwiający przeprowadzenie kontroli pomieszczenia serwerowni, by samodzielnie móc zweryfikować istnienie i prawidłowość stosowanych przez firmę zewnętrzną zabezpieczeń.

Zasady zabezpieczeń systemów informatycznych zostały określone w § 1 i § 3 Instrukcji z 2018 r. oraz § 1, § 3, § 6-10 Instrukcji z 2022 r.
[dowód: akta kontroli str. 81-92, 115-127, 539-550]

W trakcie kontroli dokonano sprawdzenia komputerów następujących pracowników kontrolowanej jednostki: Ewa Hamera, Magdalena Żurkiewicz-Jurecka, Krzysztof Olechno. Na każdym kontrolowanym komputerze był zainstalowany program antywirusowy firmy Eset endpoint security w najnowszej wersji, posiadał aktualną bazę wirusów oraz wewnętrzny moduł zapory sieciowej. Program antywirusowy jest zarządzany centralnie poprzez Eset protect cloud.

Powyższe ustalenia wskazują, iż w Kuratorium Oświaty we Wrocławiu zapewniono odpowiedni poziom bezpieczeństwa w zakresie nieuprawnionego dostępu z zewnątrz do systemów teleinformatycznych.
[dowód: akta kontroli str.: 539-550]

Jednym z newralgicznych instrumentów zarządzania bezpieczeństwem informacji w systemach teleinformatycznych jest tzw. polityka haseł. Kontrola wykazała, że w Kuratorium Oświaty we Wrocławiu dwustopniowe uwierzytelnianie użytkowników funkcjonuje jedynie przy używaniu systemu R2Płatnik, najpierw na konto użytkownika na danej stacji komputerowej, a potem do stosownego systemu teleinformatycznego, natomiast do programów edu.kuratorium.wroclaw.pl oraz kowroc.pl można dostać się z dowolnego komputera.

W myśl § 3 pkt 1-2 Instrukcji z 2018 r. dostęp do systemu informatycznego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona przez IOD do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie na wniosek tego pracownika w sposób określony w załączniku nr 5. Rejestracja użytkownika polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

Zgodnie z § 3 pkt 1-2 Instrukcji z 2022 r. dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych przez Administratora danych osobowych lub osobę przez niego upoważnioną w tym zakresie zarejestrowana jako użytkownik w tym systemie na wniosek bezpośredniego przełożonego tego pracownika. Rejestracja użytkownika polega na nadaniu identyfikatora i przydzieleniu hasła.

Z § 3 pkt 6 obydwóch Instrukcji wynika, iż użytkownik zobowiązany jest zmieniać hasło w systemie nie rzadziej niż co 30 dni, a hasło nadane przez użytkownika musi się składać co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

W wyniku kontroli stwierdzono, że w Kuratorium Oświaty we Wrocławiu nie ma wdrożonej polityki, która wymusza stosowanie haseł na stacjach roboczych zgodnie z Instrukcjami z 2018 r. i 2022 r. Na jednej z trzech kontrolowanych stacji roboczych (Pana Krzysztofa Olechno) hasło nie było zmieniane w czasie ostatnich 30 dni. Na

kontrolowanych komputerach był natomiast ustawiony wygaszacz ekranu, który uruchamiał się po 10 minutach bezczynności użytkownika.

Kontroli poddano także trzy systemy teleinformatyczne: R2Płatnik, edu.kuratorium.wroclaw.pl oraz kowroc.pl. W wyniku podjętych czynności sprawdzających stwierdzono, że dostęp do systemu R2Płatnik jest zabezpieczony loginem oraz hasłem, a sam program wymusza zmianę hasła co 30 dni oraz wymaga stosowania haseł złożonych. W odniesieniu do systemu edu.kuratorium.wroclaw.pl wykazano, że dostęp do programu wymaga wprowadzenia loginu i hasła, natomiast nie ma on uruchomionej polityki haseł i nie ma wprowadzonej blokady konta po nieudanych próbach logowania. Odnosząc się do systemu kowroc.pl stwierdzono, że posiada on uruchomioną politykę haseł, która wymusza długość hasła z co najmniej 8 znakami. Dodatkowo uruchomiona jest funkcja blokowania konta po 6 nieudanych próbach.
[dowód: akta kontroli str.: 81-92, 115-127, 539-550]

W wyniku kontroli stwierdzono, iż działania Kuratorium Oświaty we Wrocławiu podjęte w zakresie bezpieczeństwa techniczno - organizacyjnego do systemów informatycznych nie wypełniają dyspozycji przepisu § 20 ust. 2 pkt 7 lit. a r.k.r.i. Brak wprowadzenia lokalnej polityki GPO, która będzie wymuszała stosowanie haseł zgodnie z zapisami Instrukcji, przyznanie uprawnień administratora stacji roboczych każdemu pracownikowi oraz niejednolitość zabezpieczeń wprowadzonych na systemach teleinformatycznych kontrolowanego należy ocenić negatywnie.

