Szkolenie ODO:
Przetwarzanie danych osobowych w placówkach oświatowych

Słów kilka o szkoleniu

Niniejsze szkolenie jest skierowane do pracowników placówek oświatowych, w szczególności nauczycieli. W ramach tego szkolenia przypomnimy Państwu podstawowe pojęcia ochrony danych osobowych i podstawy przetwarzania, które zilustrowane zostaną przykładami.

Poza tym dowiedzą się Państwo:

- jak przetwarzać dane w ramach rekrutacji do placówki oświatowej,
- jak bezpiecznie przetwarzać dane w ramach codziennych zadań,
- jak zorganizować zdalne nauczanie.

Spis treści

Przypomnienie podstawowych pojęć

Prezentowane poniżej pojęcia stanowią najistotniejsze z naszego punktu widzenia definicje, których przypomnienia wymaga dalsza część szkolenia.

Dane osobowe

Dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Pojęcie danych osobowych jest pojęciem bardzo szerokim. Daną osobową może być imię, nazwisko, numer PESEL, ale również pseudonim lub numer w dzienniku. Kluczowym kryterium, czy jakąś informację należy uznać za daną osobową, stanowi możliwość zidentyfikowania na jej podstawie osoby fizycznej. Jeżeli więc jakaś informacja jest wystarczająca, by ustalić o kogo chodzi, będzie ona daną osobową.

Niektóre z danych osobowych, takie jak imię czy nazwisko, są oczywiste. Istnieją jednak inne dane, które niekoniecznie wydają się osobowymi. Należą do nich np. adresy poczty elektronicznej e-mail, numer w dzienniku, pseudonim, nick.

Przetwarzanie danych osobowych

Przetwarzanie to operacja lub zestaw operacji wykonywanych na danych osobowych. Przetwarzaniem będzie więc utrwalanie, modyfikowanie, przenoszenie, kopiowanie, niszczenie i inne czynności, jakie będą wykonywane na danych osobowych. Należy zwrócić uwagę na to, że przetwarzaniem mogą być również te czynności, które nie mają charakteru czynnego, takie jak przechowywanie.

Z pewnością więc będzie przetwarzaniem danych prowadzenie rekrutacji, dziennika lekcyjnego (w formie papierowej lub elektronicznej), brakowanie dokumentów z przebiegu nauczania.

Przetwarzaniem będzie również przechowywanie dokumentów w formie archiwum, choćby nawet nie do końca było wiadomo, jakie znajdują się w nich dane. Na marginesie, niewykluczone jest, że w archiwum znajdują się dane nadmiarowe, jak choćby kopie dowodów tożsamości w aktach osobowych pracowników.

Administrator

Administrator to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem jest więc placówka oświatowa. Częstym błędem jest określanie administratora zawsze jako osobę fizyczną. W przypadku szkoły, to ona będzie administratorem danych, a dyrektor występować będzie w roli przedstawiciela administratora.

Pomimo więc tego, że czynności związane z ochroną danych osobowych faktycznie wykonuje dyrektor, a w praktyce również inne wyznaczone do tego osoby, są one wykonywane w ramach organizacji administratora, czyli szkoły.

Podmiot przetwarzający i powierzenie przetwarzania danych osobowych

Mianem podmiotu przetwarzającego (zwanego również procesorem) określa się podmiot, który przetwarza dane osobowe w imieniu administratora. W uproszczeniu: jeżeli pewne czynności, które zwykle mógłby samodzielnie wykonywać administrator, nie są możliwe do zrealizowania (np. na ze względu na brak osoby posiadającej odpowiednie kwalifikacje, np. informatyka, księgowej), mogą one zostać zlecone podmiotowi zewnętrznemu. Jeżeli do realizacji tych zadań wymagane są działania obejmujące dane osobowe (np. uczniów, pracowników), to dochodzi w takiej sytuacji do powierzenia przetwarzania tych danych.

Podmiot przetwarzający przetwarza dane w imieniu administratora, który ustala sposoby i cele tego przetwarzania. Procesor nie może ustalać sposobów i celów przetwarzania, a jest zobowiązany do działania w ramach polecenia uzyskanego od administratora.

Powierzenie przetwarzania danych osobowych powinno zostać udokumentowane umową lub innym instrumentem prawnym.

Udostępnienie

Jedną z operacji przetwarzania danych osobowych jest udostępnienie. Polega ono na przekazaniu danych poza organizację administratora odrębnemu administratorowi danych.

