Dariusz Skrzyński

RODO W SZKOLE I PRZEDSZKOLU

PRAKTYCZNY PRZEWODNIK WDRAŻANIA NOWYCH PRZEPISÓW KROK PO KROKU

Przewodnik

OŚWIATA
grupa wydawnicza

Autor: Dariusz Skrzyński
Wydawca: Julita Brodzińska
Redaktor: Monika Fidler
Korekta: zespół
Projekt graficzny okładki: Magdalena Huta
ISBN: 978-83-269-7347-5

Wiedza i Praktyka sp. z o.o.
ul. Łotewska 9a, 03-918 Warszawa
tel. 22 518 29 29, faks 22 617 60 10, e-mail: cok@wip.pl

NIP: 526-19-92-256 Numer KRS: 0000098264
Sąd Rejonowy dla m.st. Warszawy,
Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy.

Wysokość kapitału zakładowego: 200.000 zł.

RODO W SZKOLE I PRZEDSZKOLU

PRAKTYCZNY PRZEWODNIK WDRAŻANIA NOWYCH PRZEPISÓW KROK PO KROKU

Każda placówka oświatowa przetwarza dane osobowe, co oznacza, że musi odpowiednio przygotować się do nowych unijnych przepisów dotyczących ochrony danych osobowych, tj. rozporządzenia Parlamentu Europejskiego i Rady (UE) 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 (ogólne rozporządzenie o ochronie danych osobowych, w skrócie: RODO).

Do podstawowych obowiązków i odpowiedzialności dyrektora szkoły i przedszkola publicznego od 25 maja 2018 r., zgodnie z RODO, będzie w szczególności należało:

1) przetwarzanie danych osobowych zgodnie z podstawowymi zasadami określonymi w rozporządzeniu,
2) wykonywanie obowiązków wynikających z praw osób, których dotyczą dane osobowe,
3) zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych,
4) przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych zgodnie z zasadami określonymi w rozporządzeniu – jeżeli takie operacje administrator realizuje,
5) wyznaczenie inspektora ochrony danych – gdy jest do tego zobowiązany na podstawie art. 37 ust. 1 rozporządzenia.

CZĘŚĆ I – Akty prawne w ochronie danych

Od 25 maja 2018 r. każdy dyrektor, przy udziale inspektora ochrony danych, będzie zmuszony dookreślić kwestie związane z poszczególnymi procedurami, wymaganymi dokumentami czy zasadami postępowania przy przetwarzaniu danych.

3 akty prawne w ochronie danych

Do tej pory przepisy ochrony danych osobowych opierały się na ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922 ze zm.) – dalej: UODO. Wraz z wejściem w życie RODO hierarchia aktów prawnych się zmieni.

Od 25 maja 2018 r. zaczną obowiązywać bezpośrednio w placówkach oświatowych nowe przepisy unijne w sprawie ochrony danych osobowych – 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 (dalej: RODO).
Unijne rozporządzenie nie wymaga podjęcia dodatkowych czynności przez polskie władze – obowiązuje bezpośrednio, dlatego wszystkie podmioty – w tym także przedszkola – muszą dostosować procedury do zawartych w nim przepisów.

Na etapie prac legislacyjnych są również:

- nowa ustawa o ochronie danych osobowych (projekt z 12 września 2017 r.), która ma uzupełnić RODO, oraz
- ustawa Przepisy wprowadzające ustawę o ochronie danych osobowych (projekt z 12 września 2017 r.).

Akty prawne regulujące prawo o ochronie danych osobowych:

- rozporządzenie RODO,
- ustawa o ochronie danych osobowych,
- ustawa Przepisy wprowadzające ustawę o ochronie danych osobowych.

CZĘŚĆ II – Co zmieni się w ochronie danych

Dostosowywanie organizacji powinno się rozpocząć już teraz. Placówka 25 maja 2018 r. musi działać zgodnie z nowymi przepisami. Sprawdź, co się zmieni.

Doprecyzowanie definicji danych osobowych

RODO przynosi przełomowe zmiany, dodatkowe wymogi i wytyczne. Wprowadza również nowe definicje danych. Aktualne standardy w rozumieniu pojęcia danych osobowych wyznacza dyrektywa 95/46/WE. Według niej termin ten oznacza wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby fizycznej. Warto zatem przyjrzeć się legalnej definicji pojęcia danych osobowych oraz nowym kategoriom danych wyodrębnionym w ogólnym rozporządzeniu o ochronie danych.
Pojęcie danych osobowych zostało utworzone w RODO oraz ustawie o ochronie danych osobowych na podstawie trzech elementów:

- informacji
- dotyczącej osoby fizycznej,
- zidentyfikowanej lub możliwej do zidentyfikowania.

Zasadniczy sposób oraz koncepcja definiowania danych nie uległy zmianie na gruncie RODO – patrz tabela 1.

Tabela 1. Dane osobowe w UODO vs RODO

UODO – art. 6	RODO – art. 4
Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej	Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na: numer identyfikacyjny, kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, kulturowe lub społeczne	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, ■ jeden bądź kilka szczególnych czynników określających: fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. **Motyw 30 preambuły** – osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawieniem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i identyfikowania tych osób
Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań	**Motyw 26 preambuły** – (...) aby stwierdzić, czy dana osoba jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób identyfikacji może być z uzasadnionym prawdopodobieństwem wykorzystany do identyfikacji danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebny do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak też postęp technologiczny

Nowa definicja – pseudonimizacja

Pseudonimizacja jest pojęciem, które nie występuje na gruncie ustawy o ochronie danych osobowych, chociaż obowiązywało w potocznym rozumieniu. Termin ten zdefiniowany został natomiast w RODO (art. 4 ust. 5, motyw 28 i 29 preambuły). Oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

ZAPAMIĘTAJ!

Pseudonimizacja danych osobowych oznacza pozbawienie informacji cech danych osobowych, a zatem możliwości identyfikacji na ich podstawie osoby fizycznej. Administrator danych, który zdecyduje się na ochronę danych poprzez ich pseudonimizację, musi pamiętać, że dane spseudonimizowane oraz informacje pozwalające na identyfikację, tj. szyfry, kody, dodatkowe informacje, muszą być przechowywane osobno, z zachowaniem odpowiednich środków ochrony.

Redefinicja danych wrażliwych

Porównując zakres szczególnych kategorii danych z art. 9 RODO z obecnym wykazem danych wrażliwych z art. 27 ustawy o ochronie danych osobowych, należy zauważyć, że niektóre kategorie danych osobowych, uznane obecnie za dane wrażliwe, nie należą do szczególnych kategorii danych osobowych na gruncie RODO.
Wrażliwe dane osobowe to m.in. dane (art. 9 ust. 1 RODO):

- ujawniające pochodzenie rasowe bądź etniczne,
- ujawniające poglądy polityczne,
- dotyczące przekonań religijnych (np. wyznanie, uczestnictwo w nabożeństwach lub ceremoniach religijnych, obchodzenie świąt właściwych dla danego wyznania) lub światopoglądowych,
- odnoszące się do przynależności do związków zawodowych (np. historia przynależności, pełnione w związku zawodowym funkcje),
- genetyczne,
- biometryczne (np. odciski palców, głos, obraz tęczówki oka, odcisk stopy lub dłoni, grupa krwi),
- o stanie zdrowia (np. przebyte choroby, planowane zabiegi medyczne oraz przepisane lekarstwa),
- o orientacji seksualnej.

Nowością jest włączenie do danych szczególnej kategorii danych genetycznych i biometrycznych. Ponadto RODO wprowadza definicję danych dotyczących stanu zdrowia.

ZAPAMIĘTAJ!

Zgodnie z definicją wprowadzoną przez RODO dane dotyczące zdrowia to dane osobowe o zdrowiu zarówno fizycznym, jak i psychicznym oraz informacje o korzystaniu z usług opieki zdrowotnej.