3.9. Rozliczalność działań w systemach teleinformatycznych.

Rozliczalność jest właściwością systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie. Z tego względu zapewnienie rozliczalności działań polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszystkie działania dostępu do systemu z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i zabezpieczeń, a także działania, gdy przetwarzanie danych podlega prawnej ochronie.

W pkt 8 Polityki Ochrony Danych Osobowych z 2018 r. opisano funkcjonowanie i strukturę Rejestru Czynności Przetwarzania Danych. Następnie wprowadzono nowy zapis w pkt 6.4 Polityki Ochrony Danych Osobowych i wskazano w nim na funkcjonowanie w jednostce Rejestru czynności przetwarzania Administratora danych oraz Rejestru wszystkich kategorii czynności przetwarzania Podmiotu przetwarzającego.

W wyniku kontroli ustalono, iż system edu.kuratorium.wroclaw.pl nie posiada modułu rozliczalności, w przeciwieństwie do systemu R2Płatnik i kowroc.pl.

Zgodnie z § 21 ust. 2 r.k.r.i. w dziennikach systemowych należy odnotowywać działania użytkowników lub obiektów systemowych polegające na dostępie do systemu z uprawnieniami administracyjnymi, konfiguracji systemu, w tym konfiguracji zabezpieczeń, przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Powyższe stanowi naruszenie przepisu § 21 ust. 1 i ust. 2 r.k.r.i., co należy ocenić negatywnie.
[dowód: akta kontroli str.: 46-80, 93-114, 539-550]

3.10. Kopie zapasowe.

Zgodnie z § 20 ust. 2 pkt 12 lit. b r.k.r.i. podmiot publiczny obowiązany jest do zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych

poprzez minimalizowanie ryzyka utraty informacji w wyniku awarii. Do realizacji owego obowiązku niezbędne jest opracowanie odpowiednich procedur i podjęcie określonych w nich działań polegających na zabezpieczaniu przetwarzanych przez jednostkę danych poprzez tworzenie kopii zapasowych zbiorów danych przetwarzanych w niej przetwarzanych.

W § 4 Instrukcji z 2018 r. wskazano procedury i częstotliwość tworzenia kopii zapasowych. Zgodnie ze wskazanym powyżej paragrafem, dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Za wykonywanie kopii zapasowych odpowiadają ASI lub użytkownik jednostki komputerowej. Kopie zapasowe tworzone są na dyskach zewnętrznych bądź nośnikach pendrive, zabezpieczonych hasłem, a wskazane nośniki przechowuje się w miejscu zabezpieczonym przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Po stronie klienta kopie tworzy się raz w miesiącu, a po stronie serwera raz w tygodniu. Wskazany § 4 Instrukcji z 2018 r. nie wskazuje na to, kto odpowiada za sprawdzanie przydatności kopii, za ich przechowywanie i usuwanie.

Kwestie dotyczące kopii zapasowych zawarto także w § 4 i § 10 Instrukcji z 2022 r. Zgodnie ze wskazanymi paragrafami dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych, analogicznie do zapisów poprzedniej instrukcji. Za wykonywanie kopii zapasowych odpowiada użytkownik stacji roboczej wspierany przez ASI. Kopie zapasowe tworzone są na dyskach zewnętrznych bądź nośnikach pendrive, zabezpieczonych hasłem, a wskazane nośniki przechowuje się w miejscu zabezpieczonym przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Kopie zapasowe systemów zewnętrznych wykonuje usługodawca, na podstawie umowy, według ustalonej częstotliwości. Dodatkowo raz w tygodniu ASI tworzy kopie zapasowe plików aplikacji, stron internetowych oraz baz danych systemów zewnętrznych. Analogicznie jak przy poprzedniej instrukcji, nie określono kto odpowiada za sprawdzanie przydatności kopii, ich przechowywanie oraz usuwanie.