Przykładem udostępnienia może być przekazanie danych do podmiotu leczniczego mającego przeprowadzić badania z zakresu medycyny pracy.

Udostępnienie bywa często mylone z powierzeniem przetwarzania. Główną różnicą pomiędzy udostępnieniem a powierzeniem przetwarzania jest to, że przy udostępnieniu podmiot pozyskujący dane samodzielnie ustala cele i sposoby ich przetwarzania, nie będąc związanym poleceniem podmiotu udostępniającego dane.

Analiza ryzyka

Analizą ryzyka określa się mechanizm pozwalający na zidentyfikowanie ryzyka wystąpienia zagrożeń oraz ich potencjalnych skutków, mające na celu takie ukształtowanie systemu ochrony danych poprzez wdrożenie środków zabezpieczeń, by ryzyko wystąpienia zagrożeń było jak najniższe.

Przeprowadzenie analizy ryzyka powinno w szczególności poprzedzać wdrożenie nowych rozwiązań, jak choćby wprowadzenie komunikatorów (np. Microsoft Teams, Google Hangouts) w celu umożliwienia komunikacji nauczycieli z uczniami w ramach zdalnego nauczania.

Analiza ryzyka polega na zidentyfikowaniu poszczególnych zagrożeń, ocenie ryzyka ich wystąpienia, a w przypadku gdyby nie było ono akceptowalne, wdrożeniu środków mających na celu obniżenie tego ryzyka.

W wyniku przeprowadzenia analizy ryzyka może okazać się, że konieczne będzie przeprowadzenie oceny skutków dla naruszenia praw i wolności osób fizycznych, a więc oceny jak daleko idące negatywne konsekwencje może wywołać wystąpienie któregoś ze zidentyfikowanych zagrożeń.

Zautomatyzowane podejmowanie decyzji

Zautomatyzowanym podejmowaniem decyzji jest wydanie decyzji w wyniku wprowadzenia do systemu kryteriów, które następnie system przetwarza i na tej podstawie wydaje samodzielnie decyzję wywołującą skutki wobec osoby, której dotyczy.

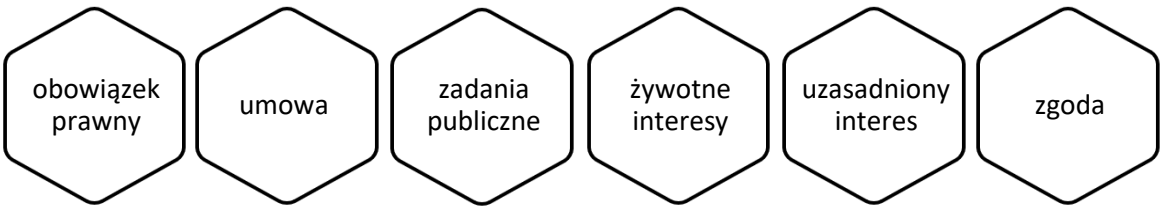
Zautomatyzowanym podejmowaniem decyzji jest więc sytuacja, gdy system podejmuje decyzję bez udziału człowieka. Z sytuacją taką można spotkać się na przykład w przypadku prowadzenia rekrutacji elektronicznej. Placówka, udostępniając formularz elektroniczny złożony z kryteriów (ustawowych i uchwalonych miejscowo), nie dokonuje sama podsumowania realizowanych kryteriów. Są one zliczane automatycznie i na podstawie tego działania system decyduje o przyjęciu albo nieprzyjęciu kandydata.

Podstawy przetwarzania danych osobowych

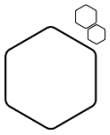
Dla przypomnienia, zgodnie z RODO, podstawą przetwarzania danych zwykłych może być:

- zgoda (art. 6 ust. 1 lit. a RODO),
- umowa (art. 6 ust. 1 lit. b RODO),
- obowiązek prawny (art. 6 ust. 1 lit. c RODO),
- żywotne interesy (art. 6 ust. 1 lit. d RODO),
- zadania publiczne (art. 6 ust. 1 lit. e RODO),
- uzasadniony interes (art. 6 ust. 1 lit. f RODO).