Zakres wrażliwych danych osobowych jest więc szeroki i obejmuje zarówno informacje nierozerwalnie związane z daną osobą (np. dane genetyczne, pochodzenie rasowe), jak i nabyte lub związane z jej działalnością (np. przynależność do związków zawodowych, światopogląd).

Szczególna podstawa prawna dla danych wrażliwych

RODO zabrania przetwarzania wrażliwych danych osobowych. Jednocześnie, w celu zgodnego z prawem ich przetwarzania, wymagane jest, aby przetwarzanie szczególnych kategorii danych osobowych miało szczególną podstawę prawną. Podstawy prawne zostały określone w art. 9 ust. 2 RODO. Jest ich 11. Na uwagę zasługują trzy z nich. I tak:

1. RODO umożliwia przetwarzanie wrażliwych danych osobowych na podstawie zgody. Zgoda na przetwarzanie wrażliwych danych osobowych musi być wyraźna, co oznacza, że nie można jej domniemywać z innych oświadczeń. Co ciekawe, zniesiono wymóg zgody na piśmie (jako jednej z przesłanek przetwarzania tych danych).
2. Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (np. dokumenty potwierdzające stan zdrowia pracownika do uzyskania zapomogi z ZFŚS).
3. Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (np. w sytuacjach zagrożenia zdrowia i życia uczeń, nauczyciel, pracownik nie będzie mógł wyrazić zgody na przetwarzanie danych wrażliwych z uwagi na jego stan zdrowia, ale lekarze czy inne osoby udzielające mu pomocy będą mogli pozyskać i wykorzystać takie dane).

Tabela 2. Porównanie – dane wrażliwe w UODO vs szczególne kategorie danych w RODO

UODO – art. 27 ust. 1	**RODO – art. 9 ust. 1**
Pochodzenie rasowe lub etniczne	Pochodzenie rasowe lub etniczne
Poglądy polityczne	Poglądy polityczne
Przekonania religijne lub filozoficzne	Przekonania religijne lub światopoglądowe
Przynależność wyznaniowa, partyjna lub związkowa	Przynależność do związków zawodowych

UODO – art. 27 ust. 1	**RODO – art. 9 ust. 1**
Życie seksualne	Dane dotyczące seksualności lub orientacji seksualnej
Wyroki, orzeczenia o ukaraniu i mandatach karnych oraz inne wydane w postępowaniu sądowym lub administracyjnym	Brak
Nałogi	Brak
Brak	Dane biometryczne Art. 4 pkt 14 – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne
Stan zdrowia	Dane dotyczące zdrowia Art. 4 pkt 15 – oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie zdrowia. Motyw 35 preambuły – do danych osobowych dotyczących zdrowia należy zaliczyć wszelkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE, numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych, informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała bądź płynów ustrojowych, w tym danych genetycznych i próbek biologicznych, oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym bądź biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne *in vitro*
Kod genetyczny	Dane genetyczne Art. 4 pkt 13 – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

UODO – art. 27 ust. 1	RODO – art. 9 ust. 1
	Motyw 34 preambuły – dane genetyczne należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, uzyskane z analizy próbki biologicznej dane osoby fizycznej, w szczególności z analizy chromosomów, DNA lub RNA bądź z analizy innych elementów umożliwiających pozyskanie równoważnych informacji

2 zadania do wykonania

Kluczowy sposób definiowania danych osobowych na gruncie RODO również nie ulega zmianie. Nie oznacza to jednak, że RODO klonuje znane z ustawy o ochronie danych osobowych definicje danych osobowych. Wyodrębnione zostały bowiem nowe kategorie danych oraz sprecyzowane te obecnie istniejące.

ZASTOSUJ!

Działania, które warto podjąć już dziś, to:

- weryfikacja danych osobowych na podstawie nowego podziału:
  1) dane zwykłe,
  2) szczególne kategorie danych (dotychczas są to dane wrażliwe);
- upewnienie się, że istnieją uzasadnione powody gromadzenia określonej kategorii danych w Twojej jednostce (monitorować zmiany Karty Nauczyciela, ustawy o systemie oświaty czy Prawa oświatowego w zakresie danych osobowych).

Przetwarzanie danych wg RODO

Placówka nie musi uzyskiwać zgody na przetwarzanie większości danych osobowych – uprawnienia w tym zakresie wynikają bowiem przede wszystkim z:

- ustawy Prawo oświatowe,
- ustawy Karta Nauczyciela,
- ustawy Kodeks pracy,
- ustawy o Systemie Informacji Oświatowej,
- innych przepisów.

Po zmianach te przepisy wciąż będą podstawą prawną dla przetwarzania danych.
Zarówno obecna *ustawa o ochronie danych osobowych,* jak i *RODO* wskazują przypadki, czynności lub zdarzenia, których spełnienie legalizuje proces przetwarzania informacji. Definicja przetwarzania danych na gruncie RODO w praktyce nie różni się od obecnie funkcjonującej definicji tego pojęcia – patrz tabela 3.

Tabela 3. Definicja przetwarzania danych UODO vs RODO

UODO – art. 7 pkt 2	RODO – art. 4 pkt 2
Przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych	„Przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych bądź zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie bądź łączenie, ograniczanie, usuwanie lub niszczenie

6 przesłanek przetwarzania danych zwykłych

Zgodnie z art. 6 RODO przetwarzanie jest zgodne z prawem, gdy:

1) osoba, której dane dotyczą, wyraziła na to zgodę,
2) jest niezbędne do wykonania umowy lub podjęcia działań przed jej zawarciem,
3) jest niezbędne do wypełnienia obowiązku prawnego nałożonego na administratora,
4) jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
5) jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej,
6) jest niezbędne do celów wynikających z prawnie uzasadnionych interesów.

RODO przewiduje zatem 6 przypadków, kiedy możemy zgodnie z prawem przetwarzać tzw. dane zwykłe.

ZAPAMIĘTAJ!

Pamiętaj, że RODO nie zmienia zasad udostępniania danych. Dotyczy to np.:

- udzielania informacji o dziecku, w przypadku gdy rodzice są po rozwodzie (wówczas określa się sposoby weryfikacji, komu można udzielić informacji oraz kiedy rodzic może zwrócić się do nauczyciela o udzielenie informacji o dziecku),
- prawa przedszkola/szkoły do żądania informacji o stanie zdrowia dziecka,
- zasad wykorzystania wizerunku dziecka,
- udostępniania danych osobowych dzieci/uczniów w materiale prasowym.

Czym jest „prawnie uzasadniony interes"

Zgodnie z obecnie obowiązującym stanem prawnym każdy administrator danych może szukać podstawy przetwarzania danych osobowych w przepisach prawa. To samo, choć w ograniczonym zakresie, będą mogli robić administratorzy po rozpoczęciu stosowania przepisów RODO. W zakresie tej przesłanki legalności RODO wprowadza, wydawałoby się, niewielką, lecz mającą istotne znaczenie zmianę. RODO zrezygnowało bowiem z legalizacji przetwarzania danych osobowych na podstawie uprawnienia wynikającego z przepisu prawa. Stanowi to celowe działanie, które powoduje zawężenie przetwarzania danych na podstawie przepisów prawa wyłącznie w zakresie realizacji nałożonego na administratora danych obowiązku. Tym samym, jeżeli teraz administrator opiera się na takim przepisie przetwarzania danych osobowych, po 25 maja 2018 r., podstawę tę utraci.

