Ochrona danych osobowych w szkołach i placówkach oświatowych

SZKOLENIE WSTĘPNE

Podstawa prawna

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.U.UE.L.2016.119.1) **RODO**

Szkoła, reprezentowana przez swojego dyrektora, przetwarza dane na podstawie przepisów odnoszących się ściśle do funkcjonowania oświaty, Przede wszystkim są to:

- Prawo oświatowe,
- Karta Nauczyciela,
- Ustawa o systemie oświaty,
- Ustawa o systemie informacji oświatowej,
- Ustawa o finansowaniu zadań oświatowych,
- Rozporządzenia do ww. ustaw.

DEFINICJE

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, genetyczna, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

CHRONIMY RÓWNIEŻ DANE KONTRHENTÓW – OSÓB FIZYCZNYCH KTÓRE PROWADZĄ DZIAŁALNOŚĆ GOSPODARCZĄ!

Przetwarzanie

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.

Przetwarzanie danych osobowych

RODO stosuje się do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz w przypadku przetwarzania w sposób inny niż zautomatyzowany, np. w formie tradycyjnej – papierowej, jeżeli dane stanowią lub mogą stanowić część zbioru. Przykładami takich zbiorów danych w szkole są: dzienniki lekcyjne,

- lista zatrudnionych pracowników,
- księga ewidencji dzieci,
- księga uczniów,
- arkusze ocen ucznia,

które są prowadzone zarówno w systemie informatycznym, jak i przetwarzane tradycyjnie.

Dane osobowe dzielą się głównie na:

Dane tzw. Zwykłe – imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wizerunek, adres e-mail. itp.

Dane szczególnej kategorii – wymienione w art. 9 RODO ujawniające: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Dodatkowo wyróżnia się dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa.

Przetwarzanie danych szczególnej kategorii jest legalne TYLKO I WYŁACZNIE w przypadku wystąpienia podstaw art. 9 ust. 2 RODO. Dane te należy szczególnie chronić!

Administrator

Administratorem może być osoba fizyczna, osoba prawna, organ publiczny, jednostka organizacyjna i inne podmioty, które decydują o celach i sposobach przetwarzania danych.

Administratorem danych osobowych uczniów, ich rodziców, nauczycieli, pracowników szkoły jest ten, kto decyduje o celach i sposobach przetwarzania tych danych, czyli szkoła, którą reprezentuje dyrektor szkoły.

Podstawowe zasady przetwarzania danych osobowych

1. ZASADA ZGODNOŚCI Z PRAWEM, RZETELNOŚCI I PRZEJRZYSTOŚCI – przetwarzanie może być tylko dokonywane na podstawie obowiązujących przepisów, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą;

2. ZASADA OGRANICZENIA CELU– przetwarzamy dane, tylko gdy ma to prawnie uzasadniony cel

np. dane kontrahentów, aby wydać im towar, dane pracowników, aby realizować postanowienia umowy o pracę. Dodatkowo pobieramy dane nam niezbędne – np. nie będzie nam potrzebne nazwisko panieńskie matki kontrahenta lub zestaw przebytych chorób pracownika biurowego.

Podstawowe zasady przetwarzania danych osobowych c.d.

3. ZASADA MINIMALIZACJI DANYCH – zbieramy tylko takie dane, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

4. ZASADA PRAWIDŁOWOŚCI – zawsze staramy się posiadać AKTUALNE dane osobowe i cały czas monitorujemy ich aktualność;

5. ZASADA OGRANICZENIA PRZECHOWYWANIA – dane osobowe przetwarzamy tylko przez ten czas na jaki są nam potrzebne lub na taki okres jak wynika to z przepisów prawa;

Podstawowe zasady przetwarzania danych osobowych c.d.

