RODO – sprawdzam.
Wyzwania w zakresie ochrony danych osobowych w szkolnictwie po 25 maja 2018 r.

Paweł Żywicki
Departament Społeczeństwa Informacyjnego
Urząd Marszałkowski Województwa Warmińsko – Mazurskiego w Olsztynie

Olsztyn, 24 marca 2018 r.

RODO – Informacje ogólne

Co to jest RODO

- RODO lub GDPR to skrót od Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
- Jest to akt prawny przyjęty przez Unię Europejską regulujący zasady ochrony danych osobowych, który zastępuje dotychczas obowiązującą dyrektywę 95/46/WE z 1995 r.
- RODO tym się różni od dyrektywy 95/46/WE, że nie będzie implementowane, czyli nie będzie trzeba przepisów RODO przyjąć w polskiej ustawie, jak to się dzieje w przypadku dyrektyw.
- RODO obowiązuje bezpośrednio tzn., że będzie **bezpośrednio stosowane i bezpośrednio skuteczne**.
- RODO zastąpi obowiązującą obecnie ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych.

Kto podlega RODO? (1)

- RODO podlega każdy podmiot, który przetwarza dane osobowe w sposób zautomatyzowany, częściowo zautomatyzowany lub przetwarza w sposób inny niż zautomatyzowany dane osobowe stanowiące część zbioru danych lub mające stanowić część zbioru danych.
- RODO odnosi się praktycznie do każdego podmiotu, który prowadzi działalność w Unii Europejskiej i nie podlega wyłączeniu określonemu w art. 2 ust. 2 Rozporządzenia.
- Wyłączenie obejmuje:
  - działalność nieobjętą zakresem prawa Unii,
  - działania osoby fizycznej w ramach czynności o czysto osobistym lub domowym charakterze,
  - działania organów właściwych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom (sądy, prokuratura, policja).

Kto podlega RODO? (2)

- RODO **nie znajduje** zastosowania do działalności osobistej lub domowej. To oznacza, że osoba fizyczna prowadząca działalność gospodarczą musi stosować RODO do danych osobowych swoich klientów, czy pracowników, ale nie stosuje RODO do danych przetwarzanych w celach czysto prywatnych, np. do danych adresatów w związku z wysyłanymi corocznie kartkami „na święta”.
- RODO dotyczy „prawie wszystkich” - zarówno małych, średnich przedsiębiorców, dużych koncernów, jak i jednostek samorządu terytorialnego oraz urzędów, a także jednostek budżetowych w rozumieniu ustawy o finansach publicznych (np. szkoły).

Data wejścia w życie i data stosowania RODO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ODLICZAMY DNI DO **RODO**

61 dni 15 godzin 59 minut 50 sekund

- Data wejścia w życie RODO – 24 maja 2016 r.
- Data rozpoczęcia stosowania przepisów RODO - 25 maja 2018 r.
- Motyw nr 171 preambuły do RODO stanowi, iż „przetwarzanie, które w dniu rozpoczęcia stosowania RODO już się toczy, powinno w terminie dwóch lat od wejścia rozporządzenia w życie zostać dostosowane do jego przepisów”.

WARMIA MAZURY®

Dane osobowe i podstawy ich przetwarzania w szkolnictwie

Czym są dane osobowe

- **Dane osobowe** są to wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, niezależnie od tego, w jakiej formie informacje te są przetwarzane (papierowej lub cyfrowej).
- **Osobą zidentyfikowaną** jest taka osoba, której tożsamość znamy i którą możemy wskazać spośród innych osób. Przykładem jest nauczyciel, zatrudniony w szkole, którego dane osobowe przetwarza Administrator jego danych, czyli szkoła.
- **Osobą możliwą do zidentyfikowania** jest taka osoba, której tożsamości nie znamy, ale możemy poznać, korzystając z tych środków, którymi dysponujemy. Przykładem jest nadawca listu poleconego, którego tożsamość może poznać pracownik poczty na podstawie numeru przesyłki.