Podstawa przetwarzania danych z monitoringu

Obecnie, jeżeli w szkołach czy przedszkolach wyodrębnia się zbiór monitoring, jako podstawę przetwarzania danych w nim zawartych podaje się właśnie prawnie usprawiedliwiony cel (art. 23 ust. 1 pkt 5 UODO) – zagwarantowanie bezpieczeństwa uczniów i innych osób przebywających na terenie placówki. Taką podstawę przetwarzania tych danych podaje również Generalny Inspektor w wydanych niedawno „Wytycznych GIODO dotyczących wykorzystania monitoringu wizyjnego w szkołach".

Organy publiczne, które obecnie powołują się na art. 23 ust. 1 pkt 5 UODO (prawnie usprawiedliwiony cel) przy przetwarzaniu danych w ramach realizacji swoich zadań, po 25 maja 2018 r. stracą tę podstawę. Od 25 maja placówki mają zakaz powoływania się na tę przesłankę przetwarzania przez organy publiczne w zakresie, w jakim dokonują one przetwarzania danych w ramach realizacji swoich zadań. Problem polega na tym, że zapewnienie bezpieczeństwa w placówce jest zadaniem publicznego przedszkola/szkoły, wynikającym z ustawy Prawo oświatowe.

Czy to oznacza, że pod koniec maja 2018 roku z polskich jednostek będą musiały zniknąć kamery? Niekoniecznie. W tym zakresie mamy dwa możliwe scenariusze.

Pierwszy z nich to określenie przez polskiego ustawodawcę ram prawnych stosowania monitoringu. Wówczas spełnione zostaną postanowienia motywu 47 RODO, który wskazuje, że dla organów publicznych podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca. Notabene ustawa o monitoringu wizyjnym jest wyczekiwana już od wielu lat. Niestety wydaje się mało prawdopodobne, że taka ustawa zostanie opracowana i wejdzie w życie w przeciągu kilku miesięcy.

Drugim scenariuszem, nieco mniej optymistycznym, jest pozostawienie sytuacji samej sobie i przymknięcie oka na to, że podmioty publiczne stracą jedną z podstaw przetwarzania danych. Wówczas m.in. przedszkolom pozostanie szukanie innych przesłanek legalizujących

wykorzystywanie kamer. Najbliższą temu przetwarzaniu przesłanką wskazaną w RODO będzie w takim wypadku wypełnienie obowiązku prawnego określonego w ustawie Prawo oświatowe w zakresie zapewnienia warunków działania jednostki, w tym bezpiecznych i higienicznych warunków nauki, wychowania i opieki.

3 zadania do wykonania:

1) upewnij się, że zidentyfikowałeś wszystkie procesy przetwarzania danych zachodzące w szkole/przedszkolu,
2) upewnij się, że dysponujesz wskazanymi w RODO przesłankami legalnego przetwarzania danych osobowych w odniesieniu do każdego ze zbiorów danych,
3) jeżeli placówka jest organem publicznym i opiera przetwarzanie danych na przesłance prawnie usprawiedliwionego celu, sprawdź, czy po rozpoczęciu stosowania RODO nadal będzie mogła korzystać z tej przesłanki, jeżeli nie, postaraj się zidentyfikować inną przesłankę przetwarzania danych.

Zgoda na przetwarzanie danych wg RODO

Najważniejsze zmiany polegają głównie na potwierdzeniu w treści RODO warunków wyrażenia zgody (art. 7 RODO). I tak, żeby przetwarzanie danych na podstawie zgody było legalne (np. na potrzeby organizowanego konkursu międzyprzedszkolnego), należy zapewnić:

- możliwość wycofania zgody w łatwy sposób i w dowolnym momencie – jeśli administrator planuje uzyskiwać zgodę, powinien już na tym wstępnym etapie przewidzieć mechanizm jej wycofania, a więc zastanowić się, jak zgodę tę będzie można odwołać (gdzie rodzic musi się zgłosić, jaki dokument wypełnić),
- dobrowolność wyrażenia zgody – chodzi o to, żeby nie uzależniać podjęcia pewnych działań od wyrażenia zgody (np. udział w konkursie uzależniony od wyrażenia zgody na przetwarzanie zgody przez podmiot fundujący nagrodę w konkursie),
- aby osoba wyrażająca zgodę rozumiała istotę zgody, jej cel i skutki, miała pełne rozeznanie, konkretnie przez kogo i w jakim celu jej dane będą przetwarzane,
- możliwość udowodnienia uzyskania zgody – jeśli administrator nie jest w stanie tego wykazać, nie dysponuje podstawą prawną umożliwiającą mu przetwarzanie danych osobowych.

Nie trzeba zbierać nowych deklaracji

Przedszkole/szkoła nie będą musiały pozyskiwać nowych zgód po 25 maja 2018 r. na wykorzystanie danych uczniów, nauczycieli, pracowników, rodziców, pod warunkiem że zebrane zgody odpowiadają warunkom RODO. Tak wskazano w motywie 171 preambuły RODO.

4 zadania do wykonania:

1. Sprawdź, czy w przypadku gdy zbierasz zgodę, jej wycofanie jest równie łatwe, jak wyrażenie zgody.
2. Sprawdź, czy w prawidłowy sposób formułowane jest zapytanie o zgodę.
3. Sprawdź, czy jesteś w stanie wykazać uzyskanie zgody osoby, której dane dotyczą.
4. Zweryfikuj, czy obecnie zbierane zgody spełniają warunki wyrażenia zgody, o których mowa w art. 7 RODO.

Warunki wyrażenia zgody przez dziecko

Jedną z najczęściej podkreślanych zmian jest to, że RODO wskazuje odrębne regulacje dotyczące warunków wyrażania zgody przez dzieci. Zgodnie z art. 8 ust. 1 RODO, jeżeli zastosowanie ma zgoda na przetwarzanie danych osobowych, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli natomiast dziecko nie ukończyło 16 lat (w Polsce ma być 13 lat), takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaakceptowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem.
Zwracam jednak uwagę, że te szczególne regulacje dotyczą usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. sprzedaż towarów za pośrednictwem strony internetowej), ale już nie zgody udzielanej w przedszkolu (np. na wykorzystanie wizerunku). W tym zakresie nic się zatem nie zmieniło. Zgodę w imieniu wychowanków wyrażają dalej rodzice. Wykorzystywanie danych osobowych uczniów na stronie WWW i rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej (nauczyciela, rodziców ucznia niepełnoletniego). Aby dyrektor mógł publikować na stronie internetowej dane osobowe uczniów, w tym wizerunek, powinien legitymować się co najmniej jedną z normatywnych podstaw przetwarzania danych osobowych, o których mowa w art. 23 ust. 1 UODO, a po 25 maja 2018 r. jedną z podstaw wskazanych w art. 6 RODO.

Publikowanie na podstawie przepisów prawa autorskiego

Nie każde zdjęcie wymaga zgody na zamieszczenie w albumie, kronice, w tym w Internecie. Jeżeli zdjęcia spełniają warunek z art. 81 ust. 2 pkt 2 prawa autorskiego, możliwa jest ich publikacja (wykorzystanie) bez zgody uwidocznionych na nich osób (czy w ich imieniu rodziców). Możliwe jest rozpowszechnianie zdjęć z imprez przedszkolnych/szkolnych (wycieczek) w przypadku publikowania zdjęć, na których sylwetka osoby jest jedynie szczegółem całości uwiecznionej na zdjęciu imprezy. Aby zamieszczenie takiego zdjęcia reportażowego było możliwe bez uzyskania zgody, to:

- osoba przedstawiona na zdjęciu nie może być głównym tematem fotografii, musi pojawić się na niej niejako „przy okazji", jako element uboczny,

- dana osoba musi być elementem danego zdjęcia, szczegółem – zgromadzenia, krajobrazu, publicznej imprezy (wyliczenie jest przykładowe, może to być również wycieczka szkolna, impreza szkolna itd.),
- co do zasady zdjęcie nie powinno też być zdjęciem pozowanym (pozowanie niejako oznaczałoby, że dana osoba jest jednak istotnym elementem zdjęcia, dopuszczalne jest jednak publikowanie zdjęć klasowych),
- dodatkowo, nawet w przypadku spełnienia powyższych zasad – zdjęcie w żaden sposób nie powinno naruszać prawa do prywatności przedstawionych na nim osób ani w żaden sposób naruszać ich dóbr osobistych.

