



EDU ODO Agencja Rozwoju Dydaktycznego  
Ul. Zamiejska 14, 44-270 Rybnik  
NIP: 6423203506, biuro@eduodo.pl

## **Materiał informacyjny dla osób przetwarzających dane osobowe w jednostkach oświatowych**

*W związku z aktualizacjami przepisów o ochronie danych osobowych i ich interpretacji, niniejszym materiałem pragniemy przybliżyć i odświeżyć Państwu zasady dotyczące przetwarzania danych. Niniejszy spis najważniejszych reguł dotyczących przetwarzania danych, wypełniania obowiązków czy zabezpieczania danych powinien rozwiązać większość Państwa wątpliwości.*

***Zapraszamy do lektury,***

***Zespół EDU ODO Agencji Rozwoju Dydaktycznego***

### **1. Co to są dane osobowe?**

Według przepisów dane osobowe „**oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej** „. Starając się przybliżyć znaczenie powyższego pojęcia, posłużymy się dość popularnym imieniem i nazwiskiem „Jan Kowalski”. W momencie podania samego nazwiska Pana Kowalskiego nie jesteśmy w stanie zidentyfikować osoby fizycznej, której te dane dotyczą, ponieważ jest to popularne nazwisko. W tej sytuacji nie mówimy o danych osobowych. Niemniej jednak dodając do nazwiska jakiegokolwiek dodatkowe dane osobowe, np. PESEL, adres, czy informacje, że jest to uczeń Państwa szkoły znacząco zawężamy krąg poszukiwań Jasia Kowalskiego, co znacząco zwiększa szanse na identyfikację konkretnego dziecka.

Często popełnianym błędem, a nawet nieświadomym naruszeniem przepisów o ochronie danych osobowych jest nieuważna wymiana informacji. Załóżmy, że dwóch nauczycieli w trakcie przerwy rozmawia na korytarzu szkoły o uczniu. W trakcie rozmowy pada nazwisko ucznia, a rozmowa dotyczy jego słabych ocen, problemów psychologiczno-pedagogicznych, czy zachowania. Jeżeli taką rozmowę usłyszy osoba postronna, np. rodzic jednego z uczniów, możemy mówić o nieświadomym

naruszeniu przepisów. Gdyby ta sama rozmowa miała miejsce np. w galerii handlowej – nikt nie będzie w stanie zidentyfikować osoby fizycznej. Jednak, jeżeli to samo zdanie zostanie wypowiedziane na korytarzu szkolnym istnieje duże prawdopodobieństwo, że rodzic słyszący rozmowę zidentyfikuje „Kowalskiego” jako ucznia szkoły, dzięki czemu będzie w stanie zidentyfikować konkretną osobę fizyczną. Oczywiście przepisy o ochronie danych osobowych nie zabraniają wymiany informacji pomiędzy nauczycielami, wręcz tego nakazują dla zachowania odpowiedniego rozwoju dziecka w szkole i spełnienia wymogów ustawowych m. in. prawa oświatowego, lecz powinniśmy mieć na uwadze fakt, że nasze rozmowy na temat dzieci powinny być poufne i prowadzone w taki sposób, aby nie dopuszczać do nieświadomych wycieków danych osobowych.

## 2. Jak dzielimy dane osobowe?

Dane osobowe przetwarzane w szkole dzielimy na dwie kategorie. Są to dane zwykłe oraz dane wrażliwe, zwane inaczej danymi szczególnymi. W przepisach dotyczących ochrony danych osobowych nie znajdziemy powyższych pojęć, ale samo rozróżnienie danych, które przetwarzamy nasuwa na myśl takie pojęcia.

Zgodnie z RODO dane wrażliwe to zamknięty katalog danych, których przetwarzania zabrania się bez uzasadnionego celu. Na dane wrażliwe składają się wszelkie dane **„ujawniające 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, której dane przetwarzamy”**. Dane te powinny być też chronione w sposób szczególny, np. poprzez stałe przechowywanie ich w szafach zamykanych na klucz.

Wszelkie pozostałe dane osobowe przetwarzane w szkole, określane są mianem danych zwykłych. Jako dane zwykłe są uznawane między innymi takie informacje jak imię, nazwisko, adres, PESEL, telefon czy adres mailowy.

## 3. Czym jest przetwarzanie danych osobowych?

**„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”**. Sama definicja przetwarzania danych osobowych zaczerpnięta z RODO wyraźnie wskazuje, że nie ma znaczenia, jakie operacje wykonujemy na danych osobowych, gdyż każda z nich oznacza ich przetwarzanie i obowiązek należytej ochrony.

Codzienną praktyką w szkołach jest sytuacja, w której nauczyciel zgodnie z wydanym upoważnieniem do przetwarzania danych osobowych „zabiera pracę do domu”. Wielu nauczycieli zabiera do domu kartkówki w celu sprawdzenia i wpisania ocen do dziennika elektronicznego. Jest to oczywiście postępowanie zgodne z prawem i nie narusza w żaden sposób bezpieczeństwa danych osobowych przy zachowaniu odpowiedniej rozważliwości. Trzeba jednak pamiętać, że wpisując oceny w domu nie powinniśmy umożliwiać osobom postronnym (nawet mężowi lub żonie) wglądu w kartkówki lub dziennik elektroniczny osób postronnych, gdyż jest to osoba nieupoważniona do przetwarzania

danych osobowych, która zgodnie z obowiązującymi przepisami nie powinna mieć wglądu w te dane, tym bardziej, że wgląd w dane osobowe też jest ich przetwarzaniem o czym wspominaliśmy wcześniej. Takie postępowanie uznawane jest za wyciek danych osobowych, który powinien zostać zgłoszony niezwłocznie do Administratora Danych Osobowych.

