

Ochrona danych osobowych w jednostkach oświatowych



Podstawy prawne regulujące ochronę danych osobowych w polskim systemie prawnym to:

- 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 (zwane również ogólnym rozporządzeniem o ochronie danych lub RODO).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

- Administrator Danych Osobowych, którego osobą reprezentującą jest Dyrektor jednostki, zobowiązany jest do zapoznania pracowników z regulacjami prawnymi dotyczącymi ochrony danych osobowych. Szkolenie ma na celu poinformowanie pracowników bezpośrednio związanych z przetwarzaniem danych osobowych o obowiązujących zasadach ochrony danych.

Definicja danych osobowych

- „dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4 RODO).

- RODO ma na celu ujednolicenie przepisów o ochronie danych osobowych, więc wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich Unii Europejskiej.
- RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową.
- Stosowane jest od 25 maja 2018 r.

Podział danych osobowych

- Dane osobowe dzielimy na:
 - dane osobowe zwykłe, czyli np. imię i nazwisko, adres zameldowania, adres zamieszkania, PESEL, seria i numer dowodu osobistego.
 - dane osobowe szczególnych kategorii, czyli np. pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Zabronione jest przetwarzanie danych osobowych szczególnych kategorii, jednak w przypadku wyrażonej zgody osoby, której dane dotyczą lub w momencie, gdy przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora czy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą zakaz ten nie ma zastosowania.

- Danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności lub gdy ich ustalenie wymagałoby nadmiernych kosztów, czasu i działań.

- „przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

- „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
- Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych odbywało się zgodnie z RODO.

- Dane osobowe muszą być:
 - a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
 - b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
 - c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja zbieranych danych osobowych – nie zbieramy niepotrzebnych danych osobowych”).
 - d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
 - e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
 - f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. (art.5 ust. 1 RODO).

Administrator jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie (art. 5 ust. 2 RODO).

Podstawy przetwarzania danych

- Dane osobowe można przetwarzać w momencie, kiedy:

- 1) osoba, której dane dotyczą wyrazi na to zgodę.
- 2) dane są niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
- 3) są konieczne do realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.
- 4) są niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
- 5) są niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza prawa i wolności osoby, której dane dotyczą.

Zgoda na przetwarzanie danych

- Zgoda osoby, której dane dotyczą oznacza - dobrowolne, konkretne, świadome i jednoznaczne oświadczenie woli, które osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdza, przyzwalając na przetwarzanie jej danych osobowych.
- **Zgodę można wycofać w każdym momencie (art. 7 RODO)**

Ochrona danych dzieci

- Szczególnej ochrony wymagają dzieci, gdyż mogą być one mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z ochroną danych osobowych.

Publikacja danych i wizerunku

- Potrzebna jest zgoda na upublicznianie wizerunku.
- Bez zgody można publikować imiona i nazwiska oraz zdjęcia laureatów konkursów, **gdy publikacja została przewidziana w regulaminie konkursu.**
- Można publikować tzw. „dane służbowe”, czyli imię i nazwisko, stanowisko, służbowy telefon i e-mail.
- Zgoda nie jest wymagana w przypadku zdjęć zbiorowych, gdzie jedna osoba stanowi jedynie szczegół całości (np. z uroczystości, wycieczki).

Bezpieczeństwo i zabezpieczenia danych

- Pracownik jest zobowiązany zachować poufność przetwarzanych danych oraz sposobów ich zabezpieczenia.
- Dane można wykorzystywać wyłącznie do celów, dla których zostały udostępnione.
- Dokumenty powinny być przechowywane w taki sposób, aby osoba nieuprawniona nie miała do nich dostępu.
- Nośniki informacji (papierowe i elektroniczne) należy zabezpieczyć przed dostępem osób nieuprawnionych.
- Dokumenty nieaktualne, błędnie wydrukowane lub wydrukowane w nadmiernej ilości należy trwale zniszczyć.
- Nie wyrzucamy dokumentów do kosza przed upewnieniem się, że dane osobowe nie zostały z nich wcześniej usunięte.

- Monitory należy usytuować w taki sposób, aby osoby nieupoważnione nie miały wglądu do danych.
- Oprogramowanie instaluje tylko i wyłącznie administrator systemu informatycznego, nigdy nie należy robić tego samodzielnie.
- Nie należy udostępniać innym haseł i identyfikatorów.
- Po zakończeniu pracy należy zawsze wylogować się z systemów, z których korzystaliśmy.
- Adres konta pocztowego – służbowy – używamy tylko do celów służbowych. Informacji służbowych nie wysyłamy pocztą prywatną.
- Zasada blokowania lub wygaszania ekranu i „czystego biurka” powinna być codziennie stosowaną „dobrą praktyką”.
- Nośniki informacji zabezpieczamy hasłem.
- Poza miejscem pracy, szczególnie w miejscach publicznych, należy unikać rozmów dotyczących informacji służbowych podlegających ochronie.

Postępowanie w przypadku naruszenia bezpieczeństwa danych osobowych

- W momencie pozyskania informacji o potencjalnym naruszeniu, wycieku danych lub wystąpienia incydentu związanego z danymi osobowymi uczniów lub pracowników należy niezwłocznie poinformować bezpośredniego przełożonego, Dyrektora jednostki oraz Inspektora Ochrony Danych. Wątpliwości powinny budzić np. widoczne próby włamania, próby wyłudzenia danych, zagubienie nośników, na których przetwarzane są dane osobowe.

Dziękuję za uwagę.