Jeżeli zdjęcie spełnia te kryteria, można śmiało publikować bez zgody (zdjęcie pozowane wychowanków może być zamieszczone bez zgody rodziców).

Prawo do bycia zapomnianym

Temat wyrażania zgody na przetwarzanie danych łączy się z tematem nowych uprawnień, jakie zyskały osoby, których dane są przetwarzane (rodzice, pracownicy). Otóż prawo to polega na żądaniu od administratora niezwłocznego usunięcia danych osobowych (tzw. bycia zapomnianym). Żądanie to może zostać wysunięte m.in. w poniższych przypadkach (art. 17 RODO):

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
- osoba, której dane dotyczą, cofnęła zgodę, na której się opiera, i nie ma innej podstawy prawnej przetwarzania,
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania,
- dane osobowe były przetwarzane niezgodnie z prawem.

ZAPAMIĘTAJ!

Prawo do bycia zapomnianym jest uprawnieniem podmiotu, którego dane są przetwarzane do żądania od administratora niezwłocznego usunięcia dotyczących go danych osobowych.

Należy jednak podkreślić, nie w każdej sytuacji, gdy zgłoszone zostanie żądanie, że administrator przetwarzający dane będzie musiał je zrealizować. Obowiązek usunięcia danych nie będzie występował, jeżeli przedszkole/szkoła dysponuje inną podstawą prawną do ich przetwarzania.

Jak prawo do bycia zapomnianym ma wyglądać w praktyce

Otóż wyzwaniem dla jednostek oświatowych będzie przede wszystkim żądanie usunięcia danych, w przypadku gdy ich przetwarzanie zależy od zgody czy to rodzica, czy pracownika,

gdyż w tym przypadku istnieje największe ryzyko, że osoba zmieni zdanie co do wykorzystywania określonych danych, na które wyraziła wcześniej zgodę.
Aby wywiązać się skutecznie z prawa do bycia zapomnianym, dyrektor będzie musiał upewnić się, że wszystkie linki do zamieszczonych w sieci do tych informacji także zostały skasowane, a kopie pousuwane, nawet jeżeli są w posiadaniu innych podmiotów przetwarzających te dane w imieniu administratora. Trzeba będzie określić w ramach placówki:

- kto ma zająć się tą kwestią,
- jakie czynności musi wykonać,
- jaki dokument sporządzi,
- gdzie zweryfikować informacje, jak i do kogo raportować.

„Administratora danych" zastąpi „administrator"

Administratorem danych jest przedszkole/szkoła, w imieniu którego/której obowiązki administratora danych osobowych wykonuje dyrektor. On decyduje o celach i środkach przetwarzania danych. Na administratorze danych spoczywa odpowiedzialność za przetwarzane dane osobowe, bez względu na to, kto faktycznie administruje tymi danymi i kto je przetwarza. Jest odpowiedzialny za bezpieczeństwo tych danych oraz ponosi odpowiedzialność za naruszanie przepisów o ochronie danych osobowych.

16 obowiązków administratora

Podstawowym obowiązkiem administratora jest dbanie o to, aby przetwarzanie danych odbywało się zgodnie z RODO i aby móc to wykazać. Administrator:

1) wyznacza inspektora ochrony danych;
2) ma wdrażać odpowiednie i skuteczne środki techniczne i organizacyjne:
   a) mają one zapewniać najwyższy znany i możliwy w chwili przetwarzania danych poziom ochrony,
   b) nie może być to czynność jednorazowa, środki te są w razie potrzeby poddawane przeglądom i uaktualniane,
   c) dokonuje on tego, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia,
   d) jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych;
3) prowadzi komunikację z podmiotem danych i przekazuje mu informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny;
4) ułatwia podmiotom danych wykonywanie ich praw;
5) nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie, czas na udzielenie informacji przez ADO to maksymalnie miesiąc;

6) weryfikuje tożsamość osób wnoszących żądania udzielenia informacji;
7) potwierdza, czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli to następuje, udziela wskazanych rozporządzeniem informacji;
8) ułatwia osobie, której dane dotyczą, wykonywanie jej praw z art. 15–22;
9) informuje osobę, której dane dotyczą, o działaniach, jakie podjął, w związku z jej żądaniami opartymi na art. 15–22;
10) uzasadnia odrzucenie żądania osoby, której dane dotyczą, i poucza ją o prawie skargi;
11) umożliwia dostęp do jej danych osobie, której one dotyczą;
12) dokonuje sprostowania i uzupełniania danych;
13) usuwa dane;
14) ogranicza przetwarzanie danych;
15) powiadamia o sprostowaniu lub usunięciu danych osobowych bądź o ograniczeniu ich przetwarzania;
16) dokonuje przenoszenia danych.

3 nowości w zadaniach dyrektora

RODO przewiduje dla administratorów w przedszkolu/szkole kilka nowych obowiązków:
1) zatrudnienie i powołanie inspektora ochrony danych osobowych,
2) rejestrowanie czynności przetwarzania,
3) informowanie o naruszeniu danych urzędu ochrony danych osobowych i osoby, których dane zostały naruszone (w przypadku placówek oświatowych ten ostatni obowiązek został zastąpiony odpowiednią informacją zamieszczaną na stronie WWW jednostki, szerzej w dalszej części tekstu).

Obowiązek powołania inspektora ochrony danych (IOD)

Najważniejszą zmianą z punktu widzenia przedszkola/szkoły jest obowiązek zatrudnienia specjalisty ds. ochrony danych osobowych. RODO nie posługuje się nazwą znaną z polskiej ustawy o ochronie danych osobowych – „administratora bezpieczeństwa informacji" (ABI), a sformułowaniem „inspektor ochrony danych" (IOD).
RODO nakłada na placówki obowiązkowe powołanie inspektora ochrony danych (art. 37 ust. 1 lit. a RODO). Rozporządzenie reguluje kwestię inspektorów w przepisach art. 37–39. Co prawda obecnie obowiązujące przepisy już określają zasady powoływania specjalistów, którzy zajmują się przetwarzaniem danych osobowych, to jednak zatrudnianie administratora bezpieczeństwa informacji (ABI) nie jest obowiązkowe.
Proszę zwrócić uwagę, że RODO w art. 37 nie wskazuje bezpośrednio, iż administrator wyznacza inspektora w przedszkolu/szkole. Stanowi jedynie, że należy powołać inspektora, gdy przetwarzania danych dokonuje organ lub podmiot publiczny.

Administrator danych (dyrektor) wyznacza inspektora ochrony danych. Jeżeli nie ma obecnie ABI, to najlepiej, żeby inspektor został wyznaczony najpóźniej od 25 maja 2018 r. W ciągu 14 dni od dnia wyznaczenia administrator danych zawiadamia Prezesa UODO o jego wyznaczeniu, wskazując (art. 5 nowej ustawy o ochronie danych osobowych):

- imię i nazwisko,
- adres poczty elektronicznej lub numer telefonu inspektora,
- adres i nazwę administratora danych (adres i nazwę placówki).

ABI zastąpi IOD

Na podstawie art. 134 projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych każdy obecnie funkcjonujący w przedszkolu/szkole administrator bezpieczeństwa danych (ABI) stanie się automatycznie inspektorem ochrony danych (IOD), ale tylko do 1 września 2018 r. (po tej dacie automatycznie przestaje być inspektorem). Zatem jeżeli na 24 maja 2018 r. funkcjonuje ABI, staje się z mocy prawa IOD tylko na pewien czas – od 25 maja do 1 września 2018 r.