#### 4. Jakie są zasady przetwarzania danych osobowych?

Przepisy o ochronie danych osobowych wyróżniają 6 podstawowych zasad, którymi powinniśmy się kierować przy przetwarzaniu danych osobowych. Poniżej wyjaśnienie znaczenia tych zasad:

- **Zgodność z prawem, rzetelność i przejrzystość** oznacza, że każde dane, które przetwarzamy, muszą być przetwarzane zgodnie z obowiązującą literą prawa, rzetelnie oraz w sposób jasny i zrozumiały dla osoby, której dane przetwarzamy,
- **Ograniczenie celu** oznacza, że dane osobowe powinny być zbierane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach, np. w celu przeprowadzenia procesu rekrutacji w szkole,
- **Minimalizacja danych**, czyli przetwarzanie powinno być adekwatne, stosowne i ograniczone do tego, co niezbędne dla celów, w których są one przetwarzane. Zasada ta mówi wprost „nie przetwarzaj, co nie potrzebne”, np. zbieranie informacji na temat miejsca pracy rodziców przy przyjęcia dziecka do świetlicy szkolnej, gdzie takie informacje nie powinny być zbierane.,
- **Prawidłowość** oznacza, że dane osobowe powinny być prawidłowe i w razie potrzeby uaktualnione. Dane nieprawidłowe w świetle ich przetwarzania najczęściej muszą być niezwłocznie usunięte,
- **Ograniczenie przechowywania** wskazuje, że dane nie powinny być przechowywane przez okres dłuższy, niż jest to niezbędne dla realizacji celów ustawowych lub celów, w których zostały one zebrane. Jednym z celów ustawowych może być np. obowiązek realizacji nauki szkolnej,
- **Integralność i poufność** to nic innego jak obowiązek przetwarzania danych w sposób zapewniający ich odpowiednie bezpieczeństwo, na które w głównej mierze składa się nasze świadome przetwarzanie i zabezpieczanie danych.

#### 5. Kim jest Administrator Danych Osobowych (ADO)?

**„Administratorem Danych Osobowych w świetle RODO jest osoba fizyczna, prawna, organ publiczny, jednostka lub inny podmiot, który ustala cele i sposoby przetwarzania danych osobowych.”** Aby łatwiej było nam zrozumieć pojęcie Administratora Danych Osobowych, zwróćmy uwagę na „organ publiczny lub jednostkę”. W myśl tego zapisu Administratorem będzie szkoła. Idąc dalej tym tropem zacznie się nasuwać jedno pytanie: „Ale jak to szkoła Administratorem, jeśli ADO ma ustalać cele i sposoby przetwarzania danych? Przecież szkoła nie może sama podjąć decyzji” I tu dochodzimy do momentu, w którym trzeba spojrzeć na „osobę fizyczną i prawną”, która ustala cele i sposoby przetwarzania. Tą osobą jest dyrektor szkoły, który jest osobą decydującą o celach i sposobach przetwarzania danych.

Należy też pamiętać, że przepisy o ochronie danych osobowych nakładają na każdą osobę upoważnioną do przetwarzania danych osobowych obowiązek ich należytej ochrony i przetwarzania na polecenie Administratora. Zakaz ujawniania danych osobowych statuuje nie tyle obowiązek przestrzegania tajemnicy danych, ile pewien rodzaj ogólnego obowiązku posłuszeństwa wobec

Administradora zobowiązanego do ochrony danych osobowych. Obowiązek ten byłby naruszony w każdym przypadku przetwarzania danych wykraczającym poza zakres obowiązków służbowych, nawet przy zachowaniu odpowiedniego bezpieczeństwa danych i ich poufności. W niedopełnieniu powyższego obowiązku przez pracownika, Administrator ma prawo upatrywać znamion ciężkiego naruszenia podstawowych obowiązków służbowych w rozumieniu Kodeksu Pracy, co może skutkować wyciągnięciem wobec pracownika odpowiednich konsekwencji, ze zwolnieniem dyscyplinarnym włącznie.

## **6. Kim jest Inspektor Ochrony Danych (IOD)?**

Inspektor Ochrony Danych to potocznie „prawa ręka” ADO. Inspektor jako osoba posiadająca pełnię władzy w związku z wykonywanymi zadaniami ma na celu przede wszystkim wspierać Administratora Danych Osobowych w wykonywanych obowiązkach związanych z ochroną danych osobowych. Do powołania IOD zobligowana jest każda jednostka publiczna, w tym także szkoła. Dodatkowo powołać IOD muszą podmioty prywatne, których główna działalność polega na regularnym i systematycznym monitorowaniu osób, których dane są przetwarzane lub jeśli przetwarzają dane wrażliwe na dużą skalę.

Inspektor wyznaczany jest na podstawie posiadanych kwalifikacji zawodowych, w szczególności fachowej wiedzy z zakresu prawa i praktyk w dziedzinie bezpieczeństwa informacji. Powinien on również posiadać odpowiednią wiedzę na temat procesów przetwarzania danych oraz zabezpieczeń stosowanych w szkole. Inspektorem może zostać jedynie osoba, która nie była wcześniej karana. Może być to osoba zatrudniona w szkole lub osoba wykonująca swoje zdania na podstawie umowy o świadczenie usług, czyli firma zewnętrzna.

## **7. Zgoda na przetwarzanie danych osobowych**

W momencie rozpoczęcia procesu przetwarzania danych osobowych poprzez ich zbieranie musimy zadbać o to, aby mieć podstawę do przetwarzania tych danych. Zgodę na przetwarzanie możemy uzyskać z dwóch źródeł.

Pierwszym z nich są przepisy inne niż ustawa o ochronie danych osobowych. W szkołach większość przypadków rozpoczęcia przetwarzania danych osobowych ma miejsce przy okazji procesu rekrutacyjnego. Prawo Oświatowe wyraźnie wskazuje jakie dane szkoła może zebrać przy naborze. W tej sytuacji nawet jeżeli rodzic składając wniosek o przyjęcie dziecka do szkoły powie „Wniosek składam, ale nie wrażam zgody na przetwarzanie danych osobowych mojego dziecka” to dla szkoły ważniejsza jest realizacja zadań narzuconych przez Prawo Oświatowe niż ustawa o ochronie danych osobowych. Musimy pamiętać, że dla szkoły realizacja wymogów ustaw takich jak ustawa o systemie oświaty, prawo oświatowe, karta nauczyciela, czy ustawa o systemie informacji oświatowej jest ważniejsza, niż RODO, które jest rozporządzeniem niższej rangi od powyższych ustaw.