Z powyższych zapisów nie wynika, aby Instrukcja określała w sposób precyzyjny jak długo i gdzie są przechowywane kopie zapasowe, czy są przechowywane w inny sposób niż opisano powyżej oraz z jaką częstotliwością są dokonywane odczyty mające potwierdzać ich zdatność do użytku.

W pkt 1-3 wyjaśnień z dnia 23 maja 2022 r. wskazano:

Pracownicy Kuratorium Oświaty we Wrocławiu, co 30 dni, sporządzają we własnym zakresie kopie bezpieczeństwa danych znajdujących się na ich stacjach roboczych oraz po konsultacji z Inspektorem Ochrony Danych Osobowych decydują, jak często i przez jaki okres czasu będzie wykonywał kopie i je przechowywał.
Kopie danych sporządzane są na szyfrowanych pendrajwach. Przestrzeganie obowiązku kopiowania danych ze stacji roboczych, jest przypominane, co jakiś czas, przez starszego informatyka KO oraz Inspektora Ochrony Danych Osobowych.
Także dwa razy w roku, w trakcie przeglądu sprzętu, informatycy przypominają pracownikom o konieczności kopiowania danych na szyfrowanym pendrajwie.
W przypadku problemów technicznych przy kopiowaniu danych, starszy informatyk KO, wspiera pracowników, a IODO udziela niezbędnych informacji dotyczących zabezpieczania kopi danych osobowych.

Kopie serwera kei.pl (pliki oraz bazy danych), na których znajdują się wszystkie aplikacje wytworzone przez pracowników KO, są wykonywane przez informatyków na dwóch niezależnych jednostkach komputerowych, na dodatkowych dyskach SSD. Kopie wykonywane są raz w tygodniu.

Dodatkowo kontrolowany przedstawił potwierdzone za zgodność z oryginałem kopie umów zawartych z usługodawcami systemów zewnętrznych. W trakcie czynności kontrolnych przeprowadzonych w dniu 11 maja 2022 r. stwierdzono, że kopie zapasowe z programu R2Płatnik są wykonywane raz w tygodniu i przetrzymywane powyżej 30 dni na dysku zewnętrznym. W odniesieniu do systemów edu.kuratorium.wroclaw.pl oraz kowro.pl kopie zapasowe są sporządzane i przechowywane przez firmę zewnętrzną.

Podsumowując należy wskazać, że zgodne z § 20 ust. 2 pkt 12 lit. b r.k.r.i. podmiot realizujący zadania publiczne ma obowiązek zapewnić odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych polegający m.in. na minimalizowaniu ryzyka utraty informacji w wyniku awarii. W wyniku kontroli stwierdzono, że kopie zapasowe są wykonywane na szyfrowanych pendrive'ach oraz na dyskach zewnętrznych przez pracowników we własnym zakresie, a w razie problemów technicznych przy wsparciu ASI i IODO. Zgodnie z wyjaśnieniami, użyteczność kopii znajdujących się na stacjach roboczych określa pracownik po konsultacji z IODO, jednakże zapis taki nie znalazł się w żadnej z instrukcji. Kontrolowany nie odniósł się też, ani w instrukcjach ani w wyjaśnieniach, w jaki sposób weryfikowane jest przestrzeganie obowiązku wykonywania kopii zapasowych przez pracowników Kuratorium Oświaty we Wrocławiu. Nie odniesiono się także do kwestii przechowywania wskazanych nośników w miejscu zabezpieczonym przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Ponadto stwierdzono brak uregulowania w dokumentach z zakresu SZBI szczegółowych wytycznych w zakresie czasu przechowywania i procedury przechowywania i usuwania kopii zapasowych. Powyższe braki należy ocenić negatywnie.
[dowód: akta kontroli str.: 81-92, 115-127, 251-253, 254-294, 539-550]

3.11. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Zgodnie z § 20 ust. 2 pkt 2 r.k.r.i. podmiot publiczny zobowiązany jest do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Posiadanie takich informacji jest niezbędne przy wprowadzaniu wszelkich zmian w środowisku informatycznym. Jednocześnie należy podkreślić, że ww. baza nie jest tożsama z zapisami księgi inwentarzowej. Zawiera ona bowiem, w szczególności informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku.

