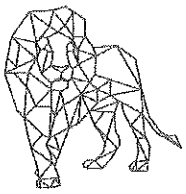

EDUODO

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

Podsumowanie realizacji audytu

Nazwa jednostki audytowanej: *Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach*
Data przeprowadzenia audytu: *19 październik 2022 r.*
Audytorzy: *Aleksandra Cnota - Mikołajec – Inspektor Ochrony Danych*

Wstęp

Niniejszy audyt bezpieczeństwa informacji przeprowadzony został w celu 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

Niniejszy audyt został przeprowadzony w siedzibie Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach, ul. Kozielska 1, 44-100 Gliwice
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 zostały wprowadzone dokumenty takie jak:*

- *regulamin ochrony danych,*
- *załącznik do regulaminu,*
- *rejestr czynności,*
- *rejestr kategorii czynności,*
- *rejestr naruszeń,*
- *instrukcja postępowania w sytuacji wystąpienia naruszenia,*
- *regulamin monitoringu wizyjnego,*
- *oceny skutków dotyczące:*
    - *monitoringu wizyjnego,*
    - *systemu informacji oświatowej,*
- *rejestr udostępnień danych osobowych,*
- *instrukcja szyfrowania plików.*

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 placówki i bramy wjazdowe*
- *wewnątrz: wejście główne oraz ciągi komunikacyjne wewnątrz budynków*

Do nagrań dostęp posiadają wyłącznie osoby upoważnione. W jednostce wprowadzono regulamin monitoringu wizyjnego, który na dzień przeprowadzania działań audytorskich jest aktualny względem przepisów oraz stanu faktycznego. Administrator wprowadził 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".

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.*
W jednostce funkcjonuje system Windows 10.

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* ***http://www.ckziu.gliwice.pl****. Obowiązek informacyjny znajduje się w zakładce „RODO", spełniany jest zgodnie z przepisami i w zrozumiałej formie. Na stronie internetowej jest wyświetlany pasek informujący użytkownika, że strona przetwarza pliki cookies dla różnych celów. Polityka prywatności wraz z informacjami dotyczącymi przetwarzania ciasteczek została przygotowana. Strona nie jest zabezpieczona certyfikatem SSL.*

Rekomendacja: *Zaleca się wykupienie certyfikatu SSL aby zabezpieczyć stronę.*

Analiza wzorów druków udostępnionych na stronie internetowej

Obszar audytowany: *Sprawdzenie, czy wzory druków udostępnionych na stronie internetowej jednostki zawierają treści wymaganych zgód i klauzulę informacyjną*

Stan faktyczny: *Na stronie internetowej jednostki udostępniono druki do pobrania.*
Nie wszystkie dokumenty zawierają niezbędne klauzule informacyjne.

Rekomendacja: *Zaleca się uzupełnienie klauzul na dostępnych do pobrania dokumentach.*

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 budynków 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 wzorowo.*
Rekomendacja: *Brak zaleceń w tym zakresie.*

Aleksandra Cnota-Mikołajec
Inspektor Ochrony Danych
(pieczęć i podpis audytora)