W przypadku rekrutacji wiele wątpliwości budzi też zbieranie danych kontaktowych rodziców i zgodność z RODO. Zwróćmy uwagę na art. 150 Prawa Oświatowego, który wyraźnie mówi, że rodzice mają obowiązek podać numer telefonu lub adres mailowy we wniosku o przyjęcie dziecka do szkoły. Przykładów przetwarzania danych osobowych na mocy przepisów innych niż przepisy o ochronie danych osobowych jest wiele. Może to być umowa podpisywana pomiędzy rodzicem, a szkołą np. na żywienie dzieci, umowa o pracę, czy zbieranie danych osobowych, nawet tych wrażliwych, takich jak:

informacje o stanie zdrowia, czy oświadczenia majątkowe w sytuacji przyjmowania wniosku do zakładowego funduszu świadczeń socjalnych.

Zgoda na przetwarzanie danych osobowych wyrażona przez osobę, której dane dotyczą jest stosowana rzadko i do małej ilości danych osobowych, lecz jest elementem bardzo ważnym, aby zachować pełną zgodność z przepisami. Taką zgodę zbieramy wyłącznie w momencie, gdy niezbędne do przetwarzania nam są dane, których przetwarzania nie wymaga żaden przepis. W świetle RODO zgoda musi być wyrażona w formie jednoznacznego okazania woli, co oznacza, że musi być ona w pełni dobrowolna, a szkoła nie może wywierać żadnego nacisku na jej wyrażenie. Dodatkowo powinna być ona zebrana w tradycyjnej formie papierowej, aby ADO mógł zachować zasadę rozliczalności. Przykładem zachowania tej zasady może być sytuacja, gdy rodzic wyraża zgodę na przetwarzanie wizerunku swojego dziecka, a w następnym roku szkolnym składa do szkoły skargę na bezpodstawnie opublikowane zdjęcie dziecka na stronie szkoły, ponieważ nie pamięta, że taką zgodę wyraził. Administrator mając podpisaną zgodę na przetwarzanie może wykazać, że nie naruszył przepisów o ochronie danych publikując zdjęcie dziecka.

W szkole tego typu zgoda najczęściej zbierana jest na przetwarzanie wizerunku dziecka, który w myśl RODO również traktowany jest jak dane osobowe, ponieważ umożliwia identyfikację osoby fizycznej. Przepisy nie określają jasno w jakiej formie i na jakie cele zgoda powinna być zebrana, dlatego zaleca się, aby była ona przygotowana w sposób ogólny na cały zakres danych przetwarzanych dodatkowo. Dlatego zbierając zgodę na przetwarzanie danych osobowych i wizerunku ucznia, jesteśmy w stanie od razu zebrać ją na wszelkiego rodzaju wycieczki, konkursy szkolne, czy publikację zdjęć ze szkolnych wydarzeń.

Równie ważne jest zebranie zgody na przetwarzanie danych osobowych uczestników konkursu. Niezależnie, czy jest to konkurs organizowany przez Państwa szkołę, czy konkurs organizuje inna szkoła zawsze trzeba pamiętać, aby każdy jego uczestnik posiadał aktualną zgodę na przetwarzanie danych osobowych. Jedynie jako organizator konkursu mają Państwo obowiązek zebrania zgód od każdego uczestnika. Najprostszym rozwiązaniem jest dołączenie jej do formularza zgłoszeniowego.

Należy pamiętać, że istnieją sytuacje, w których możemy bezpiecznie przetwarzać dane osobowe oraz wizerunek nie posiadając pisemnej zgody na ich przetwarzanie. Jedną z nich są festyny organizowane przez szkołę, np. z okazji dnia dziecka. W takich wydarzeniach bardzo często biorą udział również rodzice dzieci, ich dziadkowie, czy rodzeństwo. W praktyce niemożliwością byłoby zebranie od wszystkich osób pisemnej zgody na przetwarzanie wizerunku. Prawo w tej sytuacji dopuszcza stworzenie regulaminu imprezy niemasowej, w którym zawrzemy informację, że uczestnictwo w imprezie jest jednoznaczne z wyrażeniem zgody na przetwarzanie wizerunku. Najważniejsze jednak będzie odpowiednie oznakowanie miejsca imprezy informacją, że regulamin uczestnictwa jest dostępny w siedzibie organizatora tak, aby osoba chętna mogła się z nim zapoznać. Poza tym z pomocą przychodzi nam art. 81 ustawy o prawie autorskim i innych prawach pokrewnych, który mówi nam, że **„zezwoienia nie wymaga rozpowszechnianie wizerunku osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza”**. W tej sytuacji nawet przy braku regulaminu nie trzeba się obawiać publikacji zdjęć grupowych.

Do przepisów o ochronie danych trzeba podejść z zachowaniem zasady racjonalności. W momencie wejścia w życie przepisów wielu dyrektorów niepotrzebnie zabraniało nauczycielom czytania ocen na forum klasy, wyróżniania uczniów za szczególne osiągnięcia przed klasą, czy też na apelu szkolnym. Takie postępowanie nie narusza RODO, a z pewnością pozwala na motywowanie uczniów do lepszych osiągnięć w nauce.

## 8. Umowy powierzenia

Umowa powierzenia przetwarzania danych osobowych jest umową, która musi zostać każdorazowo podpisana w przypadku powierzenia danych osobowych do podmiotów zewnętrznych. Ma ona na celu zobowiązać podmiot, któremu dane przekazujemy do ich odpowiedniego zabezpieczenia, przetwarzania zgodnie z prawem i tylko w celu podanym przez Administratora.

Przykładem klasycznego powierzenia danych osobowych szkoły do zewnętrznego podmiotu jest zatrudnienie fotografa do wykonania grupowych lub indywidualnych zdjęć uczniów. Jak już wcześniej zaznaczyliśmy, wizerunek to też dane osobowe. W tej sytuacji przekazując dane osobowe fotografowi, który wykonuje zdjęcia na polecenie ADO, mówimy o powierzeniu. Fotograf po wykonaniu zdjęć musi zabrać je do swojej firmy, poddać obróbce graficznej oraz wywołać. Pliki ze zdjęciami bardzo często przechowywane są przez dłuższy okres w razie, gdyby któryś z rodziców chciał zakupić większą ilość odbitek. Tak jak wspominaliśmy wcześniej, proces utrwalania (wizerunku uczniów) i przechowywania jest przetwarzaniem danych osobowych, a każde dane osobowe są objęte ochroną.