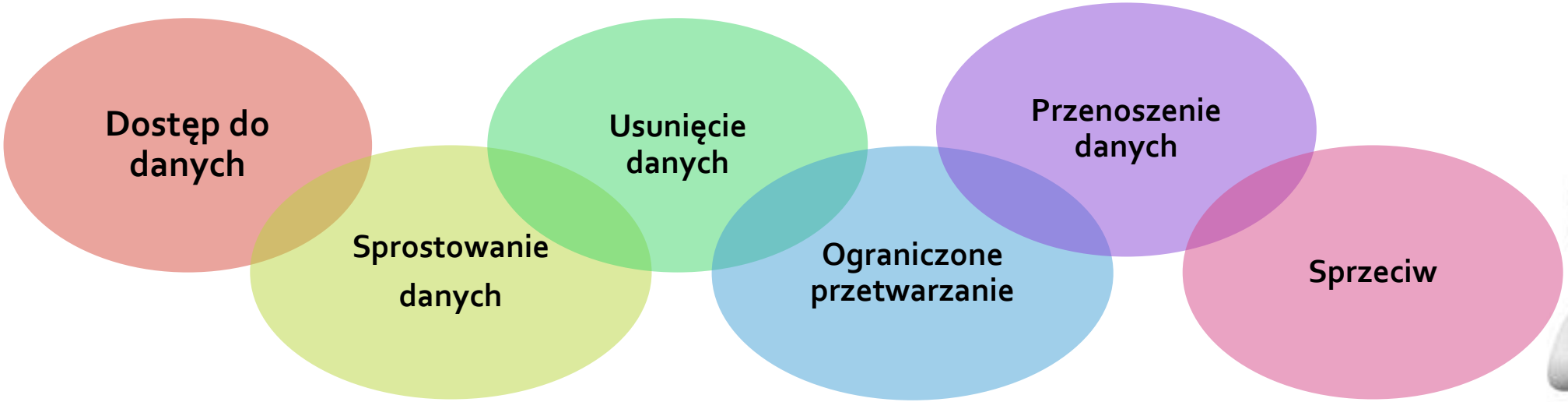
6. ZASADA ROZLICZALNOŚCI – trzeba tak pracować, aby było wiadomo kto dokonał jakich czynności w systemach – każdy korzysta ze swojego stanowiska, wskazanego komputera, swojego loginu, hasła, telefonu służbowego, aby można było zidentyfikować kto dopuścił się naruszenia i dlaczego oraz musimy umieć wykazać, że przestrzegamy wszystkich przyjętych procedur bezpieczeństwa.

7. ZASADA INTEGRALNOSCI I POUFNOŚCI – do danych mają dostęp tylko upoważnieni pracownicy i upoważnione osoby z zewnątrz, nikt kto nie jest upoważniony nie ma prawa dostępu do danych, które gromadzi pracodawca, robimy wszystko, aby danych nie utracić, czy bezpodstawnie nie modyfikować.

Szkoła lub placówka oświatowa zobowiązana jest do przestrzegania zasad ochrony danych osobowych, w tym m.in. do:

- Spełnienia względem osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO,
- Zabezpieczenia danych osobowych przez zastosowanie odpowiednich środków technicznych i organizacyjnych, tak aby dane te nie były udostępniane osobom nieupoważnionym oraz aby dane te były chronione przed zniszczeniem albo utratą (np. poprzez szyfrowanie danych i poufność),
- Respektowania prawa osób, których dane są przetwarzane, np. udzielanie informacji co do celów, sposobów, źródeł, zakresu przetwarzania danych osobowych, itd.
- Wyznaczenia Inspektora ochrony danych. Szkoła powinna opublikować dane inspektora ochrony danych i powiadomić o jego powołaniu organ nadzorczy, czyli Prezesa UODO. Stanowisko IOD ma samodzielny i niezależny charakter.

Prawa: ”Jana Kowalskiego” czyli każdego według RODO:



Niektóre z praw mogą być jednak **ograniczone.** Np. prawo do bycia zapomnianym – gdy istnieje podstawa prawna do przetwarzania danych, to wezwanie do usunięcia danych może być nieskuteczne.

PRZYKŁAD: były pracownik żąda, aby pracodawca usunął jego dane – pracodawca nie może tego uczynić, gdyż prawo zobowiązuje go do przechowywania teczek osobowych przez 50 lat od rozwiązania stosunku pracy.

Przetwarzanie danych osobowych zwykłych jest zgodne z prawem wyłącznie wtedy, gdy:

- Osoba, której dane dotyczą, wyraziła zgodę na ich przetwarzanie,
- Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub jest konieczne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
- Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
- Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
- przetwarzanie jest niezbędne do wykonywania zadania realizowanego w interesie publicznym,
- Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub prawa i wolności osoby, której dane dotyczą,

Każda z tych podstaw ma taką samą moc i wszystkie są sobie równie. Zgoda na przetwarzanie danych osobowych powinna być pobierana, gdy nie ma innych podstaw prawnych, ponieważ zgoda osoby może być zawsze cofnięta.

