RODO W PRZEDSZKOLU – ANALIZUJEMY PRZEPISY

Autor: **Dariusz Skrzyński**

Każde przedszkole 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 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.

W niniejszym opracowaniu wyjaśniamy, jak przygotować przedszkole oraz jego pracowników do rozpoczęcia obowiązywania najważniejszych przepisów dotyczących ochrony danych osobowych.

CZĘŚĆ I – AKTY PRAWNE W OCHRONIE DANYCH

Nowe zasady zaczną obowiązywać już od 25 maja 2018 r., dlatego właśnie teraz jest ostatni moment, aby zacząć dokonywać przeglądu dotychczasowych zasad ochrony i nanieść niezbędne poprawki. Nie będzie to proste, bo wielu zasad wykonywania tych obowiązków nie uregulowano, przenosząc ten ciężar na administratora.

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.

Trzy 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.).

Nowa ustawa o ochronie danych – co reguluje

Nowy tekst ustawy będzie regulował nieco inny zakres niż dotychczas. Zagadnienie uregulowane w ustawie o ochronie danych osobowych to:

- podmioty obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o wyznaczaniu,
- warunki i tryb udzielania certyfikacji i akredytacji,
- organ właściwy w sprawie ochrony danych osobowych,
- postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych,
- europejska współpraca administracyjna,
- postępowanie kontrolne,
- odpowiedzialność cywilna za naruszenie przepisów o ochronie danych osobowych,
- administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

ZAPAMIĘTAJ!

Akty prawne regulujące prawo o ochronie danych osobowych:

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

Trzy kroki do ustalenia nowych zasad

W związku z tym, że będziemy mieli w praktyce trzy dokumenty dotyczące danych osobowych, może pojawić się problem ze spójnym ustaleniem obowiązków placówki w zakresie przetwarzania i zabezpieczenia przetwarzanych w jednostce danych.

Krok 1. Najważniejszym dokumentem jest **RODO**. Zatem to w nim znajdziemy wszystkie obowiązki, jakie powinna spełniać placówka. Tym samym należy zapoznać się ze wszystkimi wymaganiami, które

reguluje. Oczywiście nie wszystkie zapisy tego rozporządzenia będą miały zastosowanie w przedszkolach (np. dotyczące akredytacji czy przekazywania danych do innych państw), ale warto zapoznać się z całością.

Przykład

PRZYKŁAD 1.

Jeżeli szukamy informacji o nowych zasadach wyznaczania inspektora ochrony danych (który zastąpi ABI), należy w pierwszej kolejności zajrzeć do art. 37–39 RODO, który regule status i obowiązki inspektora.

Krok 2. W kolejnym kroku, jeżeli wiemy, jak dane zagadnienie zostało uregulowane w RODO, sprawdzamy, czy **nowa ustawa o ochronie danych osobowych** uszczegóławia pewne elementy RODO. W naszej ustawie o ochronie danych osobowych znajdziemy przede wszystkim zasady postępowania w różnych okolicznościach, np. przy naruszeniu danych, kontroli, kompetencje i zasady działania Prezesa Urzędu Ochrony Danych Osobowych (wcześniej GIODO), informacje o karach za uchybienia, jak również zasady zawiadamiania Prezesa o wyznaczeniu inspektora ochrony danych.

Przykład

PRZYKŁAD 2.

Posiłkując się poprzednim przykładem, jeżeli zapoznamy się z regulacjami RODO o powoływaniu inspektora ochrony danych, należy następnie sięgnąć do art. 4 i 5 nowej ustawy o ochronie danych, z której dowiemy się, jaki mamy czas i do kogo należy złożyć zawiadomienie o wyznaczeniu inspektora ochrony danych (do Prezesa Urzędu Ochrony Danych Osobowych w ciągu 14 dni od jego wyznaczenia) oraz w jakiej formie.

Krok 3. W tym kroku ustalamy, czy nie ma jeszcze jakichś zasad przejściowych związanych z wprowadzeniem nowej ustawy o ochronie danych osobowych w ustawie **Przepisy wprowadzające ustawę o ochronie danych osobowych** – patrz przykład 3.

Z reguły w takich regulacjach wprowadzających zamieszcza się wykaz zmian w poszczególnych ustawach oraz szczególne zasady związane z płynnym wdrożeniem nowych przepisów. W tym przypadku ustawa wprowadzająca zawiera wykaz ponad 130 ustaw, które zostaną zmienione (np. Karta Nauczyciela, ustawa Prawo oświatowe, Kodeks pracy itd.). Pojawią się nowe przepisy, a nawet całe rozdziały zawierające kategorie przetwarzanych danych osobowych – patrz przykład 4. To w tych przepisach znajdziemy również informacje o tym, które z przepisów RODO w placówkach mają ograniczone zastosowanie.

Przykład

PRZYKŁAD 3.

W przypadku inspektora ochrony danych dowiemy się z ustawy wprowadzającej (art. 134), że dotychczasowy administrator danych osobowych (ABI) funkcjonujący w przedszkolu automatycznie po 25 maja 2018 r. będzie pełnił funkcję inspektora ochrony danych (IOD), ale tylko do 1 września 2018 r. Do tego czasu dyrektor będzie musiał poinformować o powołaniu nowego inspektora w sensie formalnym już w nowym trybie (ale może być ta sama osoba, która była ABI). Jeżeli dotychczas nie było ABI, należy obowiązkowo powołać inspektora ochrony danych.

Przykład

PRZYKŁAD 4.

Proponuje się wprowadzenie do Karty Nauczyciela przepisów określających obowiązki przetwarzania danych w związku z wykonywaniem określonych w ustawie zadań – nowy art. 91d. Ustawodawca wyraźnie określił katalog danych osobowych, jakie mogą być przetwarzane w sprawach:

- dotyczących awansu zawodowego nauczyciela (art. 9b, 9g Karty Nauczyciela),
- nadzoru nad awansem nauczyciela (art. 9h Karty Nauczyciela),
- dyscyplinarnych oraz komisji dyscyplinarnych (art. 77, art. 78 Karty Nauczyciela).

Można przetwarzać w szczególności następujące dane osobowe:

- imię i nazwisko,
- data i miejsce urodzenia,
- imiona rodziców,
- adres zamieszkania lub do korespondencji,
- wykształcenie, miejsce pracy i zajmowane stanowisko, w tym wysokość wynagrodzenia,
- numer NIP lub numer PESEL, w przypadku jego braku – rodzaj, seria i numer dokumentu potwierdzającego tożsamość,
- numer telefonu i adres poczty elektronicznej,
- numer rachunku bankowego.

