

**Sprawozdanie ostateczne
z audytu zapewnającego
Zespół Szkół Specjalnych**

Opinia audytora w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze ryzyka objętym zadaniem audytowym zapewnającym:

Audytor wewnętrzny wydaje opinię pozytywną
z nieprawidłowościami stwierdzonymi w toku zadania audytowego.

Temat audytu	Wprowadzenie regulacji dotyczących danych osobowych w jednostkach organizacyjnych miasta.
Numer audytu	1/2021
Cel zadania	Uzyskanie racjonalnej pewności, że: 1. Funkcjonujący system kontroli zarządczej stwarza warunki umożliwiające realizację i egzekwowanie działań wymienionych w Rozporządzeniu 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. 2. Przyjęte w jednostce procedury i wewnętrzne rozwiązania dotyczące ochrony i przetwarzania danych osobowych są zgodne z przepisami RODO.
Zakres podmiotowy	Zespół Szkół Specjalnych im. Matki Teresy z Kalkuty ul. Boryńska 54 Żory
Zakres przedmiotowy	1. Inspektor Ochrony Danych Osobowych 2. Upoważnienia do przetwarzania danych osobowych oraz oświadczenia o zapoznaniu się z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych osób dopuszczonych do przetwarzania danych osobowych 3. Rejestr czynności przetwarzania danych 4. Stosowanie w praktyce zasad określonych w Polityce Bezpieczeństwa i Polityce funkcjonowania monitoringu wizyjnego ZSS 5. Monitoring wizyjny w ZSS 6. Rejestr naruszeń ochrony danych osobowych.

- b) cele przetwarzania;
- c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
- f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

W jednostce jest prowadzony rejestr czynności przetwarzania i zawiera wszystkie elementy wymagane art.30 rozporządzenia RODO.

Załącznik nr 2 – Rejestr czynności przetwarzania.

Ad. 5 Monitoring wizyjny w ZSS

Przedstawiono do wglądu „Procedurę obsługi i korzystania z monitoringu wizyjnego w Zespole Szkół Specjalnych stanowiący Załącznik nr 1 do Zarządzenia nr 35/2018/2019 Dyrektora Zespołu Szkół Specjalnych z dnia 27.08.2019r. Ostatnią zmianę wprowadzono w 21.10.2020r.

1. Stwierdzono, że pomimo zapisów w Polityce monitoringu dot. informacji o nie umieszczaniu kamer w pomieszczeniach sanitarno-higienicznych Dyrektor zdecydował się na ich umieszczenie ze względu na specyfikę szkoły jaką jest Zespół Szkół Specjalnych i jej podopieczni. Dyrektor wyjaśnił, że w łazienkach dochodziło do częstych pobić. Administrator, po przeanalizowaniu czy korzyści z instalacji monitoringu przeważają nad jego niepożądanymi skutkami, decydując o montażu systemu monitoringu, powinien pamiętać o istnieniu tych przestrzeni, w których monitoring jest niedopuszczalny. Chodzi głównie o takie miejsca, jak przebieralnie, szatnie, toalety, natryski czy łazienki. Kodeks pracy wprost wskazuje, że monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni lub pomieszczeń udostępnionych zakładowej organizacji związkowej. Natomiast Prawo oświatowe do obszarów zakazanych zalicza pomieszczenia, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, czy te pomieszczenia, w których uczniom jest udzielana pomoc psychologiczno - pedagogiczna, jak również pomieszczenia przeznaczone do odpoczynku i rekreacji pracowników, sanitarnohigieniczne, gabinet profilaktyki zdrowotnej, a także szatnie i