Podobnie sytuacja wygląda przy organizacji wycieczek szkolnych. Niekiedy zdarza się, że nauczyciel korzystając z usług biura podróży musi podać jedynie liczbę uczniów i w takiej sytuacji umowa powierzenia nie jest wymagana, gdyż nie przekazuje on żadnych danych uczniów. Jeżeli jednak biuro wymaga przekazania listy dzieci, które będą brały udział w wycieczce, niezbędne jest zawarcie umowy powierzenia jeszcze przed przekazaniem pełnej listy przedstawicielowi biura.

Z tego też powodu należy pamiętać, że jeżeli nauczyciel we własnym zakresie organizuje uczniom sesję fotograficzną, wycieczkę, czy jakiegokolwiek inne wydarzenie, które wiąże się z powierzeniem danych osobowych dzieci poza szkołą, to przed podpisaniem umowy konieczne trzeba zawiadomić ADO lub IOD o takim zamiarze, aby mogli oni przygotować odpowiednią umowę powierzenia przetwarzania danych osobowych.

## 9. Obowiązek informacyjny

Zgoda na przetwarzanie danych osobowych nie jest jedynym obowiązkiem, który należy spełnić wobec osoby, której dane rozpoczynamy przetwarzać. Istotny jest również obowiązek informacyjny, zwany inaczej klauzulą informacyjną. Czym jest klauzula w świetle RODO? Otóż, obowiązek informacyjny, to obowiązek przekazania osobie, której dane dotyczą informacji na temat przetwarzania jej danych osobowych. Odpowiedzmy sobie na dwa podstawowe pytania: Co obowiązek informacyjny powinien zawierać? Jak ten obowiązek spełnić?

W pierwszej kolejności powiemy jakie dane należy podać, aby obowiązek informacyjny został spełniony. Do wiadomości osoby podajemy:

- Pełne dane Administratora Danych Osobowych – Niezbędne podanie jest pełnej nazwy szkoły wraz z adresem, np. Szkoła Podstawowa nr 1 w Warszawie, ul. Miła 1, 00-193 Warszawa
- Pełne dane Inspektora Ochrony Danych wraz z danymi kontaktowymi, np. Adam Nowak, e-mail: [adamnowak@o2.pl](mailto:adamnowak@o2.pl)
- Cele przetwarzania danych osobowych oraz podstawę prawną, np. Celem zbierania Państwa danych osobowych jest przeprowadzenie postępowania rekrutacyjnego na podstawie ustawy Prawo Oświatowe itp.

- Dane odbiorców danych, gdy ma to zastosowanie – Chodzi przede wszystkim o przekazywanie danych osobowych do państwa trzeciego (poza Europejski Obszar Gospodarczy), organizacji międzynarodowej itd.
- Okres, przez który dane będą przechowywane, a jeżeli nie jest możliwe ustalenie tego okresu, to kryteria jego ustalania, np. dokumentacja dotycząca wycieczek szkolnych musi być przechowywana przez 5 lat, licząc od rozpoczęcia roku kalendarzowego, następującego po roku, w którym dane zostały zebrane
- Informacje i prawie dostępu do własnych danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania
- Informacja o prawie do wniesienia skargi do organu nadzorczego, czyli Urzędu Ochrony Danych Osobowych
- Informacja o prawie do wycofania zgody na przetwarzanie w dowolnym momencie
- Informacja o tym, czy podanie danych jest wymogiem ustawowym, czy jest w pełni dobrowolne

Jak ten obowiązek spełnić? Przepisy jasno nie określają sposobu informowania osób, których dane przetwarzamy. Wiemy jedynie, że informacja ma zostać przekazana w prostej, łatwo dostępnej i zrozumiałej dla każdego formie. Spełnienie obowiązku zaleca się w formie pisemnej dla wygody pracowników szkoły. Rodzic, którego zapoznajemy z klauzulą informacyjną nie musi podpisywać oświadczenia, że został zapoznany.

Obowiązek informacyjny powinien być umieszczony na stronie internetowej szkoły, przy każdym wejściu do szkoły, w gabinetach pedagoga, logopedy, sekretariacie, czy we wnioskach, np. wniosku o przyjęcie dziecka do szkoły lub we wniosku do zakładowego funduszu świadczeń socjalnych.

Postępowanie Urzędu Ochrony Danych Osobowych wyraźnie wskazuje jak ważne dla zapewnienia zgodności z przepisami jest spełnianie obowiązku informacyjnego. Pierwsza kara administracyjna nałożona przez Prezesa Urzędu Ochrony Danych Osobowych od czasu wejścia w życie RODO została nałożona właśnie za niespełnianie obowiązku informacyjnego wobec osób, których dane były przetwarzane, dlatego bardzo ważne jest, aby obowiązek był każdorazowo spełniany wobec każdej osoby, której dane rozpoczynamy przetwarzać.

## **10. Wycofanie zgody na przetwarzanie danych osobowych i wniosek o ich usunięcie**

Każda osoba, której dane osobowe przetwarzamy ma prawo do złożenia na ręce ADO oświadczenia o wycofaniu zgody na przetwarzanie swoich danych osobowych. Musimy pamiętać, że wycofanie zgody na przetwarzanie danych osobowych musi być równie łatwe, co jej wyrażenie. Nie możemy w żadnym stopniu utrudniać osobie, której dane przetwarzamy wycofania zgody, gdyż jest to niezgodne z przepisami, a Prezes Urzędu Ochrony Danych Osobowych już nałożył karę administracyjną na podmiot, który wręcz uniemożliwiał jej wycofanie.