Powyższa kolejność przedstawiona w RODO nie pokrywa się jednak z kolejnością, którą należy kierować się w praktyce. Szukając podstawy do przetwarzania powinno się stosować do następującej kolejności:



Przykładem obowiązku prawnego może być prowadzenie dokumentacji przebiegu nauczania. Na podstawie umowy placówki mogą organizować dodatkowe zajęcia, obsługę księgową, itp. Działając w ramach zadań publicznych, zgodnie z poradnikiem opracowanym przez Urząd Ochrony Danych Osobowych i Ministerstwo Edukacji Narodowej, placówki realizują cele oświatowe, takie jak wyróżnianie uczniów za ich osiągnięcia i organizowanie okazjonalnych wydarzeń. Dane będą przetwarzane na podstawie żywotnych interesów w sytuacjach kryzysowych, wymagających szybkiej reakcji, takich jak wypadki. Uzasadnionym interesem placówki będzie ustalanie, dochodzenie i obrona roszczeń. Wreszcie, jeżeli nie znajdzie zastosowania żadna z powyższych przesłanek, konieczne będzie uzyskanie zgody na przetwarzanie danych, jak choćby w przypadku publikacji fotografii zawierającej wizerunek ucznia.



Rekrutacja do placówek oświatowych

Rekrutacja do placówek oświatowych stanowi jeden z głównych obszarów, w którym napotkać można wątpliwości co do ochrony danych osobowych. Poniżej postaramy się zmierzyć z najważniejszymi jej aspektami.

Podstawy przetwarzania i zakres danych osobowych

Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe reguluje prowadzenie procesu rekrutacji. Jednym z bardziej istotnych z punktu widzenia ochrony danych osobowych są przepisy art. 150 i 151. Wskazują one, jakich danych można wymagać od kandydata oraz jego rodziców lub opiekunów prawnych. Danymi tymi są imię i nazwisko, data urodzenia, numer PESEL, adres miejsca zamieszkania kandydata. Dodatkowo, możliwe jest pozyskanie innych danych na podstawie kryteriów dodatkowych uchwalanych miejscowo.

Pozyskanie danych wykraczających poza zakres wskazany w przepisach obowiązującego prawa skutkować będzie zebraniem danych nadmiarowych, a w konsekwencji bezpodstawnego przetwarzania tych danych.

Przetwarzanie danych osobowych na potrzeby rekrutacji odbywa się w ramach obowiązku prawnego placówki, a więc znajduje swoją podstawę w przepisie art. 6 ust. 1 lit. c RODO.

Mając na uwadze w szczególności przepisy regulujące zakres danych, jakich można wymagać od kandydata i jego rodziców lub opiekunów prawnych, należy zadbać o aktualność dokumentów wykorzystywanych w trakcie rekrutacji, aby nie wykraczały one poza ten zakres.

Należy pamiętać, że ponieważ rekrutacja odbywa się na podstawie obowiązku prawnego (art. 6 ust. 1 lit. c RODO), to niewłaściwym postępowaniem będzie odbieranie zgody na przetwarzanie danych w ramach rekrutacji (art. 6 ust. 1 lit. a RODO). Wymóg taki, oprócz swojej nieprawidłowości, wprowadzałby w błąd osób wnioskujących co do możliwości wycofania zgody, które to uprawnienie nie znajdzie w tej sytuacji zastosowania choćby z uwagi na obowiązek przechowywania dokumentacji z postępowania przez określony czas.

Przedwczesne oświadczenia

Kolejną związaną z rekrutacją kwestią jest odbieranie wszelkiego rodzaju oświadczeń. Częstą praktyką jest przedwczesne odbieranie oświadczeń lub innych dokumentów, jak np. upoważnienie do odbioru dziecka z placówki. Praktykę tę należy ocenić z punktu widzenia ochrony danych osobowych jako niewłaściwą, ponieważ nie są to dokumenty wymagane na etapie rekrutacji, a dopiero po przyjęciu dziecka do placówki. Z tego względu czynności te powinny odbyć się dopiero wtedy, gdy rekrutacja będzie zakończona i wiadomo będzie, względem których osób należy je przeprowadzić.

Obowiązek informacyjny

W ramach procesu rekrutacji należy pamiętać o realizacji obowiązku informacyjnego, np. poprzez przekazanie klauzuli informacyjnej zawierającej informacje dotyczące przetwarzania danych osobom składającym dokumenty rekrutacyjne.

Jednocześnie wspomnieć należy, że przekazanie tych informacji nie zwalnia później placówki z ich uzupełnienia wobec osób przyjętych, ponieważ inne będą w tym przypadku choćby cele przetwarzania danych.