Zatem dyrektor placówki, w którym obecnie jest ABI, do 1 września musi podjąć jedną z dwóch decyzji:

- zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu przez siebie IOD według nowych zasad (bo po weryfikacji dojdzie do wniosku, że dotychczasowy ABI spełnia wymagania kwalifikacyjne i może on być dalej IOD po 1 września 2018 r.),
- zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych, że ABI nie pełni funkcji IOD (wtedy musi powołać IOD na nowych zasadach).

Pracownik czy outsourcing usług IOD

Inspektor ochrony danych może (art. 37 ust. 6 RODO):

- być członkiem personelu (należy zakładać, że nie chodzi tylko o pracownika zatrudnionego na umowę o pracę, ale również na podstawie umowy cywilnoprawnej) lub
- wykonywać zadania na podstawie umowy o świadczenie usług.

Wybór należy do administratora. Oznacza to, że taka konstrukcja przepisu jednoznacznie wskazuje na możliwość outsourcingu świadczonego przez wyspecjalizowane w tym podmioty (na podstawie umowy o świadczenie usług).

Inspektor może być pracownikiem samorządowym

Jeżeli dyrektor zdecyduje się zatrudnić IOD w ramach stosunku pracy, to osoba taka będzie pracownikiem samorządowym z pełnymi tego konsekwencjami. Wydaje się, że stanowisko to powinno być stanowiskiem urzędniczym, a to na podstawie przepisów ustawy o pracownikach

samorządowych wymaga przeprowadzenia otwartego naboru. W konsekwencji też będą miały tu zastosowanie przepisy rozporządzenia płacowego dla pracowników samorządowych. Choć rozporządzenie nie przewiduje wprost stanowiska IOD, to można skorzystać z innych dostępnych nazw. Inspektor IOD może być więc głównym specjalistą, starszym specjalistą, specjalistą itp.

Nie możesz wyznaczyć siebie na inspektora

RODO przewiduje pewnego rodzaju gwarancje, które nie mogą być złamane (art. 38 ust. 6 RODO) – powierzenie inspektorowi innych zadań i obowiązków jest możliwe tylko pod warunkiem braku konfliktu interesów z innymi obowiązkami lub zadaniami. Naruszeniem tego zakazu konfliktu interesów byłoby np. powołanie na stanowisko inspektora osoby określającej w placówce cele i sposoby przetwarzania danych osobowych. Funkcji inspektora nie należy więc łączyć w szczególności z funkcjami dyrektora. Podstawowym przepisem, który dotyczy statusu IOD, jest art. 38 RODO. Na ten status składają się:

- niezależne wykonywanie zadań,
- podległość bezpośrednio kierownictwu administratora,
- brak możliwości otrzymywania poleceń przez inspektora w zakresie wykonywania przez niego swoich obowiązków,
- obowiązek wspierania IOD przez administratora w wykonywaniu przez niego zadań,
- obowiązek zapewnienia mu odpowiednich środków.

Inspektor bez studiów z ochrony danych

RODO wprowadza wymóg kwalifikacji zawodowych inspektora ochrony danych osobowych, na które składają się (art. 37 ust. 5 RODO):

- wiedza fachowa,
- umiejętności potrzebne do wykonywania zadań inspektora ochrony danych osobowych określonych w art. 39 RODO.

Do zadań inspektora należą m.in. (art. 39 RODO):

- informowanie administratora oraz pracowników o obowiązkach związanych z ochroną danych osobowych (o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych) i doradzanie im w tej sprawie,
- monitorowanie procesów przetwarzania danych osobowych zachodzących w przedszkolu,
- przeprowadzanie szkoleń z zakresu ochrony danych osobowych,
- przeprowadzanie audytów,
- ciągłe monitorowanie operacji przetwarzania danych osobowych w systemach informatycznych,

- dokonywanie oceny skutków (analiza ryzyka) na planowe operacje związane z przetwarzaniem danych osobowych,
- współpraca z organem nadzorczym (chodzi o Prezesa UODO),
- pełnienie funkcji punktu kontaktowego w kwestiach związanych z przetwarzaniem danych osobowych w placówce.

Można mieć wątpliwości, co w praktyce oznaczają te ogólne sformułowania. Wyjaśnienia tych pojęć podjęła się powołana przez państwa unijne, jako niezależny organ doradczy, Grupa Robocza ds. Ochrony Osób Fizycznych w Zakresie Przetwarzania Danych Osobowych. Jednym z efektów pracy Grupy Roboczej są „Wytyczne dotyczące inspektorów ochrony danych".

Wytyczne dotyczące inspektorów ochrony danych

Odpowiadając na pytanie o kwalifikacje zawodowe inspektora, należy wskazać, że powinien on posiadać odpowiednią wiedzę praktyczną i teoretyczną z zakresu:

- krajowych i europejskich przepisów o ochronie danych osobowych (w szczególności dokładną znajomość RODO),
- działania jednostek oświatowych,
- procedur administracyjnych i funkcjonowania jednostki oświatowej,
- operacji przetwarzania danych, systemów informatycznych i zabezpieczeń oraz powinien znać potrzeby administratora w zakresie ochrony danych.

Aby sprostać tym wymaganiom, rekomenduje się udział inspektora w odpowiednich i regularnych szkoleniach.

Jeden IOD dla kilku placówek

Zgodnie z art. 37 ust. 3 RODO, jeżeli administrator danych osobowych jest organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych. Ponieważ jednak inspektora wyznacza administrator danych, nie może go wyznaczyć dla przedszkoli/szkół gmina, a jedynie dyrektorzy tych jednostek.

Jeśli organ prowadzący zaproponuje jednostkom oświatowym oddanie do ich dyspozycji określonej liczby godzin pracy zatrudnionego w tym organie IOD w celu wykonywania obowiązków inspektora, niezależnie od dokonanego przez organ prowadzący powołania IOD, każdy dyrektor powinien powołać wskazaną osobę do pełnienia funkcji IOD w jednostce, w której jest dyrektorem. Proszę zauważyć, że nadal do wyłącznej kompetencji administratora danych będzie należało powoływanie osoby włączonej w sprawy dotyczące ochrony danych osobowych.

Rejestrowanie czynności przetwarzania

RODO nie wymaga rejestracji zbiorów danych osobowych, jednak dyrektorzy będą musieli prowadzić wewnętrzny rejestr czynności przetwarzania danych (*art. 30 ust. 1 RODO*). Dokumentacja powinna zawierać:

- informacje na temat administratora, inspektora ochrony danych,
- informacje na temat celu dokonywanych procesów przetworzenia danych osobowych, osób odpowiedzialnych za te procesy,
- informacje na temat kategorii danych osobowych i podmiotów danych objętych przetwarzaniem,
- informacje na temat okresów przechowywania danych,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Na wniosek Prezesa UODO administrator zobowiązany jest udostępnić mu taki rejestr. Rejestr będzie mógł być prowadzony zarówno w wersji papierowej, jak i elektronicznej.

Zgłoszenie naruszeń w ciągu 72 godzin

Administrator będzie miał obowiązek zgłaszania wszelkich naruszeń bezpieczeństwa danych osobowych w czasie do 72 godzin od naruszenia, bezpośrednio do właściwego organu nadzoru – Prezesa UODO (art. 33 RODO).

Należy zauważyć, że wcześniej nie było tego obowiązku. Poszczególne przedszkola/szkoły mogły regulować te kwestie w ramach swoich polityk bezpieczeństwa i szczegółowych procedur ustalanych w jednostce. Najczęściej wskazywano, w jakim czasie, w jakiej formie i do kogo należy zgłosić naruszenie zasad ochrony danych – przeważnie do osoby odpowiedzialnej za ochronę danych w jednostce, nigdy na zewnątrz placówki.