W toku czynności kontrolnych stwierdzono, iż w Kuratorium Oświaty we Wrocławiu nie ma regulacji wewnętrznych z zakresu SZBI, które wskazywałyby na obowiązek i zasady przeprowadzania inwentaryzacji sprzętu i oprogramowania informatycznego. W wyjaśnieniach z dnia 23 maja 2022 r. kontrolowany wskazał:

„Kuratorium na bieżąco dokonuje inwentaryzacji pozostałego sprzętu komputerowego oraz oprogramowania informatycznego przy pomocy zakupionego systemu finansowo-księgowego Quorum. Drugim narzędziem do inwentaryzacji sprzętu jest program INTEGRA. W programie tym, przy każdorazowym zakupie sprzętu, do każdego pracownika przypisany jest laptop, a do pokoju komputer i pozostały sprzęt np. drukarka. Dwa razy w roku wykonywane są przeglądy sprzętu, mające na celu wyłonienie jednostek kwalifikujących się do wymiany. W kuratorium nie ma regulacji wewnętrznych określających zasady przeprowadzania w/w inwentaryzacji.
Co cztery lata, zgodnie z ustawą o rachunkowości, przeprowadzany jest spis z natury środków trwałych, w trakcie którego dokonywana jest inwentaryzacja sprzętu komputerowego. Zbędny

sprzęt i oprogramowanie, jest znoszony ze stanu ewidencji. Ostatnia inwentaryzacja przeprowadzona została w roku 2018".

Następnie pismem z dnia 7 czerwca 2022 r. kontrolowany przekazał kopie spisów inwentaryzacyjnych oraz dokumentów wytworzonych w ramach przeglądów sprzętów.

W wyniku kontroli stwierdzono, że spisy sprzętu sporządzane w systemach Quorum i INTEGRA stanowią zapisy właściwe dla ksiąg inwentarzowych, zatem niewypełniające przesłanek z § 20 ust. 2 pkt 2 r.k.r.i., o których wspominano na początku omawianego zagadnienia. Najbliżej właściwej dla przedmiotowego rozporządzenia formy prowadzenia inwentaryzacji sprzętu i oprogramowania byłaby przedstawiona kontrolerom notatka z analizy rynku dotycząca ustalenia wartości szacunkowej zamówienia na sprzęt w 2021 r. Zawiera ona dokładny opis sprzętu wraz ze wskazaniem pracownika, do którego dane urządzenie zostało przypisane, w tym także system operacyjny komputerów oraz niektóre nośniki danych (pendrive, zewnętrzny dysk SSD). Brak w niej jednak dokładnego wskazania miejsca przechowywania sprzętu czy określenia systemów, które na danym komputerze są wykorzystywane (programy używane do wykonywania obowiązków służbowych). Zauważyć należy, iż przedmiotowa notatka jest zestawieniem zapotrzebowania na sprzęt, który Kuratorium Oświaty we Wrocławiu miało zakupić, nie zaś spisem inwentarza, który faktycznie posiada. Wyjaśnić należy, że brak pełnej, aktualnej informacji o stanie sprzętu i oprogramowania informatycznego może znacząco utrudnić przeprowadzanie rzetelnej analizy ryzyka i przygotowanie pełnego planu postępowania z ryzykiem. W konsekwencji, z uwagi na posiadanie niepełnej wiedzy o stanie swoich aktywów, może mieć trudności z efektywnym zarządzaniem obszarem bezpieczeństwa informacji.

Mając na uwadze powyższe braki, zarówno w regulacjach SZBI, jak i przeprowadzania inwentaryzacji sprzętu i oprogramowania, niniejszy obszar należy ocenić negatywnie.

[dowód: akta kontroli str.: 40-45, 251-253, 433, 434-457]

3.12. Serwis sprzętu i oprogramowania.

W odniesieniu do systemów teleinformatycznych i oprogramowania o znaczeniu krytycznym dla funkcjonowania jednostki niezbędne jest objęcie ich (w zakresie zarówno oprogramowania użytkowego i systemowego, jak i sprzętu) stosownymi umowami serwisowymi, aby zapewnić gwarancję odpowiednio szybkiego wznowienia pracy systemów w przypadku wystąpienia awarii. Umowy takie, zgodnie z §20 ust. 2 pkt 10 r.k.r.i. powinny posiadać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w przypadku wejścia w ich posiadanie przez podmioty serwisujące.