CZĘŚĆ II – CO ZMIENI SIĘ W OCHRONIE DANYCH

Dostosowywanie organizacji powinno się rozpocząć już teraz. Przedszkole 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.

Obecnie nie ma zamkniętego katalogu danych osobowych. Dlatego też przy rozstrzyganiu, czy określona informacja lub informacje to dane osobowe, w większości przypadków, nieunikniona jest zindywidualizowana ocena uwzględniająca konkretne okoliczności oraz rodzaj środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby. Dane osobowe odnoszą się wyłącznie do osób fizycznych, a ich ochrona przysługuje bez wyjątku każdemu, w tym również uczniom, dzieciom (wychowankom przedszkola), rodzicom, pracownikom.

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**.
Pseudonimizacja danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą, oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych.

ZAPAMIĘTAJ!

Pseudonimizacja danych osobowych oznacza pozbawienie informacji cech danych osobowych, a zatem możliwości identyfikacji na ich podstawie osoby fizycznej.

Przykład

PRZYKŁAD 5.

Można udostępnić uchwałę rady pedagogicznej, po wcześniejszej anonimizacji danych ucznia, którego dotyczy uchwała, i informacji, na podstawie których można ustalić jego personalia.

Pseudonimizacja jest z założenia działaniem odwracalnym, które polega na utajnieniu tożsamości, np. poprzez zaszyfrowanie danych za pomocą określonego klucza. Zakłada możliwość reidentyfikacji danych osobowych, dlatego właśnie **dane spseudonimizowane uważane są za dane osobowe na gruncie RODO.**

Co ważne, **stosowanie pseudonimizacji jest w wielu przepisach RODO traktowane jako spełnienie wymogu stosowania odpowiednich środków technicznych i organizacyjnych** – art. 25 ust. 1 RODO: „(…) administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja (…)".

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

RODO, podobnie jak ustawa o ochronie danych osobowych, wyodrębnia pewne kategorie danych, których przetwarzanie, co do zasady, jest zakazane, a dopuszczalne wyłącznie po spełnieniu dodatkowych warunków. **Wyjątki od zakazu – szczególne podstawy dopuszczalności zostały wskazane w art. 9 ust. 2 RODO.** Dotychczas informacje te określano mianem danych wrażliwych. Natomiast RODO posługują się pojęciem „szczególne kategorie danych osobowych".

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.

Artykuł 27 ustawy o ochronie danych osobowych do danych wrażliwych zalicza informacje o:

- przekonaniach filozoficznych,
- przynależności wyznaniowej,
- przynależności partyjnej,
- skazaniach,
- orzeczeniach o ukaraniu i mandatach karnych,
- innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym,
- nałogach.

Na gruncie RODO wyżej wymienione informacje nie stanowią szczególnych kategorii danych osobowych.

Przykład

PRZYKŁAD 6.

Informacje zawarte w orzeczeniach sądowych orzekające rozwód czy przyznające opiekę nad dzieckiem nie należą już do „szczególnych kategorii danych osobowych". Również specjalne warunki przetwarzania nie będą zatem obejmowały danych osobowych dotyczących np. decyzji administracyjnych, które dzisiaj uznawane są za dane wrażliwe. Zatem ochrona danych w tych dokumentach będzie zapewniana tak jak w pozostałych przypadkach przy danych zwykłych.

Wrażliwe dane osobowe to między innymi 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, co do zasady, 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
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. 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

DWA 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

Przedszkole 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 w przedszkolach.

ZAPAMIĘTAJ!

Jedną z podstawowych zasad przetwarzania danych osobowych stanowi zasada legalności. Sprowadza się ona do tego, że aby móc zgodnie z prawem przetwarzać dane osobowe, administrator powinien dysponować tzw. przesłanką legalizującą to przetwarzanie. Taką przesłanką są regulacje prawa oświatowego czy prawa pracy.

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 sześć 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 do żądania informacji o stanie zdrowia dziecka,
- zasad wykorzystania wizerunku dziecka,
- udostępniania danych osobowych dzieci w materiale prasowym.

W wyżej wymienionych przypadkach w dalszym ciągu będzie to przede wszystkim przepis prawa lub zgoda rodzica dziecka. Gromadzone w przedszkolu informacje o dziecku powinny być udostępniane rodzicom i służyć przede wszystkim udzielaniu dziecku konkretnej pomocy. **Udostępnienie ich innym osobom i instytucjom powinno jasno wynikać z przepisów prawa.**

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. Zatem wszędzie tam, gdzie polski ustawodawca daje podmiotowi możliwość żądania podania danych osobowych, tj. posługuje się takimi pojęciami, jak: „może”, „ma prawo”, oznacza to, że dany podmiot jest do czegoś uprawniony. Tym samym, jeżeli teraz administrator opiera się na takim przepisie przetwarzania danych osobowych, po 25 maja 2018 r., podstawę tę utraci.

Przykład

PRZYKŁAD 7.

Artykuł 22(1) Kodeksu pracy daje pracodawcy uprawnienie do żądania od osoby ubiegającej się o pracę, a następnie od pracownika, podania konkretnych kategorii danych osobowych. Tym samym przepisy te nie nakładają na osobę, której dane dotyczą, obowiązku podania tych danych, a na prawodawcę obowiązku ich zbierania. W tym zakresie planowa jest nowelizacja Kodeksu pracy, gdzie wprost zostanie wskazane, że kandydat ma obowiązek podania określonych danych.

Przykład

PRZYKŁAD 8.

Na podstawie art. 55 ust. 3 pkt 2 ustawy Prawo oświatowe przedstawiciele gmin mają prawo do wglądu w dokumentację prowadzoną przez placówki oświatowo-wychowawcze, w tym w dziennik zajęć zawierający dane osobowe dzieci, w ramach wykonywania przez gminę uprawnień nadzorczych.

Podstawa przetwarzania danych z monitoringu

Obecnie, jeżeli w 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, również przedszkola, 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 przedszkola 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, 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.