Kategorie danych osobowych

- Wyróżnia się dwie kategorie danych osobowych:
  - **Dane osobowe zwykłe** – wszystkie dane osobowe nie będące danymi szczególnie chronionymi.
  - **Dane osobowe zaliczające się do szczególnie chronionych kategorii danych** (dawniej zwane danymi wrażliwymi). Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia lub orientacji seksualnej.
- Danymi osobowymi mogą być zatem nie tylko imię i nazwisko, płeć czy numer PESEL (dane zwykłe), ale też adres e-mail, adres IP, dane o geolokalizacji, kod genetyczny, poglądy polityczne, a nawet historia zakupów.

Podstawy przetwarzania danych osobowych w szkolnictwie (1)

- Przetwarzanie danych osobowych w rozumieniu RODO i obecnie obowiązującej ustawy oznacza wszelkie operacje wykonywane na danych osobowych, w szczególności:
  - zbieranie danych osobowych,
  - utrwalanie danych osobowych,
  - przechowywanie danych osobowych,
  - usuwanie danych osobowych,
  - opracowywanie danych osobowych,
  - udostępnianie danych osobowych,
  - operacje na danych osobowych wykonywane w systemach IT.
- Każda operacja przetwarzania danych osobowych wymaga wykazania odpowiedniej podstawy prawnej, do której - z punktu widzenia RODO - zaliczamy: zgodę osoby, której dane dotyczą, odpowiednie obowiązki wynikające z przepisów prawa, konieczność realizacji zawartej umowy, a nawet dobro publiczne.

Podstawy przetwarzania danych osobowych w szkolnictwie (2)

- Co do zasady szkoła jako Administrator danych i Dyrektor szkoły, który ją reprezentuje przetwarza dane osobowe dzieci, rodziców, nauczycieli i innych pracowników na podstawie **przepisów prawa,** które w sposób szczególny regulują różne aspekty funkcjonowania systemu oświaty. Podstawą przetwarzania danych osobowych w szkole są zatem przepisy:
  - ustawy z dnia 7 września 1991 r. o systemie oświaty,
  - ustawy z dnia 26 stycznia 1982 r. Karta Nauczyciela,
  - ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej,
  - akty wykonawcze do ww. ustaw np. rozporządzenie Ministra Edukacji Narodowej z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji.
- Bywa jednak, że pojawi się konieczność przetwarzanie większej ilości danych dzieci lub ich rodziców. Wtedy przetwarzanie na podstawie ustawy jest niewystarczające, a podstawę przetwarzania stanowić musi – **zgoda** (przykładem jest uzyskanie numer telefonu do rodzica w celu umożliwienia łatwiejszego kontaktu lub umieszczenie wizerunku dzieci na stronie internetowej).

Nowe instrumenty prawne i wyzwania w zakresie ochrony danych osobowych po 25 maja 2018 r.

Wyznaczenie Inspektora Ochrony Danych Osobowych (IODO) (1)

- Administrator lub podmiot przetwarzający dane wyznaczają IODO zawsze, gdy:
  - przetwarzania dokonują organ lub podmiot publiczny (z wyjątkiem podmiotów sprawujących wymiar sprawiedliwości),
  - dane przetwarzane są na dużą skalę i dotyczą szczególnych kategorii danych osobowych,
  - działania oparte są na monitorowaniu osób.
- Jeżeli Administrator lub podmiot przetwarzający dane są **organem lub podmiotem publicznym** (np. szkoła) dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego Inspektora ochrony danych osobowych.
- Inspektor jest wyznaczany na podstawie kwalifikacji zawodowych, wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych osobowych.