Rekrutacja elektroniczna

W miarę postępu cyfryzacji w podmiotach publicznych, coraz częściej spotykana formą jest właśnie prowadzenie rekrutacji w formie elektronicznej. Tak jak w przywołanym wyżej przykładzie, rekrutacja taka polega na udostępnieniu formularza elektronicznego, przy pomocy którego należy wskazać informacje o spełnianiu poszczególnych kryteriów. Następnie system podlicza automatycznie podane dane, wskazuje wynik i decyduje o przyjęciu albo nieprzyjęciu do placówki.

Korzystanie z tego typu rozwiązań wiąże się z koniecznością zapewnienia odpowiedniego środowiska informatycznego, w szczególności z uwagi na ilość i charakter danych podlegających przetwarzaniu. Należy mieć również na względzie procedurę postępowania w przypadku zgłoszenia żądania osoby fizycznej, ponieważ zgodnie z RODO każdy ma prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu.

Publikacja wyników

Częstym pytaniem zadawanym przez dyrektorów placówek jest pytanie o zakres danych, jakie można wskazać przy publikacji wyników rekrutacji i formę takiej publikacji.

Materię tę reguluje przepis art. 158 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe. W przepisie tym wskazano, że publikacji podlega lista kandydatów zawierająca imiona i nazwiska oraz informację o zakwalifikowaniu albo niezakwalifikowaniu.

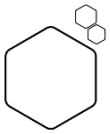
Prawo oświatowe wskazuje również sposób publikacji tych list. Zgodnie z przepisami, publikacja list polega na umieszczeniu ich w widocznym miejscu w siedzibie placówki. Z tego względu, co do zasady nie należy publikować wyników rekrutacji na stronach internetowych placówek. Wyjątkiem mogą być szczególne sytuacje, np. obostrzenia sanitarne w przypadku epidemii SARS-CoV-2.

Korzystanie z e-dziennika

W wielu szkołach zdecydowano się na prowadzenia dziennika w formie elektronicznej. Rozwiązanie to oferuje nie tylko możliwość zdalnego dostępu do ocen, ale również komunikowanie się z rodzicami lub opiekunami prawnymi, a nawet przekazywanie informacji o zwolnieniach z zajęć lekcyjnych. W związku z tym dochodzi do przetwarzania sporej ilości danych osobowych.

Tak jak w przypadku elektronicznej rekrutacji, tak i tutaj konieczne jest wdrożenie odpowiednich zabezpieczeń informatycznych. Poza tym, kluczowe jest przyswojenie podstawowych zasad ochrony danych osobowych, takich jak blokowanie dostępu w czasie nieobecności przy stanowisku, czy niezapisywanie haseł dostępu oraz ich okresowa zmiana.

Nawyki te są szczególnie istotne w przypadku korzystania z dziennika w warunkach domowych, co stanowi wyzwanie w przypadku prowadzenia zdalnego nauczania, o którym w dalszej części szkolenia.



Dane osobowe w pokoju nauczycielskim

Doświadczenie audytowe wskazuje, że częstym źródłem pytań i problemów są pokoje nauczycielskie. Oczywiście różnią się one w zależności od placówek, jednakże możliwe jest wskazanie kilku wspólnych punktów.

Dane osobowe w dokumentach i na tablicach

Przede wszystkim, pokoje nauczycielskie są miejscem, w którym można zlokalizować dużą ilość danych osobowych. Mogą to być zwolnienia, dzienniki, informacje o zastępstwach, sprawdziany i wiele innych. Najbardziej istotna jest odpowiednia kontrola nad nimi oraz właściwe ich przechowywanie. Sytuacją niedopuszczalną jest pozostawianie dokumentów w sposób umożliwiający zapoznanie się z ich treścią przez osoby nieuprawnione.

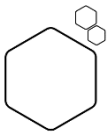
Wspólny komputer

Często spotykanym rozwiązaniem jest ogólnodostępny laptop lub komputer, z którego skorzystać mogą wszyscy nauczyciele. Często też, choć wydaje się to nie być oczywiste na pierwszy rzut oka, zapisywane są na ich dyskach dane osobowe. Z tego względu zalecane jest, aby stosować wzory bez wskazywania konkretnych danych, pamiętać o wylogowaniu się z systemu po skorzystaniu z niego, a w celu jak najdokładniejszego rozdzielenia uprawnień dostępowych, wydzielenie odrębnych kont/ profili dla nauczycieli.

