



EDUODO

EDU ODO – Kacper Gordeew
Ul. Zamiejska 14, 44-270 Rybnik
NIP: 6423203506, biuro@eduodo.pl

Podsumowanie realizacji audytu

Nazwa jednostki audytowanej: Szkoła Podstawowa nr 11 im. Hugona Kołłątaja w Gliwicach, ul. Pocztowa 31, 44-100 Gliwice.

Data przeprowadzenia audytu: 15 marca 2023 r.

Audytory: Aleksandra Cnota-Mikołajec – Inspektor Ochrony Danych

Wstęp

Niniejszy audyt bezpieczeństwa informacji przeprowadzony został w celu regularnej weryfikacji, czy ochrona danych osobowych w jednostce spełnia wymogi określone w przepisach o ochronie danych osobowych.

Cel zadania audytowego

Celem badania audytowego było ustalenie czy w jednostce dane osobowe są prawidłowo przetwarzane i chronione. Głównym przedmiotem badania było ustalenie, czy wdrożone i opracowane dokumenty i procedury związane z ochroną danych osobowych są aktualne i stosowane w praktyce przez osoby upoważnione oraz ocena, czy stosowane rozwiązania zapewniają przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa, ze szczególnym uwzględnieniem ochrony praw i wolności osób, których dane osobowe są przetwarzane.

Niniejszy raport skupia się na ochronie danych osobowych od strony formalno-prawnej oraz na ocenie rozwiązań technicznych i organizacyjnych stosowanych do ochrony danych przetwarzanych w formie papierowej i elektronicznej.

Podstawa prawna audytu

Za podstawę przeprowadzenia audytu uznaje się 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 oraz Ustawę o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. 2019 poz. 1781)

Zastosowana metodologia

Audyt został przeprowadzony z wykorzystaniem następujących metod:

- Zebranie informacji z przygotowanej ankiety audytowej,
- Wywiad z pracownikami oraz administratorem danych osobowych,
- Analiza udostępnionej dokumentacji,
- Audyt wizyjny siedziby podmiotu.

Analiza polityk bezpieczeństwa oraz procedur dotyczących bezpieczeństwa przetwarzania danych osobowych

Obszar audytowany: Sprawdzenie, czy wprowadzona dokumentacja jest aktualna względem stanu faktycznego.

Stan faktyczny: W jednostce wprowadzono wszystkie niezbędne dokumenty i procedury związane z przetwarzaniem danych osobowych. W jednostce przeprowadza się też okresowo wymagane oceny skutków i analizy ryzyka przy przetwarzaniu danych osobowych. Do tej pory sporządzono je dla następujących obszarów przetwarzania: monitoringu wizyjnego, systemu informacji oświatowej. Wszystkie dokumenty prowadzone są poprawnie, w sposób zgodny z przepisami. Są one również aktualne względem stanu faktycznego. W przypadku konieczności naniesienia zmian na dokumentację została wyznaczona osoba odpowiedzialna za ich aktualizację. Osobą tą jest Inspektor Ochrony Danych.

Rekomendacja: Zaleca się podtrzymanie zasad stosowanych do tej pory.

Analiza stanu upoważnień do przetwarzania danych osobowych

Obszar audytowany: Sprawdzenie stanu upoważnień do przetwarzania danych osobowych

Stan faktyczny: Do przetwarzania danych osobowych zgodnie z ustawą mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez Administratora Danych. W trakcie działań audytorskich stwierdzono, iż wszystkie osoby mające dostęp do danych osobowych na terenie podmiotu posiadają stosowne upoważnienia. Zatrudnienie nowych pracowników zgłaszane jest Inspektorowi Ochrony Danych, który przygotowuje w dniu zatrudnienia upoważnienie. Te z kolei przekazywane jest Administratorowi, który w momencie podpisywania umowy z pracownikiem upoważnia go do przetwarzania danych osobowych.

Rekomendacja: Zaleca się podtrzymanie aktualnie panujących zasad i zgłaszanie konieczności przygotowania dokumentów niezbędnych przy zatrudnieniu Inspektorowi Ochrony Danych.

Analiza regulacji związanych z monitoringiem wizyjnym

Obszar audytowany: Weryfikacja zgodności wprowadzonego monitoringu wizyjnego względem wymogów prawnych oraz sprawdzenie wprowadzonych dokumentów.

Stan faktyczny: Jednostka została zabezpieczona systemem kamer, który umożliwia rejestrację obrazu. Monitoring nie umożliwia rejestracji fonii. System monitoringu obejmuje teren zewnętrzny wokół szkoły oraz teren wewnątrz – korytarze na parterze, pół pięttrze i pierwszym pięttrze, suterengę i wejście główne.