Zgoda na przetwarzanie danych osobowych

Jeżeli przetwarzanie danych odbywa się na podstawie zgody, szkoła lub placówka oświatowa musi być w stanie wykazać, że osoba, której dane dotyczą (lub w przypadku osób niepełnoletnich – jej opiekun prawny), wyraziła zgodę na przetwarzanie danych osobowych. Jeżeli oświadczenie zgody zawarte jest w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Naruszenia ochrony danych

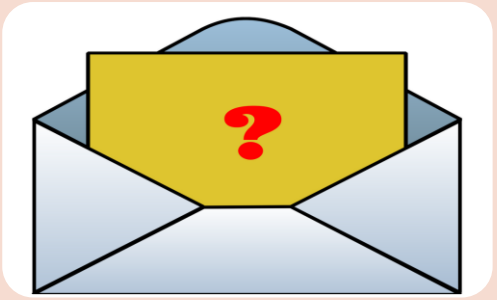
Żeby zaistniało naruszenie w zakresie ochrony danych powinny być spełnione łącznie trzy przesłanki:

1) Naruszenie dotyczy danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie,

2) Skutkiem naruszenia jest zniszczenie, utracenie, zmodyfikowania, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,

3) Naruszenie jest konsekwencją złamania zasad bezpieczeństwa danych.

Przykłady naruszeń



Przypadkowe wysłanie danych osobowych ucznia do niewłaściwego rodzica

Zgubienie lub kradzież nośnika zawierającego kopię danych osobowych

Pracownik szkoły przez pomyłkę zmienia nazwiska rodziców uczniów poprzez dopisanie litery „s” na końcu każdego z nich

Pracownik przypadkowo lub osoba nieupoważnione celowo usuwa dane z e-dziennika

Zgłoszenie naruszenia organowi nadzorczemu

Każdy pracownik ma obowiązek niezwłocznie zgłosić incydent czy naruszenie danych osobowych swojemu przełożonemu!

RODO wprowadza obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego, tj. do Urzędu Ochrony Danych Osobowych, w ciągu 72h.

To Administrator Danych decyduje o tym, czy zgłosi naruszenie, ponieważ nie każde naruszenie należy zgłaszać UODO tylko takie, które z określonym wysokim prawdopodobieństwem skutkowałoby ryzykiem naruszenia praw lub wolności osób fizycznych.

Dla prawidłowej reakcji na naruszenie, każdorazowo można wezwać do pomocy Inspektora Ochrony Danych.

DOBRE PRAKTYKI

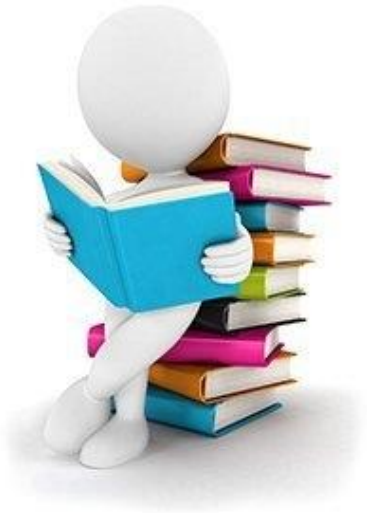
Czyli Co Mogę Zrobić, Żeby Zwiększyć Bezpieczeństwo Danych Osobowych

Dokumenty, które należy znać i bezwzględnie stosować:

Polityka bezpieczeństwa przetwarzania danych lub regulamin ochrony danych osobowych;

Instrukcja Zarządzania Systemem Informatycznym;

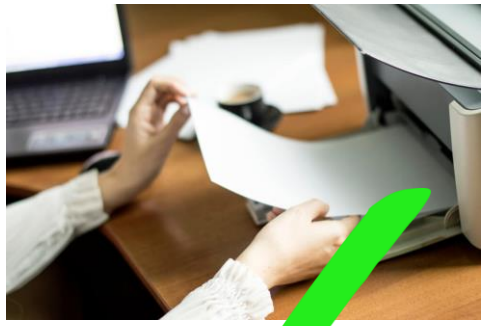
Inne dokumenty wewnętrzne chroniące dane osobowe, w tym np. regulamin pracy zdalnej, procedura postępowania z kluczami, regulamin monitoringu wizyjnego itp.