Aktualizacja dokumentacji ochrony

Obecnie na dokumentację składają się:

- polityka bezpieczeństwa,
- instrukcja zarządzania systemem informatycznym,
- upoważnienia dla pracowników,
- ewidencja upoważnień,
- umowy powierzenia przetwarzania danych osobowych.

RODO, co do zasady, nie wymaga prowadzenia tych dokumentów, co w obecnej ustawie o ochronie danych osobowych, w praktyce to na placówkach będzie spoczywał obowiązek udowodnienia, że przestrzegają regulacji.

ZAPAMIĘTAJ!

Po 25 maja 2018 r. nie będzie już obowiązku posiadania przez przedszkola/szkoły polityki przetwarzania danych osobowych, jak też instrukcji zarządzania systemem informatycznym oraz pozostałych dokumentów, które funkcjonują w jednostce.

Nie sposób sobie jednak wyobrazić, że placówka zlikwiduje instrukcję czy politykę tylko dlatego, że RODO wprost nie wymaga tych dokumentów. Proszę zauważyć, że w dalszym ciągu przepisy wymagają zapewnienia wymogów bezpieczeństwa, w tym wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stosowny stopień bezpieczeństwa. Zatem te dokumenty powinny nadal obowiązywać. Należy jedynie sprawdzić, czy przewidziane w nich regulacje są zgodne z RODO. Ponadto z dokumentów tych należy usunąć wszelkie odesłania do przepisów do ustawy o ochronie danych osobowych.

Pozostaną upoważnienia do przetwarzania danych

Po 25 maja 2018 r. nie będzie już obowiązywał przepis ustawy o ochronie danych osobowych (art. 37), który wskazuje, że każda osoba mająca kontakt z danymi osobowymi w placówce powinna mieć stosowne upoważnienie do przetwarzania tych danych, a poszczególne upoważnienia powinny być wpisane do ewidencji upoważnień. Nie oznacza to jednak, że po wejściu w życie RODO przedszkole nie będzie musiało nadawać upoważnień. O tym, że z RODO wynika obowiązek nadawania upoważnień, dowiadujemy się z kilku przepisów.

Obowiązek informacyjny

Dopełnienie obowiązku informacyjnego jest jednym z warunków legalnego przetwarzania danych osobowych. RODO rozróżnia dwa rodzaje obowiązku informacyjnego w sytuacji, kiedy administrator danych zbiera je:

- bezpośrednio od osoby,
- w sposób pośredni (od innych podmiotów).

Na gruncie przedszkolnym/szkolnym przede wszystkim chodzi o ten pierwszy przypadek.

ZAPAMIĘTAJ!

Przedszkole/szkoła przyjmując dane wychowanka, będzie musiało poinformować o szerszym zakresie prawa niż obecnie, aby spełnić obowiązek poinformowania, kto, w jakim celu, w jakim zakresie, na jak długo będzie przetwarzał dane osobowe.

Obowiązek informacji jest znacznie szerszy niż obecnie. Administrator na etapie pozyskiwania danych osobowych będzie zobowiązany m.in. do podania nowych informacji np. o podstawie prawnej przetwarzania, danych kontaktowych do IODO, okresie przechowywania danych,

prawie wniesienia skargi do organu nadzorczego, cofnięcia zgody na przetwarzanie danych w dowolnym momencie itp.

ZASTOSUJ!

Warto śledzić stronę **www.giodo.gov.pl**, być może do 25 maja 2018 r. pojawią się jakieś wytyczne co do formy i wzoru takiej klauzuli informacyjnej.

Sankcje za naruszenie przepisów RODO

Obowiązująca obecnie ustawa o ochronie danych osobowych przewiduje kary w postaci grzywny, ograniczenia wolności oraz pozbawienia wolności (art. 49–54a UODO). Administrator może zawinić, przetwarzając dane nielegalnie (np. bez zgody osoby, której dane dotyczą), nie zabezpieczając ich właściwie, umożliwiając do nich wgląd lub dostęp osobom nieupoważnionym, a także poprzez niewypełnienie obowiązku informacyjnego. Ustawa przewiduje także kary za niezgłoszenie zbioru danych do rejestru GIODO (tu zaznaczam, że nie każdy zbiór podlega zgłoszeniu, katalog wyłączeń jest w art. 43) oraz poprzez utrudnianie lub uniemożliwianie kontroli uprawnionym organom.
GIODO może jedynie nałożyć karę grzywny za niewypełnienie jego decyzji administracyjnej (GIODO nakazuje przywrócenie stanu zgodnego z prawem, np. poprzez usunięcie naruszenia w drodze decyzji administracyjnej). Maksymalna grzywna wynosi od 50 tys. zł. W wyjątkowych sytuacjach do 200 tys. zł.
Po 25 maja 2018 r. organ nadzorczy będzie mógł decydować o nałożeniu kary pieniężnej już w chwili stwierdzenia naruszenia, a nie dopiero w wyniku niewykonania decyzji administracyjnej (np. brak wymaganych rejestrów, a nie tylko w sytuacji, gdy w wyniku nieprzestrzegania zasad ochrony danych osobowych dojdzie do faktycznego naruszenia).

CZĘŚĆ III – Wdrażanie RODO krok po kroku – praktyczny przewodnik

Krok 1. Powołanie zespołu ds. zaktualizowania systemu ochrony danych

Można powołać zespół, który zajmie się przeglądem stanu ochrony danych w jednostce. Najlepiej już na tym etapie zastanowić się nad kwestią powołania inspektora ochrony danych. Formalnie jeszcze go nie powołujemy – musimy powołać IOD dopiero obowiązkowo 25 maja 2018 r. Oczywiście jeżeli obecnie w placówce jest ABI, to on, wspólnie z dyrektorem, powinien przygotować ją do zmian przepisów.

Krok 2. Przygotowanie harmonogramu wdrażania RODO

Zanim zostanie powołany inspektor ochrony danych, aby przygotować się do właściwego wypełniania nowych obowiązków, osoby wyznaczone do wdrożenia RODO w placówce

oświatowej muszą opracować szczegółowy harmonogram realizacji zadań, które należy w ramach takiego przygotowania zrealizować. Harmonogram musi być dostosowany odpowiednio do celów, zakresu i złożoności prowadzonych operacji przetwarzania danych osobowych. Powinien on określać:

- osobę (osoby), która jest odpowiedzialna za realizację zadania,
- osobę (osoby) współpracującą podczas realizacji zadania,
- sposób realizacji zadania oraz opracowania wyników jego realizacji,
- termin realizacji zadania.

Krok 3. Udział w szkoleniu

Po opracowaniu i zatwierdzeniu harmonogramu należy zorganizować szkolenie poświęcone nowym obowiązkom wynikającym z RODO, w tym w szczególności zadaniom określonym w harmonogramie (dedykowane lub wysłać pracowników na dostępne szkolenia zewnętrzne). Szkoleniem powinny zostać objęte przede wszystkim osoby, które będą realizowały zadania wskazane w harmonogramie. Udział w szkoleniu nie jest obowiązkowy, ale nabyta wiedza i uzyskane materiały będą stanowiły doskonały punkt wyjścia do dalszej pracy. W tym kroku należy zapoznać się z nowymi przepisami i informacjami o reformie.

Przygotowując się do wdrożenia RODO, można skorzystać z wytycznych **Grupy Roboczej Art. 29** – tak formalnie nazywa się ten organ. Grupa robocza do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwana Grupą Roboczą Art. 29, jako organ doradczy, składający się z przedstawicieli organów nadzorczych powołanych przez każde państwo członkowskie, podjęła się wyjaśnienia wątpliwości związanych z interpretowaniem przepisów RODO. Aktualnie wytyczne zostały przygotowane w nawiązaniu do zagadnień wynikających z przepisów RODO:

- wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego,
- wytyczne dotyczące inspektorów ochrony danych,
- wytyczne dotyczące prawa do przenoszenia danych.