Nie jest to jednak rozwiązanie niebudzące żadnych wątpliwości. Nie daje również gwarancji uznania tej przesłanki przez nowy organ nadzoru. Zwłaszcza w kontekście postanowień motywu 45 RODO, który wskazuje, **że uregulowanie prawne stanowiące podstawę przetwarzania danych powinno wprost wskazywać, iż stanowi podstawę operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, lub że przetwarzanie jest niezbędne do wykonania**

zadania realizowanego w interesie publicznym bądź w ramach sprawowania władzy publicznej, a także określać cel przetwarzania.

Ponadto prawo to może doprecyzowywać ogólne warunki dotyczące zgodności przetwarzania z prawem, określać sposoby wskazywania administratora, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty, którym można ujawniać dane osobowe, ograniczenia celu, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania.

ZASTOSUJ!

TRZY ZADANIA DO WYKONANIA:

1) upewnij się, że zidentyfikowałeś wszystkie procesy przetwarzania danych zachodzące w przedszkolu,

2) upewnij się, że dysponujesz wskazanymi w RODO przesłankami legalnego przetwarzania danych osobowych w odniesieniu do każdego ze zbiorów danych,

3) jeżeli przedszkole 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

RODO nie wprowadza rewolucyjnych zmian w kwestii zgody na przetwarzanie danych osobowych. Jeżeli chodzi o definicję zgody, to porównując zapisy art. 7 pkt 5 UODO i art. 4 pkt 11 RODO, można dojść do następujących wniosków:

- zgoda może mieć formę nie tylko oświadczenia, ale również wyraźnego działania potwierdzającego,
- podano przykłady form wyrażenia zgody (pisemne, elektroniczne lub ustne oświadczenie),
- RODO wyjaśnia, jaki minimalny zakres informacji o procesie przetwarzania danych należy przekazać osobie wyrażającej zgodę, aby była ona świadoma: tożsamość administratora i zamierzone cele przetwarzania,
- możliwe będzie zbieranie jednej zgody na przetwarzanie danych osobowych w kilku różnych celach.

Najważniejsze zmiany polegają jednak 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 nie będzie musiało 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.

Zazwyczaj brak możliwości kontynuowania przetwarzania, na podstawie dotychczasowych zgód, będzie wynikał przede wszystkim z niewyrażania zgody w sposób świadomy (np. oświadczenie: „Wyrażam zgodę na przetwarzanie danych osobowych zgodnie z Ustawą o ochronie danych osobowych", niewskazujące, komu zgoda jest udzielana i w jakim celu dane będą przetwarzane).

ZASTOSUJ!

CZTERY 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.

ZAPAMIĘTAJ!

RODO nie wymaga dochowania żadnej szczególnej formy wyrażenia zgody na przetwarzanie danych osobowych. Brak wymogu formy powoduje, że w praktyce zgoda może zostać udzielona w dowolny sposób. Zalecane jest jednak dochowanie formy pisemnej, która będzie miała znaczenie dla udowodnienia faktu wyrażenia zgody.

W odniesieniu do danych osobowych dotyczących uczniów niepełnoletnich trzeba pamiętać, że w świetle przepisów ustawy z 23 kwietnia 1964 r. – Kodeks cywilny regulujących kwestię zdolności do

czynności prawnych ewentualna zgoda uczniów na przetwarzanie danych czy wykorzystanie wizerunku jest nieważna, jeżeli nie ukończyli oni 13 lat (art. 14 § 1 Kodeksu cywilnego).

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.

ZAPAMIĘTAJ!

Artykuł 6 RODO określa katalog przesłanek warunkujących uznanie przetwarzania danych osobowych za zgodne z prawem.

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 (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 – jak realizować

Temat wyrażania zgody na przetwarzanie danych łączy się z tematem nowych uprawnień, jakie zyskały osoby, których dane są przetwarzane (rodzice, pracownicy przedszkola). Otóż prawo to polega na żądaniu od administratora niezwłocznego usunięcia danych osobowych (tzw. bycia zapomnianym). Żądanie to może zostać wysunięte w przypadku przedszkola 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 dysponuje inną podstawą prawną do ich przetwarzania.

Usuń wszystkie dane z sieci

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.

Przykład

PRZYKŁAD 9.

Przedszkole regularnie zamieszcza wpisy w sieci dotyczące pracy jednostki, prowadzi bogatą dokumentację fotograficzną. Na tę okoliczność regularnie pobierane są zgody na umieszczanie danych osobowych wychowanków w Internecie. Po 25 maja 2018 r. należy wprowadzić takie procedury, które pozwolą, w przypadku żądania osób, które chciałyby być „zapomniane", na:

- usunięcie w całości z systemu administratora,
- usunięcie z sieci wszystkich danych danego dziecka, rodzica, pracownika.

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.

A zatem administratorzy, a także podmioty przetwarzające dane na ich polecenie, będą musieli zmodyfikować metody postępowania z danymi osobowymi. 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, w imieniu którego 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.**

Te kwestie nie ulegną zmianie po wejściu w życie RODO. Odpowiedzialność jest bezpośrednia i powołanie inspektora ochrony danych osobowych czy wynajęcie firmy zewnętrznej w tym obszarze nie zwalnia z tej odpowiedzialności. Dyrektor odpowiada zarówno przed urzędem kontroli, jak i przed sądem cywilnym czy karnym. Nie może cedować tej odpowiedzialności na innych pracowników. Na administratorze ciąży odpowiedzialność prawna za wywiązanie się ze swoich obowiązków w związku z przetwarzaniem danych osobowych przez niego samego lub w jego imieniu.

ZAPAMIĘTAJ!

Dyrektor, jako przedstawiciel administratora danych, odpowiada za przetwarzanie danych. Formalnie administratorem jest jednostka – przedszkole, a dyrektor występuje w jej imieniu.

W RODO pojęcie „administrator danych" zostało zastąpione pojęciem „administrator". **Administratorem jest osoba fizyczna lub prawna, urząd publiczny, agenda lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych.**

Szesnaście 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.

Trzy nowości w zadaniach dyrektora

RODO przewiduje dla administratorów w przedszkolu 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 przedszkoli ten ostatni obowiązek został zastąpiony odpowiednią informacją zamieszczaną na stronie WWW jednostki, szerzej w dalszej części tekstu).

Obowiązek powołania inspektora ochrony danych

Najważniejszą zmianą z punktu widzenia przedszkola 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 przedszkola 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.

ZAPAMIĘTAJ!

Artykuł 37 RODO stanowi, że administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, m.in. zawsze gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów, w zakresie sprawowania przez nie wymiaru sprawiedliwości. Takim podmiotem jest publiczne przedszkole.