Zamykanie drzwi

Wreszcie, co wydaje się oczywistością, lecz w praktyce bywa często naruszane, należy przykładać szczególną uwagę do odpowiedniego zabezpieczania pokoju nauczycielskiego przed dostępem do niego osób nieuprawnionych.

Wiąże się to z koniecznością zamykania go podczas nieobecności nauczycieli, niezależnie od tego, jak długo ma być pozostawiony w tym stanie.



Ochrona danych osobowych w zdalnym nauczaniu

Obostrzenia sanitarne, będące konsekwencją epidemii SARS-CoV-2 wymusiły szybkie przejście z systemu nauczania stacjonarnego na zdalne nauczanie. Spowodowało to niemałe zamieszanie zarówno po stronie dostawców systemów, jak ich użytkowników. W wielu wypadkach niewielka ilość czasu na dostosowanie się do nowej rzeczywistości spowodowała trudności w obsłudze systemów służących komunikowaniu się z uczniami oraz prawidłowej organizacji pracy, która ewoluowała wraz z biegiem czasu.

Podstawowe zasady ochrony i przetwarzania danych osobowych

O ile nikogo nie powinno dziwić stosowanie się do zasad ochrony i przetwarzania danych osobowych na terenie placówki, o tyle przełożenie ich na pracę zdalną spotkało się z różnym przyjęciem.

Prowadzenie nauczania zdalnego w ramach domowego środowiska prywatnego, często w otoczeniu rodzin, zaufanych osób, wydaje się być w pełni bezpieczne. I jakkolwiek ciężko podważać zaufanie, którym darzymy naszych bliskich, tak niezachowanie pewnych podstawowych zasad może prowadzić do naruszeń ochrony danych spowodowanych przypadkowo i nieumyślnie. Skutki takich incydentów pozostają jak najbardziej realne.

O zagrożeniach i ryzyku ich wystąpienia w dalszej części, teraz natomiast przypomnimy podstawowe zasady przetwarzania i ochrony danych osobowych, jakie należy stosować w ramach nauczania zdalnego i pracy zdalnej.

Polityka kluczy

Chodzi tu nie tyle o zapewnienie szafy zamykanej na klucz, w której przechowywane będą dokumenty, szczególnie że w dużej mierze występują one w wersji elektronicznej. „Kluczem” jest tu zapewnienie, aby wszelkie dane jakie znajdą się w domu pozostały zabezpieczone w taki sposób, aby uniemożliwić dostęp do nich osób nieuprawnionych, do których zaliczyć należy domowników. Jeżeli istnieje możliwość skorzystania z jakiegoś zamykanego miejsca, rekomendowane jest zastosowanie takiego zabezpieczenia. Oczywiście w każdym domu zastosowanie

tej zasady wyglądać będzie inaczej. Najważniejsze, to zachować niezbędne minimum dla zabezpieczenia danych osobowych w sposób, w jaki chronimy własne mienie.

Polityka czystego biurka

Tak jak w przypadku polityki kluczy, tak i w tym przypadku najistotniejsze jest zapewnienie nadzoru nad danymi osobowymi, zarówno przed dostępem do nich osób nieuprawnionych, jak zagubieniem lub zniszczeniem.

Pomimo oczywistości takiego postępowania, stara anegdotyczna wymówka, że „pies zjadł zadanie domowe" przeżywał swój renesans, jednak tym razem po stronie niektórych nauczycieli. Podstawą prawidłowego przetwarzania danych w warunkach pracy zdalnej jest wyodrębnienie pewnego miejsca przeznaczonego wyłącznie do pracy w taki sposób, by nic nie zostało zagubione lub zniszczone, np. podczas obiadu lub zabawy dziecka.

Polityka czystego ekranu

Wreszcie najważniejsze. Ochrona danych przetwarzanych w sposób elektroniczny. Ta część nauczania zdalnego dominuje zdecydowanie nad innymi, jeżeli chodzi o liczbę zagrożeń z nią związanych. Przede wszystkim pamiętać należy, aby używać haseł, nie zapisywać ich na kartkach, jak również w systemach i przeglądarkach, a okresowo zmieniać. Ma to szczególne znaczenie w przypadku, gdy z jednego komputera korzysta więcej domowników, np. dzieci, aby wykonać własne zadania przesłane przez nauczyciela. Po zakończeniu pracy w systemie, w dzienniku elektronicznym, poczcie e-mail lub innym, należy się każdorazowo wylogować.