Do nagrań dostęp posiadają wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych w systemie monitoringu wizyjnego. W jednostce wprowadzono regulamin monitoringu wizyjnego, który na dzień przeprowadzania działań audytorskich jest aktualny względem przepisów oraz stanu faktycznego. Administrator podpisał również odpowiednie oświadczenie o wprowadzeniu monitoringu, a wszyscy zatrudnieni pracownicy podpisali oświadczenia, z których treści wynika, iż zostali oni poinformowani o tym fakcie. Obowiązek informacyjny, którego spełnienie jest istotne w przypadku stosowania monitoringu wizyjnego spełniany jest w zrozumiałej formie i zgodnie z literą prawa poprzez zamieszczenie klauzuli informacyjnej m.in. na stronie internetowej oraz na wejściach do jednostki. Każda osoba wchodząca na teren jednostki jest informowana o stosowaniu monitoringu wizyjnego przez tabliczki z napisem „obiekt monitorowany”. Tabliczki są umieszczone w taki sposób,

osoby wchodzące na teren zostały poinformowane zanim ich wizerunek zostanie przetworzony w systemie.

Rekomendacja: Zaleca się podtrzymanie aktualnego stanu oraz informowanie IOD o zachodzących zmianach w systemie monitoringu wizyjnego.

Analiza zapewnienia aktualności systemów operacyjnych

Obszar audytowany: Sprawdzenie aktualności systemów operacyjnych stosowanych na stacjach roboczych w jednostce

Stan faktyczny: W toku działań audytorskich ustalono, że jednostka posiada wyłącznie system Windows. Aktualizowany jest on każdorazowo, gdy dostępna jest aktualizacja. Jednostka posiada wyłącznie systemy, dla których oferowane jest wsparcie producenta – Windows 10 i Windows 11.

Rekomendacja: Zaleca się utrzymywanie aktualnie panujących zasad.

Analiza zapisów związanych z bezpieczeństwem informacji na stronie internetowej

Obszar audytowany: Sprawdzenie spełnienia obowiązku informacyjnego na stronie internetowej jednostki oraz sprawdzenie wprowadzenia zapisów związanych z przetwarzaniem plików Cookies.

Stan faktyczny: Jednostka posiada własną stronę internetową znajdującą się pod adresem: <https://www.sp11.gliwice.pl/>. W związku z tym, jednostka winna spełniać następujące wymogi:

- Zamieszczenie obowiązku informacyjnego: spełnia – klauzula zamieszczona jest w zakładce „RODO”,
- Zabezpieczenie strony certyfikatem SSL: spełnia – strona jest zabezpieczona certyfikatem,
- Umieszczenie na stronie danych kontaktowych Inspektora Ochrony Danych: spełnia – dane zamieszczone są w zakładce „RODO”,
- Wyświetlanie paska lub okienka informującego użytkownika strony o przetwarzaniu plików Cookies: spełnia – w pasku zamieszczono hiperłącze przenoszące użytkownika do właściwej zakładki,
- Utworzenie Polityki Prywatności dla strony: spełnia – Polityka zamieszczona jest w zakładce „Polityka Prywatności” na dole strony.

Szkoła posiada także stronę BIP: <https://sp11.bip.gliwice.eu/>. Na stronie BIP znajdują się dane Inspektora Ochrony Danych oraz klauzula informacyjna.

Rekomendacja: Zaleca się utrzymywanie aktualnie panujących zasad.

Analiza naruszeń przepisów o ochronie danych osobowych

Obszar audytowany: Sprawdzenie, czy w audytowanej jednostce odnotowano naruszenia przepisów o ochronie danych osobowych

Stan faktyczny: W trakcie działań audytorskich przeprowadzono wywiad z pracownikami oraz administratorem danych osobowych. Zgodnie z ich ustnymi oświadczeniami w jednostce nie doszło do żadnego naruszenia przepisów o ochronie danych osobowych, który wymagałby przeprowadzenia postępowania wyjaśniającego i sporządzenia protokołu wewnętrznego z naruszenia.

Rekomendacja: Zaleca się systematycznie przypominać pracownikom o konieczności zgłaszania do administratora danych lub inspektora ochrony danych każdego przypadku naruszenia przepisów o ochronie danych osobowych.

Przeprowadzenie wizji lokalnej wraz z weryfikacją wprowadzenia zaleceń z poprzednich audytów bezpieczeństwa informacji

Obszar audytowany: Sprawdzenie obszarów przetwarzania danych osobowych pod kątem przestrzegania przepisów, procedur i zasad związanych z bezpieczeństwem informacji

Stan faktyczny: Dostęp do budynku ograniczony jest poprzez stosowanie zamykanych drzwi i okien. Dostęp do pomieszczeń ograniczony jest poprzez stosowanie zamykanych drzwi. W trakcie działań audytorskich nie stwierdzono otwartych pomieszczeń pozostawionych bez opieki pracownika. Zasady czystego biurka oraz czystego ekranu są stosowane przez pracowników. Monitory wszystkich komputerów są ustawione tak, aby osoby postronne nie miały w nie wglądu. Dodatkowo wszystkie komputery zabezpieczone są hasłem systemowym, wygaszaczem ekranu i automatyczną blokadą dostępu w przypadku dłuższej nieobecności pracownika.

Rekomendacja: Brak zaleceń w tym zakresie.

Aleksandra Cnota-Mikołajec

Cnota Mikołajec Aleksandra

Inspektor Ochrony Danych

(pieczęć i podpis audytora)