Zgodnie z §8 ust. 1 Instrukcji z 2018 r. ASI w konsultacji z IOD dokonuje przeglądów technicznych sprzętu informatycznego i dba o jego dobry stan techniczny. Przeglądów okresowych dokonuje się co 3 miesiące, natomiast przeglądów generalnych raz na rok. W przypadku wystąpienia usterek technicznych, ASI ma obowiązek poinformować o tym fakcie IOD oraz ADO, a dodatkowo IOD ma obowiązek wprowadzić zabezpieczenia i procedury, by wyeliminować podobne incydenty w przyszłości. W odniesieniu do Instrukcji z 2022 r., w § 11 zawarto zapis, iż ASI w konsultacji z IOD ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego oraz dbać o jego dobry stan techniczny. Zawarto też zalecenie o przeprowadzaniu przeglądów doraźnych (bez wskazania okresów ich przeprowadzania) oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek lub wycieku danych, ASI ma obowiązek powiadomić o tym fakcie IOD oraz ADO, natomiast ADO ma obowiązek wprowadzić odpowiednie procedury i zabezpieczenia, by wyeliminować powstanie podobnego zagrożenia w przyszłości.

W ankiecie dotyczącej działania systemów teleinformatycznych kontrolowany wskazał, iż nie posiada żadnych umów z podmiotami trzecimi, które dotyczyłyby

serwisowania sprzętu lub oprogramowania używanych w Kuratorium Oświaty we Wrocławiu. Dodatkowo w pkt 5 wyjaśnień z dnia 23 maja 2022 r. kontrolowany wskazał, że:

„ W KO za naprawę i serwis IT odpowiadają informatycy. Kuratorium nie posiada żadnych umów serwisowych z podmiotami zewnętrznymi. Panel.kei.pl/webmail jest częścią serwera kei.pl i umowa na tę usługę jest podpisana z kei.pl (...), ale nie jest to umowa serwisowa".

W trakcie kontroli stwierdzono, iż w jednostce kontrolowanej obowiązywał załącznik nr 4 do Polityki ochrony danych osobowych z 2018 r., zatytułowany „wzór umowy powierzenia przetwarzania danych osobowych", określający zasady powierzenia przetwarzania danych osobowych w przypadku świadczenia różnych usług na rzecz Kuratorium Oświaty we Wrocławiu. Wzór ten przewidywał jednak jedynie odpowiedzialność zleceniobiorcy (podmiotu przetwarzającego) wynikającą z rozporządzenia RODO, nie odnosząc się do wewnętrznych regulacji jednostki kontrolowanej. Dnia 14 lutego 2020 r. wprowadzono Politykę ochrony danych osobowych z 2020 r., która uchyliła poprzedni dokument wraz z jego załącznikami (wyłączając Instrukcję z 2018 r.), a nowy dokument nie wprowadził wzoru umowy powierzenia przetwarzania danych osobowych. W piśmie dotyczącym zastrzeżeń do projektu wystąpienia pokontrolnego kontrolowany wskazał, iż w Kuratorium we Wrocławiu korzysta się ze standardowych klauzul umownych wprowadzonych Decyzją wykonawczą Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (Tekst mający znaczenie dla EOG). Zauważyć należy, iż ww. decyzja wykonawcza Komisji Europejskiej obowiązuje od 4 czerwca 2021 r., podczas gdy Politykę ochrony danych osobowych z 2020 r. wprowadzono w dniu 14 lutego 2020 r., zatem przez okres od 14 lutego 2020 r. do 4 czerwca 2021 r. w jednostce kontrolowanej nie funkcjonował żaden wzór umowy powierzenia danych osobowych. Ponadto, wskazane standardowe klauzule umowne odnoszą się jedynie do danych osobowych, nie obejmując swoim zakresem innych danych przetwarzanych w Kuratorium Oświaty we Wrocławiu[20].