Osoba nie może wycofać zgody na przetwarzanie danych osobowych, jeżeli szkoła przetwarza dane, których przetwarzanie jest niezbędne dla realizacji zadań ustawowych szkoły. Wycofanie zgody najczęściej może mieć miejsce w przypadku przetwarzania wizerunku dzieci. Jednakże samo wpłynięcie takiego oświadczenia nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej wycofaniem. Osoba, której dane dotyczą jest o tym informowana zanim wyrazi zgodę. Dlatego, jeżeli do szkoły wpłynie takie oświadczenie, Administrator nie musi

usuwać wszystkich danych przetwarzanych na podstawie zgody, a jedynie zaprzestać ich dalszego przetwarzania od dnia wpłynięcia oświadczenia.

Usunięcie danych osobowych może być konieczne dopiero w momencie, gdy osoba, której dane przetwarzamy złoży wniosek o ich usunięcie. Zgodnie z wprowadzonym przez RODO „prawem do bycia zapomnianym”, Administrator w momencie otrzymania wniosku o usunięcie danych osobowych jest zmuszony do usunięcia wszystkich danych osoby składającej wniosek, z wyjątkiem tych danych, które przetwarzamy na podstawie przepisów prawa. Spróbujmy przybliżyć sprawę w praktyce.

W pierwszej sytuacji, rodzic przy przyjęciu dziecka do szkoły wyraził zgodę na przetwarzanie danych i wizerunku dziecka. Wyrażenie zgody miało miejsce we wrześniu 2016 roku. W ciągu prawie 4 lat nauki dziecka, dyrektor szkoły opublikował na stronie internetowej kilkanaście jego zdjęć. W marcu 2020 roku do dyrektora wpłynął wniosek rodzica o usunięcie danych osobowych jego dziecka. Co w takiej sytuacji powinien zrobić dyrektor szkoły? Podstawową czynnością jest dokonanie przeglądu przetwarzanych danych osobowych dziecka. Z pewnością częściowo wniosek musi zostać odrzucony, ponieważ szkoła nie może usunąć danych osobowych dziecka np. z dziennika, arkuszy ocen czy książki uczniów, gdyż do ich przetwarzania obligują przepisy prawa. Niemniej jednak zdjęcia opublikowane na stronie szkoły w celach promocyjnych przetwarzane są na mocy zgody i dyrektor powinien usunąć wszystkie zdjęcia, na których znajduje się to dziecko.

Teraz spróbujmy cofnąć się kilkanaście lat wstecz. Wyobraźmy sobie sytuację, w której szkołę odwiedza absolwent uczęszczający do niej w latach 1993-2001. On również decyduje się na złożenie wniosku o usunięcie danych osobowych ze szkoły, lecz we wniosku wskazuje, że zależy mu jedynie na usunięciu jego zdjęć ze strony internetowej. W tej sytuacji ważne jest to, aby pamiętać na jakiej podstawie poprzedni Dyrektor szkoły przetwarzał dane osobowe absolwentów w okresie wykonywania zdjęć. Pierwsza ustawa o ochronie danych osobowych została wprowadzona w życie 29 sierpnia 1997 r. (aktualnie jest to przepis wygaszony) i jest to data graniczna, od której wymagane było posiadanie zgody na przetwarzanie danych osobowych. Przed wprowadzeniem tej ustawy dane mogły być przetwarzane do woli bez żadnych obostrzeń prawnych. Aby zachować zgodność z przepisami, dyrektor szkoły w momencie wpłynięcia takiego wniosku powinien usunąć ze strony wszystkie zdjęcia publikowane po 29 sierpnia 1997 r., a zdjęcia publikowane wcześniej mogą na stronie pozostać zgodnie z zasadą, która mówi, że **„prawo nie działa wstecz”**.

Najważniejsze jest, aby pamiętać, że każdy wniosek o usunięcie danych osobowych, czy oświadczenie o wycofaniu zgody na ich przetwarzanie powinien być złożony na piśmie. Nawet jeżeli osoba chce złożyć takie oświadczenie ustnie, powinniśmy poprosić o przesłanie informacji mailowo lub przekazanie jej w postaci pisemnej dla zachowania zasady rozliczalności, o której wspominaliśmy wcześniej.

## **11. Wniosek o udostępnienie danych osobowych**

Wniosek o udostępnienie danych osobowych tak samo jak wnioski o usunięcie danych czy oświadczenia o wycofaniu zgody powinny być dostarczone pisemnie. Niejednokrotnie o udostępnienie danych osobowych zwracają się rodzice, policja lub sąd. Każdy taki wniosek powinien być podparty podstawą prawną umożliwiającą żądanie udostępnienia danych osobowych. Po otrzymaniu takiego wniosku, Administrator musi przygotować dane osobowe do udostępnienia. Po ich udostępnieniu warto dodać adnotację na wniosku, że dane osobowe zostały przekazane, a sam fakt ten należy niezwłocznie odnotować w rejestrze udostępnień danych, podając dane osoby, której zostały przekazane dane osobowe.



W szkole najczęściej występują dwa rodzaje wniosków o udostępnienie danych osobowych. Pierwszym z nich są wnioski z innych instytucji publicznych, takich jak policja, sąd, prokuratura, komornik, miasto czy pomoc społeczna. Z reguły są to wnioski podparte konkretną podstawą prawną, na które musimy udzielić stosownej odpowiedzi – czyli udostępnić dane osobowe.

Skupmy się przede wszystkim na częstych wnioskach rodziców o udostępnienie nagrania z monitoringu. Posiadając w szkole monitoring musimy być świadomi jego działania. W momencie, gdy na terenie szkoły dojdzie do bójki między dziećmi lub wypadku, rodzic ma prawo zgłosić się do Administratora o wgląd lub udostępnienie kopii nagrania ze zdarzenia. Należy pamiętać, że nie możemy tego rodzicom umożliwić! Wgląd w monitoring na którym przetwarzany jest wizerunek dzieci – czyli dane osobowe – jest przetwarzaniem, a udostępnienie danych osobowych osobie postronnej stanowi poważne naruszenie przepisów o ochronie danych osobowych. Jak w takiej sytuacji postąpić? Rozwiązań jest kilka. W pierwszej kolejności Administrator lub inna osoba upoważniona do przeglądania nagrań z monitoringu powinna samodzielnie zweryfikować, czy szkolne kamery zarejestrowały zdarzenie. Jeśli tak, kolejnym krokiem jaki należy podjąć jest poinformowanie rodzica, że takie nagranie mamy. Następnie nagranie należy zabezpieczyć, czyli zgrać na inny nośnik oraz przechować w miejscu do tego wyznaczonym, zgodnie z funkcjonującym regulaminem monitoringu. Jeżeli szkoła będzie chciała udostępnić rodzicowi kopię nagrania, może to zrobić dopiero po wykonaniu **pseudonimizacji** wizerunku pozostałych osób znajdujących się na nagraniu, co oznacza, że wizerunek pozostałych osób powinien zostać przetworzony w taki sposób, aby uniemożliwić ich rozpoznanie.