Wyznaczenie Inspektora Ochrony Danych Osobowych (IODO) (2)

- Inspektor może być członkiem personelu Administratora lub wykonywać zadania na podstawie umowy o świadczenie usług, jednakże **nie może** otrzymywać instrukcji dotyczących wykonywanych zadań **(ma być niezależny)**, a jego dane winny być upublicznione **(punkt kontaktowy)**.
- Zakres obowiązków IODO reguluje art. 39 RODO – w skrócie dotyczą one monitorowania wewnętrznego przestrzegania wymogów RODO.
- Zgodnie z założeniami nowego Projektu Ustawy o ochronie danych osobowych dotychczasowi Administratorzy Bezpieczeństwa Informacji (o ile byli powołani) z dniem 25 maja 2018 r. rozpoczynają pełnienie funkcji IODO.

Stworzenie rejestrów czynności przetwarzania danych osobowych (1)

- Od 25 maja 2018 r. zniesiony zostaje obowiązek zgłaszania zbiorów danych osobowych do organu nadzorczego (obecny GIODO). W przypadku szkół obowiązek ten był ograniczony jeśli powołany był ABI.
- Zamiast tego każdy podmiot przetwarzający dane osobowe ma obowiązek dokumentować czynności związane z przetwarzaniem danych osobowych.
- RODO nakłada na Administratorów, w tym **podmioty publiczne – także szkoły,** obowiązek prowadzenia tzw. **Rejestru czynności przetwarzania danych osobowych.**
- Rejestr czynności przetwarzania danych osobowych prowadzi i aktualizuje IODO.
- Administrator danych osobowych ma obowiązek udostępniać Rejestr na każde żądanie organu nadzorczego.

Stworzenie rejestrów czynności przetwarzania danych osobowych (2)

- Rejestr czynności przetwarzania danych osobowych powinien zawierać co najmniej:
  - Dane Administratora i IODO,
  - Podstawę prawną przetwarzania danych osobowych,
  - Cel przetwarzania danych osobowych,
  - Komu i kiedy dane zostały udostępnione,
  - Opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
  - O ile to możliwe – terminy usunięcia danych osobowych oraz opis technicznych i organizacyjnych środków zastosowanych by przetwarzanie było bezpieczne.

Obowiązek zgłaszania naruszeń ochrony danych

- W przypadku zaistnienia **incydentu bezpieczeństwa** zwanego w RODO **naruszeniem ochrony danych osobowych,** administrator bez zbędnej zwłoki – w miarę możliwości, ale nie później niż w terminie 72 h po stwierdzeniu naruszenia – ma obowiązek zgłosić je do organu nadzorczego.
- Dodatkowo, o ile naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia również osobę, której dane dotyczą, o takim naruszeniu.
- Realizacja obowiązku będzie wymagać wypracowania krok po kroku ścieżki postępowania w przypadku zaistnienia takiego incydentu.
- Incydent bezpieczeństwa może polegać na:
  - naruszeniu bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania danych osobowych (np. zgubienie nośnika z danymi),
  - naruszeniu bezpieczeństwa prowadzącym do nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (np. włamanie do systemu służącego do przetwarzania danych osobowych).

Zapewnienie środków technicznych i organizacyjnych dla realizacji nowych praw

- Realizacja przykładowych praw podmiotu, którego dane dotyczą:
  - Prawo do **sprostowania danych** – prawo osoby do żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
  - Prawo do **usunięcia danych (tzw. prawo do bycia zapomnianym**) - prawo osoby do żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, o ile spełnione są określone warunki (np. ustał cel przetwarzania danych, cofnięta została zgoda, wniesiony został sprzeciw, dane były przetwarzane niezgodnie z prawem).
  - Prawo do **ograniczenia przetwarzania danych** np. gdy osoba kwestionuje prawidłowość danych osobowych. Ograniczenie następuje na okres pozwalający administratorowi sprawdzić prawidłowość danych.
  - Prawo do **przenoszenia danych,** tj. prawo osoby do otrzymania w ustrukturyzowanym, powszechnie używanym formacie, swoich danych osobowych, które dostarczone zostały administratorowi, w tym ma prawo żądania przesłania tych danych innemu administratorowi bez przeszkód ze strony administratora.