Krok 4. Przeprowadzenie audytu systemu

Kolejnym zadaniem będzie przeprowadzenie sprawdzenia, czy dane osobowe są przetwarzane zgodnie z zasadami określonymi w RODO, tzn. czy zbierane są tylko dane wynikające z przepisów, czy na inne dane są wyrażone zgody itd. Taką analizę i ocenę powinny przeprowadzić osoby, które mają istotny wpływ na określenie celów przetwarzania danych osobowych oraz zorganizowanie procesu ich przetwarzania w placówce oświatowej.

ZAPAMIĘTAJ!

Wytyczne do przeprowadzenia takiej analizy i oceny powinien przygotować ABI, jeżeli został powołany, albo dyrektor.

W ramach tego zadania, za pomocą odpowiednich środków technicznych lub organizacyjnych, należy sprawdzić, czy dane osobowe są przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Należy również zastanowić się, jakie zabezpieczenia są w stanie zagwarantować, że dane osobowe będą bezpieczne i że nie uzyska do nich dostępu nikt nieuprawniony.
Wskazówek możesz szukać w obowiązującym do 25 maja 2018 r. rozporządzeniu wykonawczym do ustawy o ochronie danych osobowych dotyczącym środków technicznych ochrony danych osobowych (jest to rozporządzenie, które mówi, co powinno być uregulowane w polityce bezpieczeństwa i instrukcji). Taką analizę powinny przeprowadzić osoby odpowiedzialne w placówce oświatowej za projektowanie, wdrażanie, funkcjonowanie oraz ocenę skuteczności środków technicznych i organizacyjnych, których zadaniem jest zapewnienie odpowiedniego bezpieczeństwa danych osobowych. Po przeprowadzeniu analizy ABI albo dyrektor powinien ocenić, czy bezpieczeństwo danych osobowych jest zapewnione na odpowiednim poziomie.
Pomocne w ustalaniu kryteriów zabezpieczenia danych w dalszym okresie mogą być mechanizmy certyfikacji. Niestety jeszcze nie określono kryteriów, po spełnieniu których można ubiegać się o certyfikat spełniania obowiązków z RODO.

Krok 5. Zweryfikowanie aktualności polityki bezpieczeństwa przetwarzania danych osobowych i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Należy sprawdzić, czy informacje zawarte w tych dokumentach odpowiadają temu, co dzieje się w placówce, gdy chodzi o przetwarzanie danych osobowych. Zastanów się również, czy wdrożone i opisane środki bezpieczeństwa i ochrony danych osobowych są wystarczające z uwagi na to, w jaki sposób i w jakich celach przetwarzasz dane osobowe. Być może warto rozważyć wdrożenie dodatkowych środków, które poprawią bezpieczeństwo ochrony danych osobowych? Być może uważasz, że jakieś informacje w tych dokumentach nie opowiadają rzeczywistości, należy je poprawić. Jeżeli nie masz polityki bezpieczeństwa i instrukcji, to warto, byś przygotował choćby jeden dokument opisujący postępowanie z danymi osobowymi w jednostce. W takim dokumencie powinny znaleźć się wszystkie istotne informacje dotyczące obiegu danych osobowych. Zanim przygotujesz dokumentację, wdróż odpowiednie procedury i środki ochrony danych osobowych, a dopiero potem je opisz. Chodzi o to, by dokumentacja odpowiadała rzeczywistości, a nie była tylko kolejnym niechcianym dokumentem.

Krok 6. Ustalenie zbiorów danych

Jeżeli masz politykę bezpieczeństwa przetwarzania danych osobowych, to załącznikiem do niej powinien być wykaz zbiorów danych osobowych funkcjonujących w placówce. Zastanów się, czy w tym wykazie znajdują się wszystkie zbiory danych osobowych.
Jeżeli jakiś zbiór został pominięty, to należy go odnotować. Pomyśl, gdzie w jednostce masz do czynienia z danymi osobowymi. Nie ograniczaj się wyłącznie do oczywistych sytuacji. Pamiętaj, że dane osobowe mogą być na umowach, fakturach, w treści korespondencji e-mailowej, w systemie księgowym, w księdze korespondencji, w listach obecności w pracy, w listach osób uprawnionych do odebrania dzieci itd.
Upewnij się również, czy wykaz ten zawiera wszystkie informacje, jakie powinien zawierać rejestr czynności przetwarzania danych osobowych. W tym celu musisz zapoznać się z art. 30 RODO. W ten sposób dostosowując treść obecnego dokumentu, unikniesz konieczności tworzenia dodatkowych dokumentów. Możesz zmienić dotychczasowy załącznik i określić, że teraz ten wykaz będzie się nazywał rejestrem czynności przetwarzania danych.
Rejestr powinien zawierać:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora,
- kategorie osób, których dane dotyczą,
- określenie celu przetwarzania danych w odniesieniu do poszczególnych kategorii,
- określenie, jaki warunek jest podstawą prawną do przetwarzania danych,
- określenie, jaki warunek stanowi podstawę prawną do przetwarzania szczególnych kategorii danych osobowych,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Krok 7. Ustalenie, komu powierzane są dane osobowe

Zastanów się, jakie podmioty mają dostęp do danych osobowych, które przetwarzasz. Firmy, którym placówki zlecają zadania, to tzw. podmioty przetwarzające. Pamiętaj, że nie chodzi tylko o rzeczywisty dostęp do danych, ale również o sam fakt ich przechowywania. Oznacza to, że przetwarzanie danych osobowych będziesz powierzał choćby dostawcy dziennika elektronicznego, który przechowuje dane na serwerze.
Gdy już zdiagnozujesz, komu powierzasz przetwarzanie danych osobowych, to sprawdź, czy podmioty te dają gwarancję odpowiedniego postępowania z danymi, które im powierzasz.

ZAPAMIĘTAJ!
RODO wymaga, by zasady ich współpracy z przedszkolami/szkołami były precyzyjnie określone.

Przepisy zakazują zewnętrznym firmom przekazywania informacji innym podmiotom bez uzyskania zgody administratora. Najlepiej, gdybyś miał możliwość kontroli ich postępowania, ale jeżeli nie jest to możliwe, zabezpiecz się stosownymi oświadczeniami w umowach powierzenia. Jeżeli zawarcie umów powierzenia również nie jest możliwe, sprawdź, jakie informacje o danych osobowych znajdują się w politykach prywatności podmiotów, które biorą udział w przetwarzaniu danych.

Krok 8. Ustalenie, czy dostęp do danych mają osoby do tego uprawnione

Pamiętaj, by nadać stosownej treści upoważnienia do przetwarzania danych osobowych tym osobom, które będą miały dostęp do danych. Dokumenty upoważnień mogą być takie same jak te, które obecnie wykorzystuje placówka. Należy tylko sprawdzić i usunąć zapis dotyczący odesłania do art. 37 ustawy o ochronie danych osobowych. Warto zaktualizować wszystkie dotychczas wydane upoważnienia. Dalej można prowadzić ewidencję osób upoważnionych, by odnotowywać w niej wszystkie osoby, które upoważnisz do przetwarzania danych osobowych.

Krok 9. Aktualizacja klauzul dotyczących spełnienia obowiązku informacyjnego

RODO wprowadza rozszerzony obowiązek informacyjny, co oznacza, że musisz rodzicom czy innym osobom, od których pozyskujesz dane, przekazać więcej informacji niż na gruncie dotychczas obowiązującej ustawy o ochronie danych osobowych (np. osobom upoważnionym do odbioru dziecka z przedszkola).