## 12. Kategorie naruszeń przepisów o ochronie danych osobowych

W świetle przepisów o ochronie danych osobowych wyróżniamy trzy kategorie naruszeń:

- **Naruszenie poufności,**
- **Naruszenie dostępności,**
- **Naruszenie integralności.**

**Naruszenie poufności** może mieć miejsce np. w sytuacji, gdy nauczyciel chce poinformować rodzica, że jego dziecko zachowuje się niewłaściwie i prosi o stawienie się osobiście na rozmowę u wychowawcy. W momencie, gdy nauczyciel wysyła wiadomość prywatną, może się zdarzyć, że zaznaczy zły kontakt i wiadomość trafi do rodzica innego dziecka. W takiej sytuacji mówimy o naruszeniu poufności danych osobowych.

**Naruszenie dostępności** występuje najczęściej w przypadku zagubienia danych osobowych. Najprostszym przykładem naruszenia dostępności może być sytuacja, w której nauczyciel zabiera do domu kartkówki w celu ich sprawdzenia. Opuszczając szkołę wkładamy kartkówki do samochodu, a w domu w trakcie sprawdzania okazuje się, że brakuje np. kartkówek klasy piątej. Wywnioskować można, że przez nieuwagę nauczyciela kartkówki wypadły z samochodu.

**Naruszenie integralności** może wystąpić w momencie, gdy jeden z rodziców, np. Pan Kawowski zgłosi się do wychowawcy, aby poinformować go o zmianie numeru telefonu. Wychowawca, aby zachować aktualność danych osobowych decyduje się na zmianę numeru telefonu Pana Kawowskiego w dzienniku elektronicznym, a przypadkowo nowy numer zostaje wpisany przy nazwisku innego rodzica, Pana Kowalskiego. W takiej sytuacji mówimy o naruszeniu integralności.

W momencie wystąpienia jakiegokolwiek naruszenia, nauczyciel powinien natychmiast poinformować o zaistniałym fakcie Administratora Danych Osobowych lub Inspektora Danych Osobowych. Muszą oni podjąć odpowiednie kroki w celu wyjaśnienia sytuacji, sporządzenia protokołu i wysłania ewentualnego zgłoszenia do Urzędu Ochrony Danych Osobowych. Niezwłoczny kontakt z ADO lub IOD jest konieczny, ponieważ przeprowadzenie wszystkich czynności musi nastąpić bez zbędnej zwłoki, lecz nie później niż w ciągu 72 godzin od wystąpienia naruszenia.

### **13. Rodzaje naruszeń przepisów o ochronie danych osobowych**

Każde z wyżej wymienionych naruszeń nie musi być zabiegiem świadomym. Większość naruszeń występuje przez nasze codzienne nawyki i często nieświadomie. Przeprowadziliśmy kilkaset audytów bezpieczeństwa, dlatego pragniemy podzielić się z Państwem naszym doświadczeniem i pokazać jakie błędy najczęściej popełniają pracownicy jednostek oświatowych oraz powiedzieć co należy robić, aby nie dochodziło do naruszeń i wycieków.

- Podstawowym błędem jest pozostawienie pomieszczeń otwartych. Nie ma znaczenia, czy opuszczamy je na minutę, godzinę, czy na kilka sekund. Pomieszczenia, w których przetwarzane są dane osobowe muszą być każdorazowo zamykane na klucz. Wystarczy chwila nieuwagi, by osoba postronna wykorzystała to przeciwko nam, wchodząc do pomieszczenia. Trzeba również pamiętać, że nie możemy pozostawiać osób postronnych samych w pomieszczeniach. Jeżeli dochodzi do sytuacji, w której np. nauczyciel musi opuścić rodzica w trakcie rozmowy, nauczyciel musi poprosić rodzica, aby ten opuścił pomieszczenie razem z nim.
- Nie tylko pomieszczenia pozostają otwarte. Zagadnienie dotyczy również szafek oraz szuflad biurkowych, które również po zakończeniu pracy należy zamykać, a klucze schować tak, aby były one niedostępne dla osób postronnych. Kluczy do pomieszczeń również nie powinniśmy pozostawiać w zamkach drzwi, nawet od strony wewnętrznej. Nauczyciel pobierający klucz jest za niego odpowiedzialny, więc powinien pozostawiać cały czas pod jego opieką.
- Bardzo często popełnianym błędem jest zabałaganione biurko i porozrzucane na nim dokumenty. Osoby wchodzące do pomieszczenia, w którym pracujemy mają możliwość wglądu w dokumenty leżące na naszym stanowisku pracy. Tak jak wcześniej wspomnieliśmy, nawet sam wgląd w dane osobowe jest ich przetwarzaniem, a dopuszczenie do przetwarzania osoby nieupoważnionej stanowi naruszenie przepisów o ochronie danych osobowych. Konieczna jest większa dbałość o „czyste biurko”, na którym powinny znajdować się tylko te dokumenty, które są nam niezbędne do bieżącej pracy. Aby zachować również te dane w poufności warto wyrobić sobie nawyk odwracania dokumentów „czystą stroną do góry” w taki sposób, aby uniemożliwić odczytanie danych.
- Sekretarze szkoły często zapisują swoje hasła do programów, czy numery telefonów rodziców na kartkach i wywieszają dla wygody na tablicy korkowej obok stanowiska pracy. Na tablicy nie powinny być wywieszane żadne dane osobowe. Teoretycznie hasła nie powinny być zapisywane w ogóle, lecz niejednokrotnie praktyka pokazuje, że sekretarz szkoły ma dostęp do kilku programów, a w każdym inne hasło przez co nie jest w stanie ich wszystkich zapamiętać. Jeżeli zachodzi konieczność ich zapisania, należy pamiętać, że muszą być one zabezpieczone w taki sposób, aby uniemożliwić do nich dostęp innym pracownikom czy osobom postronnym. Przy okazji hasel warto również zaznaczyć, że złą praktyką jest zapisywanie przez nauczycieli hasła do dziennika elektronicznego w przeglądarkach. Takie postępowanie może doprowadzić do nieuprawnionego dostępu do dziennika elektronicznego, np. przez ucznia.