Zalecane jest stosowanie programów antywirusowych, przy czym należy mieć na względzie, że niektóre z darmowych oprogramowań zbierają dane dotyczące aktywności w sieci, wykorzystując je następnie w celach marketingowych lub przekazując je swoim partnerom.

Szczególnie w przypadku stosowania nowych systemów, z których działaniem nie jest się jeszcze w pełni zaznajomionym, uważać należy na podejrzane linki. W przypadkach wątpliwych należy zawsze upewnić się, czy pochodzi on z odpowiedniego źródła lub po prostu nie otwierać jego zawartości.

Korzystanie ze sprzętu prywatnego wiąże się z kolei z odpowiedzialnością za zapisane na nim pliki, tak więc konieczne jest bieżące ich kontrolowanie, choćby przez wydzielenie odrębnego folderu na przesyłane przez uczniów prace.

Wynoszenie dokumentacji

Naturalną konsekwencją przeniesienia pracy do domu jest potrzeba posiadania przy sobie niezbędnych dokumentów. To zaś wiąże się z koniecznością dopasowania odpowiedniego modelu wynoszenia dokumentacji, aby klarowne były zasady udzielania do tego uprawnień i określania jakie dokumenty podlegają wyniesieniu przez kogo. Ponadto, szczególnie w przypadku większej ilości dokumentów, należy zadbać o bezpieczeństwo w ich transporcie, aby nie uległy one zagubieniu lub zniszczeniu.

Kanały komunikacji i zagrożenia ochrony danych w zdalnym nauczaniu

Poza wskazanymi już wcześniej zagrożeniami, wspomnieć należy przede wszystkim o zagrożeniach wynikających z korzystania z wszelkiego rodzaju komunikatorów i systemów informatycznych, przy pomocy których nauczyciele kontaktują się z uczniami, prowadzą lekcje, a także przesyłane są zadania i prace.

Często spotykanymi incydentami były włamania na zajęcia prowadzone przy wykorzystaniu systemów komunikacji na odległość. Niektóre z takich „wizyt" wynikały z przekazywania linków dostępu przez uczniów osobom do tego nieuprawnionym. Nie brakowało jednak również incydentów wynikających z luk w zabezpieczeniach systemów.

Aby zapobiec takim sytuacjom należy zapewnić blokowanie dostępu do systemów hasłami, a także edukować uczniów, aby nie przekazywali oni nawet dla żartu danych dostępowych.

Ponadto, wprawdzie administrator powinien zapewnić wszelkie narzędzia potrzebne do prowadzenia zdalnego nauczania, to często – choćby z potrzeby szybkiego działania – umożliwione zostało korzystanie z prywatnych systemów i komunikatorów. Korzystanie z nich rodzi wiele problemów z zakresu ochrony danych osobowych, jak również może naruszać warunki udzielonych licencji.

Analiza ryzyka

Wprowadzanie nowych systemów do korzystania w ramach nauczania zdalnego stanowi jeden z przykładów sytuacji, która wymaga przeprowadzenia analizy ryzyka. Jak wspomniano na początku, analiza ryzyka ma na celu zidentyfikowanie zagrożeń oraz ocenę ryzyka ich wystąpienia, w gdy to będzie konieczne wdrożeniu odpowiednich środków ochrony, mających na celu zminimalizowanie tego ryzyka lub wręcz jego wyeliminowanie.

W przywołanym przykładzie należy wziąć pod uwagę zagrożenia takie jak możliwość nieuprawnionego dostępu, utrata danych, trudności z obsługą systemu, zależność od sieci Internet, możliwość nieuprawnionej modyfikacji danych, itp.

W zależności od oceny administratora, co do możliwości wystąpienia tych zagrożeń, dostosować należy system ochrony danych poprzez wdrożenie nowych środków. W wielu wypadkach za wystarczające będzie można uznać odpowiednie przeszkolenie użytkowników systemu, zainstalowanie oprogramowań antywirusowych czy też ustawienie odpowiednio silnego hasła dostępu.

Za przeprowadzenie analizy ryzyka odpowiedzialny jest administrator, tym niemniej powinien on korzystać z wiedzy i doświadczenia pozostałych osób działających w organizacji.