Proszę zwrócić uwagę, że RODO w art. 37 nie wskazuje bezpośrednio, iż administrator wyznacza inspektora w przedszkolu. Stanowi jedynie, że należy powołać inspektora, gdy przetwarzania danych dokonuje **organ** lub **podmiot publiczny**. Definicję „organów" i „podmiotów publicznych" znajdziemy w nowej ustawie o ochronie danych osobowych, która uzupełni tutaj przepisy RODO. I tak, w art. 4

projektu ustawy wskazano, że podmiotami publicznymi obowiązanymi do wyznaczenia inspektora są podmioty publiczne wskazane w art. 9 o finansach publicznych (m.in. samorządowe przedszkola). **A zatem nie ma żadnej wątpliwości, że każde samorządowe przedszkole publiczne (nawet najmniejsze) jest obowiązane powołać inspektora ochrony danych.**

Administrator danych (w imieniu przedszkola – 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 przedszkola).

Wzór 1. Procedura zgłaszania IOD do Prezesa UODO na stronie www.przedszkole.wip.pl

Powołanie inspektora ochrony danych nie oznacza nałożenia na niego pełnej odpowiedzialności za naruszenie i niezgodność działań organizacji z RODO. Obowiązek zapewnienia zgodności spoczywa na administratorze (art. 24 RODO), choć należy podkreślić kluczową rolę inspektora w tym procesie i znaczenie zapewnienia przez administratora gwarancji niezależności i rzeczywistych możliwości wykonywania zadań przez inspektora.

Inspektora ochrony danych będzie musiało powołać każde samorządowe przedszkole. W pozostałych przypadkach wyznaczenie inspektora ochrony danych jest fakultatywne. Przedszkola niesamorządowe i niepubliczne nie są jednostkami budżetowymi i nie zostały wskazane jako podmioty publiczne w rozumieniu przepisów RODO. Oznacza to, że w ich przypadku wyznaczenie inspektora jest nadal dobrowolne.

ABI zastąpi IOD

Na podstawie art. 134 projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych **każdy obecnie funkcjonujący w przedszkolu 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. w przedszkolu funkcjonuje ABI, staje się z mocy prawa IOD tylko na pewien czas – od 25 maja do 1 września 2018 r.

Takie rozwiązanie podyktowane zostało tym:

- **po pierwsze**, aby zapewnić ciągłość wykonywania funkcji, która ma gwarantować przestrzeganie zasad ochrony danych osobowych,
- **po drugie**, że zgodnie z RODO na inspektorów ochrony danych osobowych nałożone zostały znacznie większe wymagania niż te, które obecnie obowiązani są spełniać administratorzy bezpieczeństwa informacji – należy zweryfikować dotychczasowych ABI pod kątem nowych wymagań kwalifikacyjnych.

Zatem dyrektor przedszkola, 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 przedszkola (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).

RODO jasno precyzuje, że IOD może wykonywać inne zadania i obowiązki – oznacza to, iż przepisy wprost wskazują, że nie jest wyznaczany tylko do wykonywania obowiązków inspektora ochrony danych (art. 38 ust. 6 RODO). Zatem to administrator, podobnie jak obecnie, musi pamiętać, że ta osoba powinna spełniać określone ustawowo wymogi oraz mieć zapewnioną możliwość realizacji ustawowo nałożonych na nią zadań. Do dyrektora należy również rozstrzygnięcie, czy konkretny pracownik będzie w stanie pogodzić swoje obowiązki z obowiązkami wynikającymi z pełnienia funkcji IOD.

Przykład

PRZYKŁAD 10.

Czy IOD może być nauczycielem? Teoretycznie tak, jednak należy liczyć się z tym, że nauczyciel nie pogodzi dodatkowych obowiązków z pracą dydaktyczną, wychowawczą i opiekuńczą, jest także inaczej usytuowany organizacyjne, niż wymaga tego RODO. Lepszym rozwiązaniem wydaje się wyznaczenie pracownika niepedagogicznego, a optymalnym − utworzenie nowego stanowiska niepedagogicznego dla inspektora (nawet na część etatu).

Inspektor może być pracownikiem samorządowym

Inspektor ochrony danych może wykonywać inne zadania i obowiązki, pod warunkiem że administrator zapewni takie warunki pracy, by dodatkowe zadania i obowiązki nie powodowały konfliktu interesów (art. 38 ust. 6 RODO). Zatem może to być pracownik, który w ramach stosunku pracy będzie wykonywał różne zadania, w tym zadania IOD. Na podstawie powyższego należy sobie odpowiedzieć na pytanie, jaki będzie charakter wykonywanych czynności przez inspektorów oraz jaki rodzaj relacji ma łączyć inspektora z przedszkolem, na rzecz którego ma działać. Jest to kluczowe, gdyż jeśli ta relacja będzie miała cechy charakterystyczne dla stosunku pracy, to należy zawrzeć umowę o pracę (art. 22 § 1 Kodeksu pracy).

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 przedszkolu 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 ochrony danych nie jest odwoływany ani karany przez dyrektora za wypełnianie swoich zadań.

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

Zgodnie z tym dokumentem niezbędny poziom fachowej wiedzy inspektora należy oceniać stosownie do prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe (punkt 97 preambuły RODO). Wobec tego wiedza musi być współmierna do charakteru, skomplikowania i ilości przetwarzanych danych. Wyboru inspektora należy dokonać z zachowaniem należytej staranności. Fachowość inspektorów wyeksponowano przez zobowiązanie administratorów danych i podmiotów przetwarzających do zapewnienia inspektorom zasobów niezbędnych do utrzymania wysokiego i aktualnego poziomu wiedzy (art. 38 ust. 2 RODO).

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.

Przy ocenie umiejętności realizacji zadań uwzględnia się ich charakter i zakres. Proszę zauważyć, że inspektor będzie miał obowiązek identyfikowania obowiązków oraz doradzania administratorowi i podmiotowi przetwarzającemu (w tym kierownictwu i wszystkim osobom przetwarzającym dane).

Trzeba podkreślić, że obecnie brak jest przepisu, który precyzuje, jakie konkretne wymagania stawiane są inspektorom. Kwalifikacje zawodowe determinowane będą przede wszystkim skalą przetwarzania danych osobowych. RODO nie określa, w jaki sposób weryfikowane będą wymogi stawiane inspektorom, ani nie stawia warunku przedstawienia przez inspektora jakichkolwiek dokumentów potwierdzających jego wiedzę (nawet certyfikatów ze szkoleń).