- Komputery służące do przetwarzania danych osobowych w szkole powinny być zabezpieczone odpowiednim hasłem do systemu, wygaszaczem ekranu i blokadą dostępu przy dłuższej nieobecności pracownika. Pracownicy szkoły powinni również zadbać o to, aby monitory były ustawione tak, by uniemożliwić wgląd w nie osobom postronnym.
- Zatrzymując się przy komputerach, trzeba zaznaczyć, że uczniowie nie mogą mieć dostępu do tej samej sieci WI-FI, z której korzystają pracownicy szkoły. Korzystając z tej samej sieci uczeń posiadający szeroką wiedzę informatyczną jest w stanie wkraść się do komputera nauczyciela i uzyskać dostęp do dziennika elektronicznego.
- Kończąc tematykę zabezpieczeń trzeba zwrócić uwagę na przesyłanie danych osobowych drogą mailową. W momencie, gdy przez e-mail mamy zamiar przestać dokumenty zawierające dane wrażliwe, np. kopię orzeczenia z poradni psychologiczno-pedagogicznej, czy protokół rady pedagogicznej, niezbędne jest zaszyfrowanie dokumentu. Hasła do odszyfrowania nie powinniśmy wysyłać drugą wiadomością mailową, a przekazać ustnie bądź telefonicznie osobie, do której wysyłamy dokumenty.
- Kolejnym często popełnianym błędem jest wywieszanie na tablicy korkowej zwolnień lekarskich uczniów w gabinecie w-f. Zwolnienie lekarskie traktowane jest jako informacja o stanie zdrowia ucznia, przez co mówimy o danych wrażliwych. Te z kolei muszą być przechowywane stale w szafie zamykanej na klucz tak samo jak opinie poradni psychologiczno-pedagogicznej w gabinecie psychologa.

## 14. Organy nadzorcze

Kolejną kwestią konieczną do poruszenia są organy nadzorcze. Krótko wymienimy najważniejsze z nich, aby mieli Państwo świadomość ich istnienia. Są to:

- **Urząd Ochrony Danych Osobowych** – wcześniej GIODO (Generalny Inspektor Ochrony Danych Osobowych). Od 25 maja 2018 r. zmieniona została nazwa Urzędu. Jest to organ odpowiedzialny za nadzór nad przestrzeganiem przepisów o ochronie danych osobowych w Polsce.
- **Europejska Rada Ochrony Danych Osobowych** – jest niezależnym organem, mającym za zadanie zapewnienie spójnego stosowania RODO w Unii Europejskiej. Jest organem centralnym UE w kwestiach nowego prawa o ochronie danych osobowych.

## 15. Dokumentacja

Przepisy o ochronie danych osobowych narzucają na Administratorów obowiązek prowadzenia podstawowej dokumentacji określającej zasady przetwarzania danych osobowych na terenie szkoły. Jednak mając na uwadze fakt, że prowadzeniem dokumentacji powinien zająć się ADO wraz z Inspektorem, pracownicy szkoły powinni przede wszystkim zostać zaznajomieni z takim dokumentem jak **Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych**. Jest to dokument określający tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku, gdy stwierdzono naruszenie przepisów o ochronie danych osobowych. Każdy pracownik szkoły powinien poświęcić czas na zapoznanie się z dokumentem, aby mieć pełną świadomość jakie kroki należy podjąć w momencie, gdy dojdzie do naruszenia przepisów o ochronie danych osobowych.

## 16. Sankcje

Na zakończenie wątek, który nie należy do przyjemnych. Jest nim temat dotyczący stosowanych kar za naruszenie przepisów o ochronie danych osobowych, czy niewypełnienie obowiązków przez nie nakładanych.

Do czasu wejścia w życie RODO, maksymalna kara wynosiła od 10 tys. do 50 tys. złotych. Aktualnie kary są dużo wyższe i wynoszą:

- **Jednostki publiczne** – kara do 100.000 zł,
- **Podmioty prywatne** – kary do 4 % rocznego obrotu światowego za poprzedni rok rozliczeniowy lub do 20.000.000 euro z zachowaniem kwoty wyższej.

Dlaczego kary są takie wysokie? Nie mamy w tym kierunku oficjalnego stanowiska władz, lecz przypuszczamy, że mają one na celu wystraszyć podmioty, które bardzo chętnie dopuszczają się naruszeń przepisów w celu osiągnięcia korzyści majątkowych. Przykładem tego mogą być częste telefony z zaproszeniami na prezentację różnych sprzętów gospodarstwa domowego i możliwość odbioru darmowej nagrody. Takie firmy najczęściej są w posiadaniu informacji na temat właściciela telefonu, jego wieku, czy miejsca zamieszkania, a same dane osobowe pochodzą z handlu lub naszej nieuwagi. Niskie kary pieniężne, które regulowała nasza stara ustawa o ochronie danych osobowych, nie pozwalały na skuteczne odstraszenie potężnych przedsiębiorstw od łamania przepisów.

Do tej pory na dwa podmioty publiczne została nałożona kara finansowa.

Gmina Aleksandrów Kujawski otrzymała karę w wysokości 40.000 zł za brak zawartej umowy powierzenia przetwarzania danych osobowych na prowadzenie Biuletynu Informacji Publicznej przez podmiot zewnętrzny. Dodatkowo jak wskazuje Prezes Urzędu Ochrony Danych Osobowych brak współpracy w trakcie trwania kontroli i zbagatelizowanie zaleceń pokontrolnych przyczyniło się do ustalenia wysokości nałożonej kary administracyjnej.