	4. Polityka bezpieczeństwa w Zespole Szkół Specjalnych im. Matki Teresy z Kalkuty, 5. Polityka funkcjonowania monitoringu wizyjnego w Zespole Szkół Specjalnych im. Matki Teresy z Kalkuty wprowadzona 21.10.2020r. <u>Ustalenia stanu faktycznego:</u> <u>Ad. 2 Upoważnienia do przetwarzania danych osobowych oraz oświadczenia o zapoznaniu się z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych osób dopuszczonych do przetwarzania danych osobowych w ramach projektu " Wzmocnienie potencjału edukacyjnego Zespołu Szkół Specjalnych im. Matki Teresy z Kalkuty o numerze: RPSL.11.01.04-IŻ.01-24-254/18</u> Upoważnienia do przetwarzania danych osobowych w ramach projektu RPSL.11.01.04-IZ-24-254/18 otrzymali: - - - - - - - - - - - - - - - - - - - Wszyscy w/w pracownicy zostali wpisani do Ewidencji osób upoważnionych do przetwarzania danych osobowych, która prowadzona jest w wersji elektronicznej przez Inspektora ochrony danych.
III. Kategoria oceny kontroli zarządczej - efektywność.	Kryterium oceny: dostępność – ocena, czy dane systemy informatyczne (zasoby) były dostępne zgodnie z wymaganiami użytkownika poufność – ocena, czy dane i informacje były ujawnione tylko tym, którzy mają prawo je poznać integralność – ocena, czy dane i informacje były zabezpieczone przed nieautoryzowanymi (zarówno umyślnymi, jak i nieumyślnymi) modyfikacjami

Na podstawie obserwacji ustalono, iż na biurku znajdują się dokumenty niezbędne do wykonywanej w danym momencie pracy. Zastosowano zabezpieczenie przed dostępem osób nieupoważnionych do biurka, dokumentów poprzez właściwe ustawienie biurka.

- Sposób niszczenia niepotrzebnych dokumentów i danych wygenerowanych z systemu:

Zgodnie z informacjami uzyskanymi od pracowników podczas rozmowy niepotrzebne dokumenty niszczone są w niszczarce.

- Obowiązek informacyjny wynikający z art. 13 RODO:

Na stronie Zespołu Szkół Specjalnych, w zakładce Aktualności/ Rodo, zamieszczona została Klauzula informacyjna zawierająca wszystkie informacje zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO) (Dz. Urz. UE L 2016 Nr 119, s.1).

- Blokowanie systemu podczas opuszczenia stanowiska pracy w trakcie dnia pracy

Zgodnie z § 10 pkt 4 Polityki Bezpieczeństwa ZSS pracownik zobowiązany jest do niepozostawiania bez kontroli włączonych urządzeń zawierających dane osobowe oraz niezabezpieczonych dokumentów (czasowe opuszczania stanowiska pracy jest dopuszczalne dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu urządzenia w inny sposób). W Monitorach komputerów zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.

- Stosowanie identyfikatorów i haseł

Zgodnie z Polityką bezpieczeństwa dostęp do zbiorów danych służącym do przetwarzania danych osobowych w ZSS wymaga podaniu identyfikatora i właściwego hasła. Z przyjętych dobrych praktyk hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem. Hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego. Hasła są zmieniane przez użytkownika. System informatyczny winien być wyposażony w mechanizm wymuszający zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła (w Polityce jest tylko informacja o

Ustalenia w zakresie słabości kontroli zarządczej:

Nr ustalenia i poziom ryzyka	Nr ustalenia stanu faktycznego: 1. Poziom ryzyka: wysokie/ <u>średnie</u> /niskie
Kategoria / kryterium których ustalenie dotyczy	Kategoria kontroli zarządczej: legalność <u>Kryterium ustalenia stanu faktycznego:</u> art. 10 ust.4 ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2019r, poz. 1781),
Treść ustalenia dot. słabości kontroli zarządczej wraz ze wskazaniem ich przyczyn. Nr dowodu	<u>Ustalenia stanu faktycznego:</u> Inspektorem ochrony danych osobowych w dniu rozpoczęcia audytu zgodnie ze zgłoszeniem była Pani Aleksandra Cnota Mikołajec, a faktycznie funkcję tę pełnił Pan Roman Kamiński, który został zgłoszony do UODO z dniem 29.06.2021 roku. <u>Przyczyny:</u> Nieznajomość przepisów – zgłoszenie zmiany IOD należy zgłosić w ciągu 14 dni od dnia jego wyznaczenia.
Skutki lub ryzyka wynikające ze wskazanych słabości kontroli zarządczej	Brak zgłoszenia inspektora danych osobowych pomimo powołania go w jednostce.
Zalecenia w sprawie wyeliminowania słabości kontroli zarządczej lub wprowadzenia usprawnień	Należy postępować zgodnie z art. 10 ust.4 ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2019r, poz. 1781).
Adresat	Dyrektor ZSS
Drobne uwagi / spostrzeżenia	