Tym samym to w szczególności na dyrektorze przedszkola będzie ciążyć odpowiedzialność za wybór na stanowisko inspektora osoby posiadającej wystarczającą wiedzę i umiejętności w dziedzinie ochrony danych osobowych.

Stopień skomplikowania, charakter oraz liczba przetwarzanych danych w przedszkolu nie wymagają, by osoba pełniąca funkcję inspektora ukończyła studia podyplomowe z zakresu ochrony danych osobowych. Odbycie przez inspektora szkolenia organizowanego dla celów przygotowania do pełnienia tego stanowiska w przedszkolu, uzupełniane regularnym aktualizowaniem wiedzy z zakresu ochrony danych osobowych, spełnia wymagania stawiane przez prawo unijne co do kwalifikacji zawodowych inspektora ochrony danych.

Przykład

PRZYKŁAD 11.

Przedszkole chce powierzać dalej funkcję inspektora obecnemu ABI. To dyrektor musi ocenić, czy powoływana osoba rzeczywiście dysponuje kwalifikacjami zawodowymi w zakresie ochrony danych osobowych, np. ukończyła studia podyplomowe, szkolenia, czy ma odpowiednią fachową wiedzę i doświadczenie. Chodzi o to, żeby była pewność, że powierza funkcję IOD osobie kompetentnej.

Jeden IOD dla kilku przedszkoli

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 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 również w przedszkolu, 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. Więcej informacji na str. XX.

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 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.

Zawiadamianie osoby o naruszeniu jej danych

W przypadku przedszkoli ten obowiązek (art. 34 RODO) został ograniczony na podstawie zmian w ustawie Karta Nauczyciela 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).

RODO określa minimum informacji, które powinny znaleźć się w zgłoszeniu naruszenia organowi nadzorczemu. Zgodnie z nimi zgłoszenie musi:

- opisywać charakter naruszenia, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

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 przedszkolach będzie spoczywał obowiązek udowodnienia, że przestrzegają regulacji.

ZAPAMIĘTAJ!

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

Nie sposób sobie jednak wyobrazić, że przedszkole 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.

ZASTOSUJ!

Warto świadomie wykorzystać już istniejącą dokumentację w przedszkolu. Pozwoli łatwiej przygotować się do zmian i uniknąć wprowadzania naraz zbyt wielu dokumentów.

Nowe obowiązki to poważne wyzwanie dla administratora ze względu na brak gotowych rozwiązań/regulacji. RODO nie wskazuje wprost, jakie dokumenty, procedury i polityki należy wdrożyć. Ogólnie wspomina, że to podmiot musi się wykazać starannością w zabezpieczeniu tych procesów, aby podczas przetwarzania danych osobowych nie doszło do nieprawidłowości. Chociaż dotychczasowe rozporządzenia, na podstawie których przygotowano przedszkolne dokumenty dotyczące ochrony danych osobowych, stracą moc, warto na ich podstawie opracować nowe.

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.

Po raz pierwszy pojęcie upoważnienia pada w art. 4 pkt 10 RODO. Przepis ten zawiera definicję podmiotu określonego jako „strona trzecia". Jest to m.in. osoba fizyczna (bo mogą to być też inne kategorie podmiotów) inna niż m.in. osoba (bo i tu przepis wymienia inne kategorie podmiotów), która, z upoważnienia administratora lub podmiotu przetwarzającego, może przetwarzać dane osobowe. **Strona trzecia to zatem człowiek inny niż ten, który przetwarza dane osobowe z upoważnienia administratora lub podmiotu przetwarzającego.**

O upoważnieniu dowiadujemy się z art. 29 RODO. Stanowi on, że każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora. **Powołany przepis potwierdza istnienie obowiązku nadawania upoważnień do przetwarzania danych osobowych.** Z przepisu wynika również konieczność zadbania o to, by dostęp do danych osobowych miały wyłącznie osoby, którym dyrektor nadał upoważnienie.

Zasady nadawania, zmiany, odwołania upoważnień nadal mogą zostać określone w polityce bezpieczeństwa (równocześnie jest to jeden ze stosowanych przez administratora danych środków organizacyjnych mających na celu zapewnienie poufności informacji). Warto jednak obecne zapisy zweryfikować i odnieść do RODO, a nie art. 37 ustawy o ochronie danych osobowych.

Zatem w dalszym ciągu dostęp do danych osobowych w przedszkolu mogą mieć wyłącznie osoby uprawnione – upoważnione, czyli tacy pracownicy (nauczyciele i niepedagogiczni), którzy wykonują swoje obowiązki służbowe na stanowisku związanym z przetwarzaniem danych – patrz wzór 2.

Wzór 2. Procedura nadawania uprawnień do przetwarzania danych osobowych pobrana na stronie www.przedszkole.wip.pl

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 przede wszystkim chodzi o ten pierwszy przypadek.

ZAPAMIĘTAJ!

Przedszkole 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.

Warto porównać art. 13 i 14 RODO i art. 24 i 25 obecnej ustawy o ochronie danych osobowych.

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.

Do niezbędnych elementów informacyjnych od osoby, od której pozyskuje się dane, należy zaliczyć podanie (art. 13 ust. 1 i 2 RODO):

- tożsamości administratora, danych kontaktowych (pełnej nazwy przedszkola, NIP, REGON, adresu siedziby, numeru telefonu, faksu, poczty elektronicznej, formularza kontaktowego na stronie internetowej),
- danych kontaktowych inspektora ochrony danych (imienia i nazwiska, adresu, numeru telefonu, adresu poczty elektronicznej),
- celu przetwarzania danych osobowych oraz podstawy prawnej przetwarzania (wskazanie jednej z przesłanek legalizujących przetwarzanie danych, określonych w art. 6 ust. 1 RODO lub art. 9 ust. 1 RODO),
- obowiązku wskazania prawnie uzależnionych interesów realizowanych przez administratora, jeżeli przetwarzanie danych następuje na podstawie tej przesłanki,
- informacji o odbiorcach danych osobowych (oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe) lub o kategoriach odbiorców,
- informacji o zamiarze transferu danych osobowych do państwa trzeciego (gdy ma to zastosowanie),
- okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu,
- informacji o prawie do żądania od administratora dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania bądź o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO (na podstawie zgody) – informacji o prawie do cofnięcia zgody w dowolnym momencie bez

wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

- informacji o prawie wniesienia skargi do organu nadzorczego,
- informacji, czy podanie danych jest wymogiem ustawowym/umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Jeżeli pozyskujemy dane w sposób pośredni od innych podmiotów, oprócz powyższych informacji należy podać (art. 14 RODO):

- źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych,
- informacje o kategoriach danych osobowych, które są przetwarzane – a więc rodzaju przetwarzanych danych (np. imię, nazwisko, adres, data urodzenia itd.).