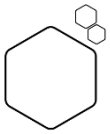
Zgłaszanie incydentów

Wszelkie sytuacje stanowiące lub mogące stanowić zagrożenie dla ochrony danych osobowych należy niezwłocznie zgłaszać administratorowi, a konkretnie wyznaczonej do tego w ramach organizacji osoby. Każde takie zdarzenie powinno podlegać ocenie, czy doszło do naruszenia, a jeżeli tak, to jakiej jest ono wagi.

Przypomnieć należy o obowiązku zgłoszenia Prezesowi Urzędu Ochrony Danych Osobowych naruszenia, którego waga jest wyższa niż „niska" zgodnie z przyjętą przez administratora metodologią

oceny naruszeń. Na przeprowadzenie czynności związanych z naruszeniem, w tym z dokonaniem zgłoszenia, administrator ma 72 godziny.

Informowanie o zdarzeniach stanowiących incydenty ochrony danych osobowych (a więc niekoniecznie naruszenie, jednakże są to sytuacje, gdy nie jest to jeszcze przesądzone) powinno odbywać się w ramach przyjętej przez administratora procedury.



Mity ochrony danych osobowych w placówkach oświatowych

Od początku stosowania RODO narosło wokół niego wiele mitów, wynikających z nieprawidłowego zrozumienia ustalonych w nim zasad. Absurdy nie ominęły również placówek oświatowych. Poniżej rozprawiamy się z kilkoma z nich.

Wywoływanie uczniów

Jednym z mitów, który znalazł swoje miejsce nie tylko w przychodniach lekarskich, to wywoływanie uczniów bez wykorzystania ich imion oraz nazwisk. W wielu placówkach wprowadzono porozumiewanie się z uczniami przy pomocy nadanych im pseudonimów lub inicjałów. W taki sam sposób mieli również podpisywać swoje sprawdziany. Jest to oczywiście nieprawidłowe postępowanie, ponieważ szkoła ma prawo używać danych osobowych uczniów, jak również rozwiązania te stanowią fikcję, że uczniowie nie znają się wzajemnie. Dlatego, z punktu widzenia ochrony danych osobowych, jakkolwiek można zwracać się do uczniów przy pomocy pseudonimów czy tez numerów z dziennika, to nie ma takiego obowiązku.

Odpowiedzialność szkoły za zdjęcia

Kolejnym mitem jest przeświadczenie o tym, że szkoła odpowiada za zdjęcia wykonane przez rodziców i inne osoby uczestniczące w wydarzeniach organizowanych przez szkołę. Należy rozprawić się z tym mitem i jednoznacznie powiedzieć, że szkoła jest administratorem danych zawartych na zdjęciach w sytuacji, gdy sama decyduje o celach i sposobach przetwarzania danych w tym zakresie. Z tego względu zawierane są umowy powierzenia z fotografami, którzy wykonują pamiątkowe zdjęcia klasowe.

Należy również wspomnieć, że RODO nie znajduje zastosowania do przetwarzania danych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. Za takie natomiast należałoby uznać wykonanie pamiątkowych fotografii swojego dziecka grającego jedną z ról w szkolnym spektaklu.

Zakaz publikowania wyników rekrutacji

Jak już wcześniej wspomniano, publikacja wyników rekrutacji do placówki oświatowej podlega przepisom ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe i stanowi obowiązek prawny ciążący na administratorze (a więc opiera się na przesłance przetwarzania z art. 6 ust. 1 lit. c RODO).

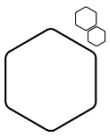
Należy jednak powtórzyć, że zakres danych jakie mogą podlegać publikacji został jasno określony przepisami Prawa oświatowego i nie powinien być on rozszerzany. To samo dotyczy sposobów publikacji list kandydatów.

Zakaz przetwarzania danych bez zgody ucznia

Temat ten również został już poruszony wcześniej, tym niemniej należy powtórzyć, że – co do zasady – szkoła nie potrzebuje zgody ucznia na przetwarzanie danych osobowych. Jest tak dlatego, że działając w ramach wykonywania swoich obowiązków, szkoła przetwarza dane przede wszystkim na podstawie obowiązku prawnego (art. 6 ust. 1 lit. c RODO) lub interesu publicznego (art. 6 ust. 1 lit. e RODO). Wyjątkami są sytuacje niemieszczące się w tych podstawach, takie jak publikowanie fotografii zawierającej wizerunek ucznia. W takich sytuacjach może być wymagana jego zgoda lub zgoda wyrażona przez rodziców lub opiekunów prawnych

Zakaz podpisywania prac uczniów

Była już mowa o podpisywaniu prac uczniów stanowiących sprawdziany, teraz natomiast mowa o pracach wieszanych na korytarzach, gazetkach lub w ramach konkursów i wyróżnień z tym związanych. Zgodnie z poradnikiem utworzonym przez Urząd Ochrony Danych Osobowych i Ministerstwo Edukacji Narodowej, działanie takie jest dozwolone i opiera się na postawie interesu publicznego, tj. podstawy przetwarzania z art. 6 ust. 1 lit. e RODO.