Nr ustalenia i poziom ryzyka	Nr ustalenia stanu faktycznego: 2. Poziom ryzyka: wysokie/ <u>średnie</u> /niskie
Kategoria / kryterium których ustalenie dotyczy	<u>Kategoria kontroli zarządczej:</u> efektywność <u>Kryterium ustalenia stanu faktycznego:</u> Polityka bezpieczeństwa ZSS
Treść ustalenia dot. słabości kontroli zarządczej wraz ze wskazaniem ich przyczyn. Nr dowodu	<u>Ustalenia stanu faktycznego:</u> System w jednostce nie wymusza zmiany hasła, użytkownik systemu powinien mieć obowiązek i zmieniać to hasło co 30 dni. System informatyczny powinien być wyposażony w mechanizm pozwalający

	Natomiast Prawo oświatowe do obszarów zakazanych zalicza pomieszczenia, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, czy te pomieszczenia, w których uczniom jest udzielana pomoc psychologiczno - pedagogiczna, jak również pomieszczenia przeznaczone do odpoczynku i rekreacji pracowników, sanitarnohigieniczne, gabinet profilaktyki zdrowotnej, a także szatnie i przebieralnie. Miejsca monitorowane powinny być wyznaczone tam, gdzie dochodzi do incydentów albo istnieje realne zagrożenie dla bezpieczeństwa, zaś niemożliwe jest objęcie takich miejsc innymi formami nadzoru, jak np. w przypadku szkół dyżurami nauczycieli czy pracowników. W polityce monitoringu znajduje się zapis dot. przechowywania obrazu z monitoringu, który jest nietożsamy z informacją przedkładaną pracownikom odnośnie stosowania monitoringu wizyjnego w jednostce: w §4 pkt 10 zapisano: Pełny obraz z monitoringu przechowywany jest na dysku twardym przez minimum 14 dni, nie dłużej jednak niż 3 miesiące, (materiał na dysku komputera nadpisuje się , a jego długość przebywania na dysku jest uzależniona od ilości ruchu obiektu).” W informacji o stosowaniu monitoringu dla pracowników: „Nagrania z monitoringu przechowywane są do 30 dni licząc od daty nagrania (w przypadku gdy nagranie będzie stanowić dowód, lub będzie mogło stanowić dowód w postępowaniu prowadzonym na podstawie przepisów prawa – do czasu prawomocnego zakończenia postępowania).” Dodatkowo stwierdzono w Rejestrze czynności przetwarzania: Cel przetwarzania: zapewnienie bezpieczeństwa uczniów i pracowników oraz ochrony mienia (dot. Monitoringu) w rubryce Planowany termin usunięcia danych wpisano: dane nadgrywają się po 8 dniach licząc od daty zapisu. <u>Przyczyny:</u> Brak spójności w dokumentach dotyczących czasu przechowywania na dyskach zapisów z monitoringu.
Skutki lub ryzyka wynikające ze wskazanych słabości kontroli zarządczej	Ryzyko działania niezgodnie z przepisami prawa.
Zalecenia w sprawie wyeliminowania słabości kontroli zarządczej lub wprowadzenia usprawnień	Ujednolicenie dokumentacji wewnętrznej dotyczącej terminu przechowywania zapisów z monitoringu wizyjnego.
Adresat	Dyrektor ZSS
Drobne uwagi / spostrzeżenia	