Mając na uwadze powyższe należy pozytywnie ocenić niniejszy obszar, mimo braków w regulacjach wewnętrznych dotyczących serwisowania sprzętu i oprogramowania. W przedstawionej kontrolerom dokumentacji nie określono w sposób precyzyjny procedur postępowania w przypadku wystąpienia awarii sprzętu bądź systemu oraz osób odpowiedzialnych za fizyczne dokonanie stosownych napraw.
[dowód: akta kontroli str.: 40-45, 46-80, 81-92, 93-114, 115-127, 251-253,]

3.13. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Zgodnie z § 20 ust. 2 pkt 6 r.k.r.i kierownictwo podmiotu realizującego zadania publiczne ma obowiązek zapewnienia szkoleń dla osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Zgodnie z pkt 14.2 Polityki ochrony danych osobowych z 2018 r. Kuratorium Oświaty we Wrocławiu zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych. W pkt 4.5.4 lit. c Polityki ochrony danych osobowych z 2020 r. zawarto zapis, iż Inspektor Ochrony Danych podejmuje działania zwiększające świadomość

[20] Kategorie danych przetwarzanych w Kuratorium Oświaty we Wrocławiu wskazano w pkt 3.1. niniejszego pisma.

pracowników, szkolenia personelu uczestniczącego w operacjach przetwarzania danych osobowych oraz realizacji powiązanych z tym audytów. W Instrukcji z 2022 r. nie znajdują się żadne zapisy dotyczące szkoleń pracowników.

W ankiecie dotyczącej działania systemów teleinformatycznych kontrolowany wskazał, iż w okresie objętym kontrolną nie odbywały się szkolenia w przedmiotowym zakresie oraz iż ostatnie szkolenie dotyczące cyberbezpieczeństwa odbyło się w 2019 roku. Jednocześnie kontrolowany wskazał, iż pracownikom wysyłane są materiały i informacje do samokształcenia. Dodatkowo w punkcie 6 wyjaśnień z dnia 23 maja 2022 r. kontrolowany wskazał, że:

„Zgodnie z art. 39 ust. 1 RODO, IODO przeprowadza szkolenie każdego nowoprzyjętego pracownika, przed przystąpieniem do pracy, w zakresie przetwarzania i ochrony danych osobowych. Potwierdzeniem takiego stanu rzeczy są załączone kserokopie zaświadczeń przeszkolenia. Szkolenia wstępne prowadzone są m.in. z wykorzystaniem załączonej do pisma prezentacji. Po przeszkoleniu każdy pracownik Kuratorium przetwarza dane osobowe na podstawie upoważnienia wydanego przez administratora danych osobowych, którym jest Dolnośląski Kurator Oświaty. W celu zachowania zasady rozliczalności, upoważnienia wydawane są w formie pisemnej.
W latach ubiegłych, ze względu na panującą epidemię, elementy szkolenia przypominającego z zakresu ochrony danych umieszczane były na wniosek dyrektora wydziału w szkoleniach w formie zdalnej na Platformie TEAMS. Dla pracowników KO inspektor ochrony danych przygotował również filmy instruktażowe, np. Jak hasłować pliki MS Office lub Hasłowanie plików PDF. W celach edukacyjnych wykorzystywane były również ogólnodostępne filmy na kanale Youtube.com. Adresy dostępowe do nich zawarte są w załączonych kserokopiach e-maili wysyłanych do pracowników.
IODO przekazuje pracownikom Kuratorium informacje i materiały do samokształcenia, lub wskazówki jak zgodnie z prawem, w ramach wykonywanych obowiązków służbowych przetwarzać dane osobowe, jak należy realizować obowiązek informacyjny wynikający z art. 13 RODO, jak realizować prawa osób wynikające z art. 15-21 RODO. Potwierdzeniem tego są załączone do pisma wydruki wysyłanych do pracowników e-maili.
Każdy pracownik ma również możliwość skonsultowania z IODO problemów wynikających z ochrony danych osobowych w ramach realizacji obowiązków służbowych.
W zakładce RODO, na wewnętrznej stronie KO, pracownicy mogą zapoznać się z treścią najważniejszych dokumentów dotyczących przetwarzania danych osobowych.
W roku 2019 odbyło się wyjazdowe szkolenie pracowników KO, dotyczące bezpiecznego korzystania z komputera podłączonego do internetu, programu pocztowego, przeglądarki lub pakietu biurowego Office oraz aktywności w internecie. Szkolenie przeprowadzone zostało przez firmę "niebezpiecznik.pl" z Krakowa. Materiały ze szkolenia w załączeniu."
Do przedmiotowych wyjaśnień kontrolowany załączył stosowną dokumentację.