W art. 12 RODO ustawodawca opisał, w jakiej formie obowiązek ten ma zostać spełniony. **Przekazywana informacja w swojej treści, poza jej prostotą i jasnością przekazu, ma być zwięzła, przejrzysta, zrozumiała i dostępna w łatwej formie.** RODO dopuszcza różne formy przekazu wymaganych informacji o przetwarzaniu danych. Poza powszechną formą pisemną w grę wchodzi również forma elektroniczna, a także forma ustna – gdy takie jest żądanie wnioskodawcy, o ile innymi sposobami potwierdzi on swoją tożsamość.

Wzór 3. Klauzula informacyjna na stronie www.przedszkole.wip.pl

Zabezpiecz dane osób upoważnionych do odbioru dziecka

Przepisy nie wskazują, w jaki sposób zapewnić bezpieczeństwo danych osobowych. Tutaj należy stosować zasady ustalone w stosunku do pozostałych danych osobowych dzieci, rodziców i pracowników. Powinno się ustalić na podstawie zapisów statutowych w przedszkolu, jakie dane osobowe wymagane są przy upoważnianiu do odbioru wychowanków. **Po 25 maja 2018 r. dyrektorzy będą musieli prowadzić wewnętrzny rejestr czynności przetwarzania danych** (art. 30 ust. 1 RODO). W tym rejestrze trzeba będzie ująć osoby upoważnione do obioru dzieci. Następnie należy ustalić:

- jakie dane osobowe są pozyskiwane od osób, które mogą odbierać dzieci,
- w jakim celu są pozyskiwane dane,
- komu dane będą przekazywane (jeżeli będą),
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (np. że upoważnienia są przechowywane w sekretariacie w zamykanej szafce, do której dostęp ma tylko osoba upoważniona),
- termin, w którym te dane będą przetwarzane i kiedy będą usunięte (np. dane przetwarzane w roku szkolnym 2018/2019 do dnia X następnie zostaną usunięte w sposób ustalony w odpowiedniej procedurze).

CZĘŚĆ III – SANKCJE ZA NARUSZENIE PRZEPISÓW W 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).

1. Ogólne warunki nakładania kar pieniężnych

Przy ustaleniu wysokości kary organ nadzorczy będzie brał pod uwagę (art. 83 RODO):

1) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody,

2) umyślny lub nieumyślny charakter naruszenia,

3) działania podjęte przez administratora w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą,

4) stopień odpowiedzialności administratora z uwzględnieniem środków technicznych i organizacyjnych przez niego wdrożonych,

5) wszelkie wcześniejsze naruszenia ze strony administratora,

6) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków,

7) kategorie danych osobowych, których dotyczyło naruszenie,

8) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności czy i w jakim zakresie administrator zgłosił naruszenie,

9) jeżeli wobec administratora, którego sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie uprawnienia naprawcze, a jeśli tak, czy podmiot się do nich zastosował,

10) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji,

11) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy.

Postępowanie w sprawie naruszenia przepisów

Prezes UODO może działać z własnej inicjatywy, jak również w wyniku skarg osób pokrzywdzonych. W przypadku odnotowania skargi Prezes UODO może np.:

- nałożyć karę finansową,
- udzielić upomnienia,
- nakazać ograniczenie przetwarzania danych przez administratora.

Nie zdecydowano się na odgórne ustalenie maksymalnych terminów na rozpatrywanie skarg.

Postępowanie kontrolne

Do tej pory przebieg postępowania kontrolnego nie był uregulowany w przepisach zbyt szczegółowo. W nowej ustawie o ochronie danych osobowych dodano cały szereg przepisów mających zagwarantować zarówno skuteczność kontroli, jak i prawa osobom, które podlegają kontroli. Ustawowo zagwarantowano też, że kontrola może trwać maksymalnie 1 miesiąc. Do tej pory zdecydowana większość kontroli GIODO była zapowiadana, jednak przepisy nie regulowały tej materii wprost.

Uproszczenie postępowania przed UODO

Zamysłem ustawodawcy jest przyspieszenie i uproszczenie postępowania przed UODO. Warto zauważyć, że postępowanie dotyczące ochrony danych osobowych pozostało dalej we właściwości sądów administracyjnych, tym samym dalej odbywa się ono na gruncie przepisów Kodeksu postępowania administracyjnego (k.p.a.) oraz Kodeksu postępowania przed sądami administracyjnymi (p.p.s.a.). Sądy administracyjne posiadają bogate orzecznictwo oraz doświadczenie w rozpatrywaniu spraw dotyczących ochrony danych osobowych. Istotną zmianą ma być natomiast zrezygnowanie z dwuinstancyjności postępowania przed Urzędem Ochrony Danych Osobowych. Jedyną formą odwołania się od decyzji UODO na gruncie projektu ustawy o ochronie danych będzie więc droga sądowoadministracyjna

Za złamanie przepisów kara do 100 tys. zł

Konieczność wyposażenia Prezesa UODO w możliwość nakładania kar finansowych wynika wprost z treści RODO. Ściągane kary będą stanowiły dochód budżetu państwa.

Poza nakładaniem kar finansowych do kwoty 20.000.000 euro lub do 4% całkowitego rocznego obrotu Prezes UODO:

- kieruje wystąpienia do organów publicznych, zmierzające do zapewnienia skutecznej ochrony danych osobowych,
- przygotowuje wykaz operacji na danych osobowych, wymagających sporządzenia oceny skutków, i publikuje go na swojej stronie internetowej (należy śledzić te ustalenia),
- prowadzi system teleinformatyczny, za pomocą którego będzie można zgłaszać naruszenia ochrony danych osobowych (w ciągu 72 godzin od naruszenia).

ZAPAMIĘTAJ!

Kary dla administracji publicznej, w tym przedszkoli, za złamanie przepisów o ochronie danych osobowych zostały obniżone do 100 tys. zł (art. 83 ust. 1 projektu ustawy o ochronie danych osobowych).