W marcu 2020 roku zakończyło się postępowanie wobec Szkoły w Gdańsku na którą nałożono karę w wysokości 20.000 zł za zbieranie danych biometrycznych uczniów (odcisków palca) korzystających ze stołówki szkolnej. Dane te były zbierane w celu weryfikacji płatności za obiady. Uczeń przed odebraniem posiłku skanował odcisk palca, aby potwierdzić swoją tożsamość w systemie szkoły.

## 17. Najważniejsze daty

Poruszając się wśród przepisów dotyczących ochrony danych osobowych, w tym wszelkich zgód, klauzul czy wniosków warto znać cztery najważniejsze daty, jakimi operujemy mówiąc o przepisach o ochronie danych osobowych:

- **29 sierpnia 1997 r.** – data wprowadzenia pierwszej ustawy o ochronie danych osobowych. Ustawa ta została wygaszona w momencie wejścia w życie RODO,
- **27 kwietnia 2016 r.** – jest to data wprowadzenia RODO Europejskim Dziennikiem Ustaw. Od tego dnia kraje członkowskie Unii Europejskiej dostały ponad 2 letni okres przejściowy na przygotowanie zmian w wewnętrznych przepisach na wejście w życie RODO,
- **10 maja 2018 r.** – dzień wprowadzenia w Polsce nowej ustawy o ochronie danych osobowych,
- **25 maja 2018 r.** – data wygaszenia starej ustawy o ochronie danych osobowych z 1997 r., data wejścia w życie nowej ustawy o ochronie danych osobowych z 2018 r. i jednocześnie data wejścia w życie RODO.

## 18. Dodatkowe informacje

W związku z wejściem w życie ustawy z o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO, wprowadzone zostały zmiany w ustawie o zakładowym funduszu świadczeń socjalnych. Zmiany określają, że beneficjent funduszu udostępnia dane osobowe pracodawcy w celu przyznania ulgowej usługi i świadczenia oraz dopłaty z funduszu i ustalenia ich wysokości. Udostępnienie danych następuje w formie oświadczenia. Zaznaczono również, że Dyrektor szkoły może żądać udokumentowania danych osobowych, ale wyłączenie w zakresie niezbędnym do ich potwierdzenia. Samo potwierdzenie może odbywać się na podstawie oświadczeń i zaświadczeń o sytuacji życiowej (w tym zdrowotnej), rodzinnej i materialnej osoby uprawnionej do korzystania z funduszu.

Osoby dopuszczone do przetwarzania danych osobowych w ZFŚS powinny zostać dodatkowo upoważnione pisemnie, do przetwarzania danych osobowych zawartych w funduszu.

Zmiany dotyczą również okresu przechowywania danych osobowych. Administrator nie może ich przetwarzać dłużej niż przez okres niezbędny do przyznania świadczenia z funduszu socjalnego lub przez okres niezbędny do dochodzenia praw lub roszczeń. Nowym obowiązkiem Administratora jest dokonywanie przeglądu danych osobowych nie rzadziej niż raz w roku kalendarzowym w celu ustalenia niezbędności dalszego przechowywania danych. Jeśli ADO uzna, że część danych jest zbędna do realizacji określonych celów – natychmiast je usuwa.

Kolejną istotną zmianą dotyczącą ustawy z o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO jest zmiana w Kodeksie Pracy. Przede wszystkim zmienia się zakres danych zbieranych przez Administratora od kandydata i pracownika. Od osoby ubierającej o zatrudnienie żąda się podania imienia i nazwiska, daty urodzenia, danych kontaktowych, wykształcenia, kwalifikacji zawodowych i przebiegu dotychczasowego zatrudnienia. Jednak w tym przypadku też są pewne obostrzenia. Dane kontaktowe wskazuje kandydat dobrowolnie, poprzez podanie telefonu, adresu e-mail lub obu jednocześnie. Podanie wykształcenia, kwalifikacji zawodowych oraz przebiegu dotychczasowego zatrudnienia jest obowiązkiem tylko wtedy, gdy informacje te są niezbędne do wykonywania pracy na określonym stanowisku. Dodatkowo pracodawca nie ma prawa żądać od kandydata jego adresu zamieszkania lub imion rodziców.

Od osoby zatrudnionej można żądać takich danych jak adres zamieszkania, PESEL lub numer dokumentu potwierdzającego tożsamość, jeżeli osoba nie posiada numeru PESEL, numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę do rąk własnych oraz inne dane osobowe pracownika, jego dzieci i członków najbliższej rodziny, jeżeli podanie takich danych jest konieczne, gdyż pracownik korzysta ze szczególnych uprawnień przewidzianych w prawie pracy.

Inne dane osobowe mogą być żądane przez pracodawcę, tylko gdy jest to niezbędne do spełnienia obowiązku wynikającego z przepisu prawa. Niezbędne w tej sytuacji jest zebranie pisemnej zgody pracownika lub kandydata do pracy na ich przetwarzanie.

Jeżeli Administrator prowadzi oficjalny proces rekrutacji warto ustalić odgórnie zakres danych jakie powinny znaleźć się w CV kandydata do pracy. Pozwoli to uniknąć zbierania zgody na przetwarzanie danych osobowych. Jeżeli jednak kandydat do pracy zamieści dodatkowe informacje na swój temat, niezbędne będzie dodanie klauzuli zgody. Dodatkowo warto zaznaczyć, że niezależnie od zakresu podanych danych osobowych w CV, jeżeli ADO nie prowadzi procesu rekrutacji, a osoba sama zgłasza

swoją kandydaturę, niezbędne jest to, aby w CV została zawarta zgoda na przetwarzanie oraz przechowywanie kandydatury do przyszłych rekrutacji.

Zmiany także są widoczne w monitoringu. Od dawna wiadomo, że Administrator musi poinformować pracowników o wprowadzeniu monitoringu, oznaczyć pomieszczenia i teren monitorowany w widoczny i czytelny sposób, a także przekazać pracownikom informacje o celu prowadzenia monitoringu. W związku ze zmianami zakazano jednak monitorowania pomieszczeń udostępnianych organizacjom związkowym, szatni, stołówek, palarni czy pomieszczeń sanitarnych.