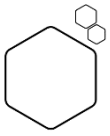


Przetwarzanie danych osobowych w celach oświatowych

W sierpniu 2018 r. wydany został opracowany przez Urząd Ochrony Danych Osobowych i Ministerstwo Edukacji Narodowej poradnik skierowany do placówek oświatowych zatytułowany: „Ochrona danych osobowych w szkołach i placówkach oświatowych”. Poruszył on zagadnienia związane z ochroną danych w placówkach oświatowych, w szczególności szkołach. Szczególnie istotne z punktu widzenia podstaw przetwarzania danych okazały się wskazówki dotyczące przetwarzania danych osobowych w celach oświatowych.

Zgodnie z poradnikiem, przetwarzanie danych w celach oświatowych, w tym określonych w ustawie z dnia 14 grudnia 2016 r. – Prawo oświatowe, opiera się na podstawie interesu publicznego, a więc na postawie art. 6 ust. 1 lit. e RODO.

Jako działania podejmowane w ramach realizowania celów oświatowych zostały uznane publikowanie osiągnięć, wyróżnianie i nagradzanie uczniów, a także organizowanie akademii, przedstawień i innych wydarzeń, które mają miejsce w ciągu roku szkolnego.



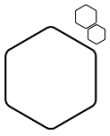
Organizacja wycieczek szkolnych

Konieczność przetwarzania danych osobowych w celu zorganizowania wycieczki szkolnej nie powinna budzić wątpliwości. Do załatwienia jest wiele spraw, jak choćby związane z ubezpieczeniem uczniów, zapewnieniem transportu, noclegów i opieki.

Należy w tym miejscu zwrócić uwagę, że w przypadku, gdy rodzice pełnią funkcję opiekunów, podlegają oni zasadom organizacyjnym administratora, w związku z czym powinni zostać upoważnieni do przetwarzania danych oraz złożyć stosowne oświadczenia, zgodnie z przyjętą przez administratora procedurą w tym zakresie.

Warto też poruszyć temat odrębnych administratorów jakimi są hotele, które same decydują o celach i sposobach przetwarzania danych, w związku z czym dane uczniów – o ile w ogóle są przekazywane – podlegać będą udostępnieniu. Oznacza to, że nie będzie zawierana z hotelem umowa powierzenia przetwarzania danych osobowych.

Nieco inaczej będzie wyglądała sytuacja w przypadku zakładów ubezpieczeń, w którym to przypadku praktyka wygląda dwojako. Niektóre z zakładów wymagają zawarcia umowy powierzenia przetwarzania danych osobowych, inne natomiast pozyskują dane na podstawie udostępnienia, co zależy od podejścia organizacyjnego tych podmiotów.



Podsumowanie

Ochrona danych osobowych w placówkach oświatowych to zagadnienie bardzo szerokie, bo niemal w każdym z obszarów działalności placówek przetwarzane są dane uczniów, rodziców lub opiekunów prawnych i innych osób, z którymi styczność mają na co dzień. Wyzwanie zapewnienia bezpieczeństwa

danych osobowych uczniów to z jednej strony obowiązek czysto prawny, z drugiej natomiast wielka odpowiedzialność za podopiecznych. Warto pamiętać, że dane osobowe posiadają wymierną wartość, dlatego należy je chronić tak samo jak własne „skarby” czy własne sekrety.

Jest to szczególnie ważne względem dzieci, które często nie są świadome ilości danych osobowych, które udostępniając codziennie przy wykorzystaniu aplikacji w swoich smartfonach. Budowanie świadomości tego czym są dane osobowe, jakie czyhają na nie zagrożenia i jak je chronić, powinno stanowić jeden ze wspomnianych wyżej celów oświatowych. Edukowanie prowadzone w tym duchu od podstaw wspomaga dojrzały rozwój życia, w tym również cyfrowego, każdego ucznia.