4. Ograniczenie odpowiedzialności karnej

Do tej pory postępowania karne prowadzone w sprawie naruszenia przepisów ustawy o ochronie danych osobowych były bardzo rzadkie i mało skuteczne. Jednocześnie ponoszenie

odpowiedzialności karnej wydawało się nieadekwatnie dotkliwą sankcją. Zwłaszcza że przepisy były w wielu obszarach mało precyzyjne.

Przykład

PRZYKŁAD 12.

Niezgłoszenie bazy danych do GIODO obecnie wciąż jest uznawane za przestępstwo (art. 53 UODO). Jednak samo pojęcie zbioru danych osobowych jest pojęciem nieostrym. Może być interpretowane na różne sposoby. Oczywiście GIODO w zdecydowanej większości przypadków nie angażował w takich sytuacjach prokuratury. Wskazywał jedynie brak rejestracji jako uchybienie i wzywał do zgłoszenia bazy. Nie zmienia to faktu, że literalnie rzecz ujmując, przestępstwo zostało popełnione.

Pojawiły się zaledwie dwa przepisy karne (wcześniej było sześć przepisów). To, co dziś jest przestępstwem, a odnosi się do udaremnienia lub utrudnienia inspektorowi GIODO czynności kontrolnej, zostanie w nowym systemie prawnym wykroczeniem i będzie podlegać grzywnie. Natomiast z pozostałych pięciu obowiązujących obecnie przestępstw ustawodawca chce wprowadzić wyłącznie jedno przestępstwo. Jego przedmiotem będzie przetwarzanie, bez podstawy prawnej, danych osobowych kategorii szczególnej (m.in. dane osobowe ujawniające poglądy polityczne, przekonania religijne, przynależność do związków zawodowych, przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia). Będzie to skutkować pozbawieniem wolności do roku. Wydaje się, że takie podejście zostało podyktowane wprowadzonymi przez RODO wysokimi karami finansowymi i skierowaniem ciężaru, gwarantującego legalne przetwarzanie danych, na aspekty finansowe.

5. NOWOŚĆ: odpowiedzialność cywilna

Istotnym novum w stosunku do przepisów aktualnej ustawy o ochronie danych osobowych są zapisy o odpowiedzialności cywilnej. Zapewniają one niezależną (wobec trybu postępowania administracyjnego przed Prezesem UODO) drogę dochodzenia roszczeń z tytułu naruszeń przepisów o ochronie danych osobowych.

Na podstawie tych przepisów osoba, której dane osobowe zostały naruszone, będzie mogła wystąpić z pozwem przeciwko temu, kto dopuścił się takiego naruszenia. Właściwymi do rozpoznawania takich spraw mają być sądy okręgowe.

CZĘŚĆ IV – WDRAŻANIE RODO KROK PO KROKU – PRAKTYCZNY PRZEWODNIK

Poniżej znajdziesz najważniejsze zadania, które pozwolą Ci przygotować się do RODO. Pamiętaj, że RODO musi być stosowane od 25 maja 2018 r. i do tej daty trzeba przygotować placówkę.

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 przedszkolu jest ABI, to on, wspólnie z dyrektorem, powinien przygotować przedszkole 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 – patrz wzór 1. 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.

Tworząc harmonogramy poszczególnych dni sprawdzeń, warto pamiętać o przerwach oraz pozostawieniu pewnego marginesu czasowego.

Wzór 4. Przykładowy harmonogram wdrożenia RODO na stronie www.przedszkole.wip.pl

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.

Grupa Robocza planuje wydawanie dalszych wytycznych, lecz terminy ich publikacji nie są bliżej określone. Warto także wspomnieć, że Grupa Robocza przekształci się z 25 maja 2018 r. w Europejską Radę Ochrony Danych.

Kolejnym źródłem informacji jest strona internetowa GIODO (**www.giodo.gov.pl**). Można na niej znaleźć informacje o wydarzeniach, takich jak warsztaty, konferencje i szkolenia. W zakładce „Prawo" znajdują się zarówno informacje dotyczące reformy ochrony danych osobowych (w sekcji Reforma przepisów), jak i treść nowych przepisów RODO (w sekcji Przepisy prawa). W tej samej zakładce dostępne są też pozostałe, obowiązujące w zakresie ochrony danych osobowych akty prawne (m.in. krajowe). Na tej stronie można ponadto znaleźć pozostałe informacje i wskazówki co do wdrażania nowych zasad. Materiały są na bieżąco aktualizowane i rozszerzane.

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 przedszkola powinien ocenić, czy bezpieczeństwo danych osobowych jest zapewnione na odpowiednim poziomie.

Aby ułatwić pracę, zamieszczamy przykładowe narzędzia pomocne przy wdrażaniu RODO. Można je odpowiednio zmodyfikować do własnych potrzeb – patrz wzór 5.

Wzór 5. Checklista kontrolna zgodności z RODO na stronie www.przedszkole.wip.pl

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.

ZAPAMIĘTAJ!

Certyfikację zrealizuje Prezes UODO

Dostępne będą mechanizmy certyfikacji oraz znaki jakości i oznaczeń mające świadczyć o zgodności z RODO. Dyrektor przedszkola będzie mógł ubiegać się o nadanie takiego certyfikatu. Prezes UODO będzie opracowywał i udostępniał kryteria certyfikacji. Uzyskanie certyfikatu nie będzie darmowe. Podmiot wnioskujący będzie uiszczał opłatę w wysokości około 12 tys. zł, co stanowi odpowiednik trzykrotności przeciętnego miesięcznego wynagrodzenia za pracę. Certyfikaty ma nadawać Prezes UODO (obecny GIODO). Postępowanie certyfikacyjne będzie możliwe do przeprowadzenia zdalnie w formie elektronicznej.

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 przedszkolu, 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 w przedszkolu. 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 funkcjonujących w przedszkolu

Jeżeli masz politykę bezpieczeństwa przetwarzania danych osobowych, to załącznikiem do niej powinien być wykaz zbiorów danych osobowych funkcjonujących w przedszkolu. Zastanów się, czy w tym wykazie znajdują się wszystkie zbiory danych osobowych – patrz wzór 6.

Wzór 6. Wykaz zbiorów danych osobowych na stronie www.przedszkole.wip.pl

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.

ZASTOSUJ!