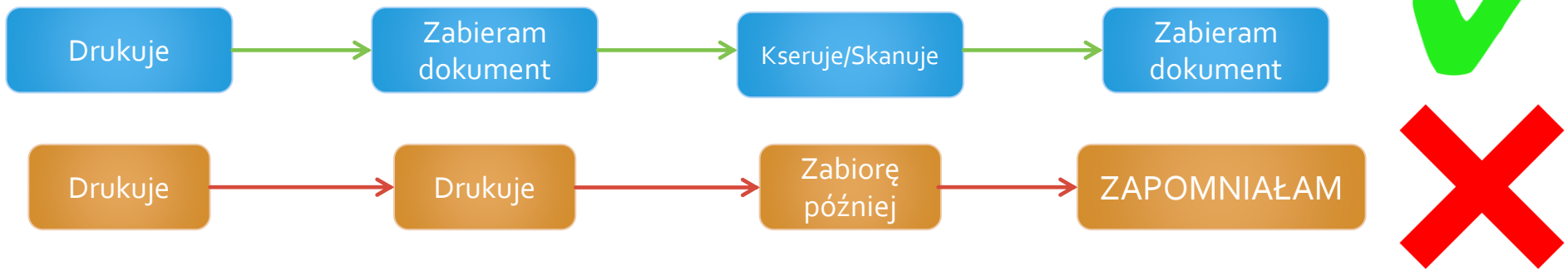


Polityka czystego druku

Drukarki, skanery, kserokopiarki należy traktować jako potencjalne źródło zagrożenia, dlatego:

- ✓Nie pozostawiaj wydruku bez nadzoru na drukarce, ksero czy skanerze,
- ✓Nie rób tzw. brudnopisu z wydruku z danymi osobowymi,
- ✓Korzystać z urządzenia mogą tylko osoby upoważnione,
- ✓Zwróć szczególna uwagę na drukowanie na urządzeniach sieciowych!





Polityka czystego biurka

- ✓Nie umożliwiaj dostępu osobom nieupoważnionym do poufnych informacji na biurku, pieczątek, dysków itp.
- ✓Zawsze umieszczaj dokumenty i nośniki informacji co najmniej w szafach lub szufladach zamykanych na klucz.
- ✓Pamiętaj! Aby w momencie przyjmowania interesanta, Twoje biurko było czyste od dokumentów. Będzie to zabezpieczenie przed celowym lub nieumyślnym np. zabraniem dokumentów wraz z tymi, po które przyszedł interesariusz.
- ✓Na koniec dnia pracy chowaj wszystkie dokumenty i nośniki danych do zamykanych szafek.

Bezpieczne niszczenie

Dokumenty zawierające dane osobowe i informacje poufne zawsze niszcz za pomocą niszczarek biurowych!

Polityka czystego ekranu

- ✓Nie umożliwiaj dostępu osobom nieupoważnionym do informacji wyświetlanych na ekranie Twojego komputera służbowego
- ✓Ustawienie monitora nie może pozwalać na dostęp do informacji osobom do tego nieupoważnionych – sprawdź czy Twoje biurko stoi w odpowiedniej pozycji!
- ✓Blokuj dostęp do urządzenia kiedy opuszczasz miejsce pracy,
- ✓Nie zostawiaj interesanta samego w pomieszczeniu, w którym przetwarzane są dane osobowe,

Polityka haseł

- ✓Zachowaj hasło w tajemnicy
- ✓Nie zapisuj haseł ani loginu i nie pozostawiaj ich w miejscu ogólnie dostępnym np. nie przyklejaj kartki z zapisanym hasłem na monitorze komputera!
- ✓Nie używaj tych samych haseł w pracy i w domu – czyli hasło, którym logujesz się na facebook'a nie może służyć do logowania się do poczty służbowej lub innego oprogramowania

Nośniki informacji, urządzenia mobilne i kopie zapasowe

- ✓Jeżeli tworzysz kopie zapasową, na nośniku typu np. pendrive pamiętaj, aby zablokować dostęp do urządzenia, folderu itp. hasłem,
- ✓Zawsze przechowuj je w bezpiecznym miejscu, najlepiej w zamykanych na klucz szafkach lub szafach,
- ✓Zaleca się jednak ograniczanie korzystania z nośników wymiennych,
- ✓Jeżeli jesteś użytkownikiem urządzenia mobilnego, dbaj o jego bezpieczeństwo, zapewnij bezpieczny transport i przechowanie – nigdy nie udostępniaj go osobom nieupoważnionym!
- ✓Jeżeli przesyłasz pliki zawierające dane osobowe lub informacje poufne za pomocą poczty elektronicznej, używaj do tego bezpiecznych oprogramowań, zabezpiecz je hasłem, które podasz adresatowi w inny sposób – sprawdzając jego tożsamość,
- ✓Zawsze sprawdzaj poprawność adresu korespondencyjnego (tradycyjnego lub e-mail)

Dziękuje!

Anita Sienicka

Inspektor Ochrony Danych

55 625 68 08

iod@ecuw.elblag.eu