Krok 10. Opracowanie procedur na wypadek korzystania z prawa przysługującego osobom, których dane są przetwarzane

Gdy już poinformujesz osoby, których dane przetwarzasz, o przysługujących im uprawnieniach, to należy również być gotowym na to, że osoby te mogą zechcieć takie uprawnienia zrealizować. Przygotuj odpowiednie procedury.

Krok 11. Opracowanie procedur analizy ryzyka i zarządzania nim w przetwarzaniu danych

Poziom bezpieczeństwa przetwarzanych danych osobowych powinien być odpowiedni do zidentyfikowanego ryzyka naruszenia praw i wolności osób fizycznych wiążącego się z przetwarzaniem danych (*art. 32 oraz pkt 83 preambuły RODO*).

ZASTOSUJ!

Aby zapewnić odpowiedni poziom bezpieczeństwa danych, placówka oświatowa musi wdrożyć odpowiednie środki techniczne i organizacyjne, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Dotychczas było to określone w polityce bezpieczeństwa i instrukcji zarządzania systemami informatycznymi.

RODO nie nakłada wprost na placówkę oświatową obowiązku zarządzania ryzykiem naruszenia praw i wolności osób fizycznych, które wiąże się z przetwarzaniem danych, jednak z treści i logiki przepisów RODO wynika, że właściwą drogą do zapewnienia odpowiedniego do tego ryzyka poziomu bezpieczeństwa jest zarządzanie tym ryzykiem.
Należy wdrażać następujące środki techniczne i organizacyjne, które zapewniają stopień bezpieczeństwa odpowiadający zarządzanemu ryzyku (*art. 32 ust. 1 lit. a, b, c oraz d RODO*):

- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych, które mają zapewnić bezpieczeństwo przetwarzania.

ZASTOSUJ!

Dyrektor powinien wypracować odpowiednie dla siebie podejście do zarządzania ryzykiem naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych, uwzględniające swoje środowisko, specyfikę prowadzonej działalności oraz posiadane doświadczenie, a w szczególności charakter, zakres oraz cele i sposób przetwarzania danych osobowych.

Krok 12. Opracowanie procedur zgłaszania naruszeń ochrony danych

Kolejną nowością RODO jest obowiązek zgłaszania naruszeń ochrony danych osobowych. Administrator będzie miał obowiązek zgłaszania wszelkich naruszeń bezpieczeństwa danych osobowych, w czasie do 72 godzin od naruszenia, bezpośrednio do właściwego organu nadzoru – Prezesa UODO (*art. 33 RODO*). Nie trzeba będzie zgłaszać naruszeń do organu nadzorczego, jeśli dyrektor oceni, że jest mało prawdopodobne, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych.
Nie zapomnij wypracować odpowiednie procedury, które pozwolą na:

- monitorowanie,
- ewidencjonowanie,
- zgłaszanie

naruszeń danych.

Krok 13. Informowanie osób, których dane dotyczą, o naruszeniu

Zgodnie z RODO (art. 34 RODO) o naruszeniu ochrony danych trzeba zawiadomić osoby, których dane dotyczą. W przypadku przedszkoli/szkół ten obowiązek został ograniczony w nowych przepisach dotyczących ochrony danych w Karcie Nauczyciela, ustawie o systemie oświaty i ustawie Prawo oświatowe. Wystarczy, że administrator danych zamieści na swojej

internetowej stronie podmiotowej lub w BIP komunikat o zaistniałym naruszeniu nie później niż 72 godziny od stwierdzenia naruszenia (może to robić IOD). Należy opracować zasady, wzór i sposób zamieszczania komunikatu.

Krok 14. Zamieszczenie informacji o ograniczonym zakresie stosowania przepisów RODO na BIP

Dyrektor na podstawie nowych przepisów wprowadzonych do Karty Nauczyciela, ustawy o systemie oświaty, ustawy Prawo oświatowe jest zobowiązany do informowania o ograniczeniach w stosowaniu niektórych przepisów RODO na swojej stronie podmiotowej Biuletynu Informacji Publicznej lub na swojej stronie internetowej. Poniżej zamieszczamy zestaw przepisów RODO, których stosowanie w przedszkolu/szkole zostało częściowo ograniczone – patrz tabela 4.

Tabela 4. Wykaz przepisów RODO, których stosowanie zostało ograniczone

Przepis RODO	Zakres ograniczenia
Art. 5	Do przetwarzania danych osobowych, o których mowa w art. 188a ust. 1 ustawy Prawo oświatowe, art. 91e Karty Nauczyciela, art. 95b ustawy o systemie oświaty, nie stosuje się art. 5 ust. 2 RODO – w zakresie obowiązku wykazywania przestrzegania przepisów art. 5 ust. 1 RODO.
Art. 12	Obowiązki z art. 12 realizowane są bezpłatnie raz na sześć miesięcy. W pozostałych przypadkach administrator danych ma prawo pobrać opłatę w wysokości odpowiadającej kosztom sporządzenia odpowiedzi lub kopii danych *(art. 188a ustawy Prawo oświatowe, art. 91e Karty Nauczyciela, art. 95b ustawy o systemie oświaty)*.
Art. 15	
Art. 13	Do przetwarzania danych osobowych nie stosuje się danych z ustawy Prawo oświatowe, Karta Nauczyciela, ustawy o systemie oświaty.
Art. 14	
Art. 17	Do przetwarzania danych osobowych nie stosuje się danych z ustawy Prawo oświatowe, Karta Nauczyciela, ustawy o systemie oświaty.
Art. 18	
Art. 19	
Art. 34	Przepisu art. 34 RODO nie stosuje się, jeśli administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej Biuletynu Informacji Publicznej lub na swojej stronie internetowej.

Krok 15. Zatrudnienie inspektora ochrony danych

Należy zatrudnić IOD, który może być zatrudniony na część etatu. Dopuszczalną formą jest zatrudnienie inspektora przez organ prowadzący, ale wtedy dyrektor powinien powołać go do pełnienia funkcji w przedszkolu/szkole.

Krok 16. Współpraca z nowym organem – UODO

Kolejnym środkiem bezpieczeństwa, zgodnie z RODO, jest współpraca z organem nadzorczym – na jego żądanie oraz w ramach wykonywanych przez niego zadań. Współpraca z organem nadzorczym należy do jednych z podstawowych zadań IOD (*art. 39 ust. 1 pkt d RODO*). GIODO przestanie istnieć. Jego miejsce zajmie Urząd Ochrony Danych Osobowych, na czele którego stanie Prezes. UODO będzie prawnym następcą GIODO.

Krok 17. Zweryfikowanie obowiązku informacyjnego

RODO nakłada na przedszkola/szkoły również dodatkowe obowiązki informacyjne, dlatego konieczne będzie opracowanie specjalnych formularzy przedstawianych osobom, od których zbierane są dane. Administrator danych na etapie pozyskiwania danych osobowych będzie zobowiązany m.in. do podania nowych informacji, np.: o podstawie prawnej przetwarzania, danych kontaktowych do IODO, okresie przechowywania danych, prawie do ich przenoszenia, prawie wniesienia skargi do organu nadzorczego, cofnięcia zgody na przetwarzanie danych w dowolnym momencie itp.

§ ŹRÓDŁO:

- art. 4, art. 5 projektu ustawy o ochronie danych osobowych (z 12 września 2017 r.),
- art. 134 projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych (z 12 września 2017 r.).

§ PODSTAWA PRAWNA:

- ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922),
- art. 9 ustawy z 27 sierpnia 2009 r. o finansach publicznych (tekst jedn.: Dz.U. z 2017 r. poz. 2077),
- punkt 83, 97 preambuły, art. 24, art. 28, art. 32−39 rozporządzenia 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.Urz. UE. L nr 119, str. 1).

OŚWIATA
grupa wydawnicza

ISBN 978-83-269-7347-5

1BA93