W wyniku kontroli stwierdzono, iż Polityki ochrony danych osobowych z 2018 r. i 2020 r. zawierają jedynie wzmianki na temat szkoleń przeprowadzanych w Kuratorium Oświaty we Wrocławiu, określając ogólnikowo przedmiot i osobę odpowiedzialną za ich przeprowadzanie. W przedmiotowych dokumentach nie zawarto zapisów dotyczących szkoleń dla nowych pracowników ani nie poruszono kwestii monitorowania i stałego podnoszenia poziomu wiedzy pracowników z zakresu bezpieczeństwa informacji.

W Kuratorium Oświaty we Wrocławiu przeprowadzano szkolenia nowych pracowników, w zakresie ochrony danych osobowych, przed ich przystąpieniem do przetwarzania wyżej wymienionych danych, co wskazano w wyjaśnieniach i wykazano poprzez przedstawienie stosownych zaświadczeń.

Zgodnie z wyjaśnieniami oraz przedstawioną dokumentacją, IODO wysyłał pracownikom wiadomości e-mail, które zawierały informacje m.in. o hasłowaniu plików, szyfrowaniu wiadomości e-mail, obowiązkach wynikających z RODO, filmów tłumaczących

kwalifikacje danych jako danych osobowych czy też zasad przetwarzania danych osobowych w warunkach pracy zdalnej.

Podsumowując należy wskazać, iż w Kuratorium Oświaty we Wrocławiu nie organizowano cyklicznych szkoleń z obszaru bezpieczeństwa informacji, a jedynie wysyłano pracownikom materiały do samokształcenia oraz określono zasad dotyczących zapewnienia wiedzy pracownikom w zakresie bezpieczeństwa teleinformatycznego. Wyjaśnienia kontrolowanego dotyczące braku szkoleń z uwagi na wprowadzony w 2020 r. stan epidemii nie mogą zostać uznane za zasadne, gdyż wiele podmiotów oferuje szkolenia online, niewymagające osobistych spotkań organizatora z beneficjentami szkolenia. Mając na uwadze powyższe, wskazany obszar należy ocenić negatywnie.
[dowód: akta kontroli str.: 40-45, 46-80, 93-114, 251-253, 295-330]

Na podstawie ustaleń kontroli, w celu dalszego usprawnienia realizacji kontrolowanego zadania należy:

1. Opracować i wdrożyć kompleksową dokumentację z zakresu SZBI, uwzględniającą wszystkie rodzaje danych, które są przetwarzane w Kuratorium Oświaty we Wrocławiu.
2. Regularnie opracowywać i przeprowadzać analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz audyty z zakresu bezpieczeństwa informacji (nie rzadziej niż raz na rok), uwzględniając w nich wszystkie ryzyka zagrożenia danych.
3. Monitorować posiadane przez pracowników uprawnienia na stacjach roboczych oraz systemach teleinformatycznych, a w razie konieczności podejmować stosowne działania celem dostosowania ich do pełnionych bądź zakończonych funkcji.
4. Wyznaczyć osobę do kontaktu w przypadku wystąpienia sytuacji nadzwyczajnej, niosącej za sobą ryzyko utraty danych, ich dostępności lub integralności.
5. Zawrzeć w SZBI regulacje dotyczące monitorowania aktywności poszczególnych użytkowników systemu oraz wprowadzić rozliczalność w użytkowanych systemach teleinformatycznych zgodnie z § 21 r.k.r.i.
6. Wprowadzić zabezpieczenia techniczno-organizacyjne systemów teleinformatycznych w zakresie lokalnej polityki GPO oraz ujednolicić zabezpieczenia wprowadzone w systemach teleinformatycznych.
7. Doprecyzować w dokumentacji SZBI kwestie tworzenia, przechowywania i usuwania kopii zapasowych oraz kwestie dotyczące odpowiedzialności osób w powyższych procesach.
8. Prowadzić i utrzymywać aktualności inwentaryzacji sprzętu i oprogramowania.
9. Doprecyzować w SZBI zapisy dotyczące serwisu sprzętu i oprogramowania.
10. Prowadzić okresowe szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Proszę o poinformowanie o sposobie wykonania powyższych zaleceń, lub o przyczynach ich niewykonania, w terminie **do dnia 26 sierpnia 2022 r.** (art. 49 ustawy o kontroli w administracji rządowej).

WOJEWODA DOLNOŚLĄSKI
Jarosław Obremski