DWA ZADANIA DO WYKONANIA

1) dokonaj przeglądu zbiorów danych z punktu widzenia: ilości oraz zakresu znajdujących się w nich danych, czasu ich przechowania, lokalizacji, w których dane się znajdują,

2) zweryfikuj zapisy Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemami Informatycznymi w zakresie zgodności z RODO.

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 – patrz wzór 7:

- 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.

Co prawda z RODO wprost nie wynika, że przedszkole jest zobowiązane do prowadzenia tego rejestru, ale pozwoli to zorientować się, jakiego rodzaju dane, jakich podmiotów, w jakim celu, na jakiej podstawie prawnej są gromadzone dane.

Wzór 7. Rejestr czynności przetwarzania danych osobowych na stronie www.przedszkole.wip.pl

Jeżeli nie masz polityki bezpieczeństwa oraz wykazu zbiorów danych osobowych, to w ramach przygotowywanego dokumentu związanego z ochroną danych osobowych uwzględnij informacje o wszystkich swoich zbiorach danych osobowych, kierując się wytycznymi co do zawartości rejestru czynności przetwarzania danych osobowych zawartymi w art. 30 RODO.

Jeżeli w ramach któregoś ze zbiorów stwierdzisz, że podstawą przetwarzania jest zgoda, to upewnij się, czy masz odnotowaną taką zgodę użytkownika i czy jej treść odpowiada wymogom stawianym przez RODO (art. 13 RODO). W sytuacji gdyby zgoda okazała się odebrana wadliwie, zaplanuj procedurę uzyskania zgody jeszcze raz, tym razem już poprawnej i odpowiadającej wymogom RODO.

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 były precyzyjnie określone.

Przepisy RODO wspominają o umowie lub innym instrumencie prawnym, który wskazuje: przedmiot i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także jaki jest cel przetwarzania informacji (art. 28 RODO). Zatem nie jest to nowy standard, ale należy skontrolować zawarte z podwykonawcami umowy pod kątem wymagań nowych przepisów (np. w związku z prowadzeniem dziennika elektronicznego).

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. Wdróż takie zabezpieczenia techniczne czy organizacyjne, by tylko osoby upoważnione mogły uzyskać dostęp do danych

osobowych i je przetwarzać. 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).

ZASTOSUJ!

Jeżeli zdajesz sobie sprawę z rozszerzonego obowiązku informacyjnego, to zastanów się, w jaki sposób wypełnisz go w stosunku do osób, których dane już znajdują się w przedszkolu, i do tych, których dane dopiero będziesz pozyskiwał.

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.

Wziąwszy pod uwagę prawa osób, których dotyczą przetwarzane przez placówkę dane, przygotowując się do stosowania przepisów ogólnego rozporządzenia o ochronie danych, osoby odpowiedzialne w placówce oświatowej za wdrożenie RODO powinny podjąć działania, by ustalić:

- które z praw i w jakim zakresie będą przysługiwały osobom, których dotyczą dane,
- które z praw oraz wynikające z tych praw obowiązki zostały ograniczone (odpowiedzi należy szukać w nowych przepisach Karty Nauczyciela, ustawy o systemie oświaty czy ustawy Prawo oświatowe – projekt ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych),
- kto, w jakim zakresie i w jaki sposób będzie realizował obowiązki wynikające z praw osób, których dotyczą dane.

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.

Przeprowadzenie analizy ryzyka będzie obowiązkowe przed podjęciem działań „wysokiego ryzyka", takich jak np.: przetwarzanie danych dzieci, danych wrażliwych (art. 35, 36, 39 RODO). Analiza ryzyka powinna zapewnić wykazanie się starannością co do poprawności przetwarzania danych, szczególnie przed organem nadzorczym w momencie kontroli.

Proponuję opracować checklistę punktów kontrolnych i okresowo dokonywać sprawdzeń.

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). Pojęcie „naruszenie ochrony danych osobowych" zasługuje na szczególną uwagę w związku z tym, że zostało zdefiniowane jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

ZAPAMIĘTAJ!

Nie trzeba będzie zgłaszać naruszeń do organu nadzorczego, jeśli dyrektor przedszkola 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 – patrz wzór 8.

Wzór 8. Zgłoszenie naruszenia ochrony danych osobowych Prezesowi UODO na stronie www.przedszkole.wip.pl

Nie trzeba jednak zgłaszać każdego naruszenia. RODO wprowadza tutaj pewne kryterium, z pomocą którego możesz ustalić, czy zdarzenie zgłaszać, czy nie. Chodzi o ocenę prawdopodobieństwa naruszenia praw lub wolności osób, które dane przetwarzasz (art. 33 ust. 1 RODO). Zatem to administrator, w praktyce inspektor ochrony danych, powinien ustalić w procedurze, na podstawie jakich kryteriów kwalifikować dane naruszenie jako naruszenie prawa i wolności osób.

Wzór 9. Elementy wewnętrznej procedury postępowania w przypadku naruszenia ochrony danych na stronie www.przedszkole.wip.pl

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 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 – patrz wzór 10.

Wzór 10. Komunikat o naruszeniu ochrony danych na stronie www.przedszkole.wip.pl

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 zostało częściowo ograniczone – patrz tabela 5.

Tabela 5. 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
Art. 14	

	systemie oświaty.
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.

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 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.

Listy kontrolne pomocne przy wdrażaniu zmian

Aby ułatwić pracę, proponujemy skorzystanie z przykładowych narzędzi pomocnych przy wdrażaniu RODO.

Na stronie www.przedszkole.wip.pl:

Wzór 11. Lista kontrolna – jak zapoznać pracowników z RODO.

Wzór 12. Lista kontrolna – jak powierzyć przetwarzanie danych osobowych zgodnie z RODO.

Wzór 13. Lista kontrolna – w jaki sposób jako administrator będziesz musiał realizować prawa osób, których dane dotyczą, zgodnie z RODO.

Wzór 14. Lista kontrolna – jakie wymogi musi spełniać klauzula zgody na przetwarzanie danych osobowych zgodnie z RODO.

Wzór 15. Lista kontrolna – jak będzie trzeba prowadzić rejestr czynności przetwarzania danych i rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

Wzór 16. Lista kontrolna – jak zmodyfikować klauzule obowiązku informacyjnego, by były zgodne z RODO.

Podstawa prawna:

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).

Autor: Dariusz Skrzyński prawnik, specjalista prawa oświatowego i autorskiego