Inne obowiązki wynikające z RODO (1)

- Stosowanie zasad, które przed rozpoczęciem stosowania RODO były dobrymi praktykami, a po 25 maja 2018 r. staną się obowiązkiem:
  - zapewnienie prywatności w fazie projektowania (Privacy by design) - przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża się odpowiednie środki techniczne i organizacyjne (takie jak pseudonimizacja), zaprojektowane w celu skutecznej realizacji zasad ochrony danych (takich jak minimalizacja danych) oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą,
  - zapewnienie prywatności w ustawieniach domyślnych (Privacy by default) - administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Inne obowiązki wynikające z RODO

- Przeprowadzenie oceny skutków naruszenia (DPIA) - jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
- DPIA dokonuje się we współpracy z IODO.
- Przykład łączący ww. zasady i DPIA to case study aplikacji ClassDojo.
  - konstrukcja aplikacji ClassDojo uwzględnia powyższe zasady, daje bowiem możliwość dowolnego wypełnienia formularzy osobowych bez utraty funkcjonalności (postać awatara, wpisywanie „nicka” zamiast imienia i nazwiska etc.).
  - Jednakże potencjalne - pełne uzupełnienie danych osobowych (imię i nazwisko ucznia, klasa, szkoła, dane kontaktowe) i przyznawanie punktów za określone zachowania już mogą po 25 maja 2018 r. wymagać dokonania oceny skutków naruszenia danych osobowych.
  - Serwery ClassDojo są w USA.

Etapy wdrożenia RODO w szkole

Wdrożenie RODO w szkole (1)

- Identyfikacja procesów przetwarzania danych osobowych – analiza dokonana przez powołany /wyłoniony przez Dyrektora szkoły zespół, mająca na celu ustalenie, gdzie w szkole przetwarzane są dane osobowe, np. w obszarach:
  - wykorzystywania dzienników papierowych lub e-dzienników,
  - przetwarzania danych kadrowo-płacowych,
  - zamówień publicznych,
  - ustalania list rodziców (osób) upoważnionych do odbioru dzieci ze świetlicy szkolnej.
- Weryfikacja podstawowych parametrów procesów przetwarzania danych osobowych:
  - określenie podstawy przetwarzania danych osobowych zgodnie z RODO (czy dane są przetwarzane w oparciu o przepisy prawa, czy zgody etc.)
  - sprawdzenie, czy aby nie przetwarzamy zbyt wielu danych osobowych, które nie są potrzebne (minimalizacja danych).
- Wdrożenie podejścia opartego na ryzyku – sprawdzenie, czy zidentyfikowane procesy, gdzie przetwarzamy dane osobowe są odpowiednio zabezpieczone, adekwatnie do przetwarzanych danych.

Wdrożenie RODO w szkole (2)

- Identyfikowanie procesów, gdzie powierzamy przetwarzanie danych osobowych (np. jeśli szkoła ma podpisaną umowę o niszczenie dokumentów papierowych przez firmę zewnętrzną. Wtedy należy zweryfikować, czy firma taka zapewnia przestrzeganie RODO).
- Powołanie IODO w szkole lub zawarcie umowy z podmiotem trzecim na świadczenie usług IODO (może pełnić tę rolę dla kilku szkół).
- Weryfikacja, czy szkoła jest w stanie realizować nowe prawa osób, których dane dotyczą (np. prawo do bycia zapomnianym).
- Wypracowanie ścieżki zgłaszania incydentów bezpieczeństwa.
- Szkolenia personelu szkoły i nauczycieli w zakresie danych osobowych (np. instruktaż, że wyniesienie dziennika przez ucznia, nie obciąża jego, a za incydent bezpieczeństwa odpowiada administrator danych tj. szkoła, a nie uczeń).
- Opcjonalnie: przeprowadzenie procedury oceny skutków dla ochrony danych.

Dziękuję za uwagę!

Kontakt: Paweł Żywicki
e-mail: p.zywicki@warmia.mazury.pl