Jarosław Feliński

Ochrona danych osobowych w oświacie

RODO 2018

Wolters Kluwer

Jarosław Feliński

Ochrona danych osobowych w oświacie

Wolters Kluwer

Warszawa 2018

Stan prawny na 15 maja 2018 r.

Wydawca serii
Elżbieta Piotrowska-Albin

Wydawca
Izabella Małecka

Redaktor prowadzący
Joanna Ołówek

Opracowanie redakcyjne
Elżbieta Lipińska

Łamanie
Kamila Tomecka

ISBN 978-83-8124-800-6

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

ABI	–	administrator bezpieczeństwa informacji
ADO	–	administrator danych osobowych
ASI	–	administrator systemu informatycznego
CCTV	–	telewizja przemysłowa
CUW	–	centrum usług wspólnych
IODO	–	inspektor ochrony danych osobowych
JRWA	–	Jednolity Rzeczowy Wykaz Akt
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. poz. 483 ze zm.)
OPZ	–	opis przedmiotu zamówienia
PPP	–	poradnia psychologiczno-pedagogiczna
rozporządzenie KRI	–	rozporządzenie Rady Ministrów z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247)
RODO	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (tekst mający znaczenie dla EOG) (Dz.Urz. UE L 119, s. 1)
SIWZ	–	specyfikacja istotnych warunków zamówienia
u.f.p.	–	ustawa z 27.08.2009 r. o finansach publicznych (Dz.U. z 2017 r. poz. 2077 ze zm.)

UODO	– ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.)
u.SIO	– ustawa z 15.04.2011 r. o systemie informacji oświatowej (Dz.U. z 2017 r. poz. 2159 ze zm.)

WSTĘP

Terminy: „prywatność", „intymność", „identyfikacja", „monitoring" i „szyfrowanie", wraz z liczną grupą nowych pojęć wprowadzone zostały do polskiego porządku prawnego rozporządzeniem RODO[1]. Problem ochrony prywatności wykazał natomiast już ponad 30 lat temu – w przełomowym artykule w krakowskich „Studiach Cywilistycznych" – prof. Andrzej Kopff. Jego *Koncepcja praw do intymności i do prywatności życia osobistego*[2] określała uniwersalną wartość publicznej dyskusji dotyczącej praw podstawowych każdego człowieka.

Prawo do prywatności, ochrony wizerunku, decydowania o swoim życiu prywatnym nabiera, wraz z rozwojem nowoczesnych technologii informatycznych i komunikacji elektronicznej, coraz większego znaczenia. W oparciu o konstytucyjne i ustawowe gwarancje wprowadzone w 1997 r. przepisami prawa o ochronie danych osobowych[3] zobligowano administratorów danych do zachowania równowagi przetwarzania i zabezpieczania danych.

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (tekst mający znaczenie dla EOG) (Dz.Urz. UE L 119, s. 1).

[2] A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne*, „Studia Cywilistyczne", t. XX, Kraków 1972.

[3] Ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.).

Dylematem każdego administratora stały się pytania: kto może przetwarzać dane osobowe? W jaki sposób należy realizować obowiązki pracodawcy w procesie przetwarzania danych, a także w jakim zakresie realizować przetwarzanie danych w ramach działań podmiotu zobowiązanego do wykonania zadań ustawowych? Kiedy?

W szerokim rozumieniu przetwarzanie danych jest procesem uprawnionego przekazywania, udostępniania i przesyłania danych połączonego z umiejętnością wykazania ich odpowiedniego zabezpieczenia. Zabezpieczenie na poziomie instytucji, organu lub przedsiębiorcy, a także przez usługodawców oznacza konieczność doskonalenia wszystkich uczestników posiadających prawo do dysponowania danymi zgodnie z określonym zakresem prac lub zleconych zadań.

Odpowiedź na wyrażone wątpliwości administrator uzyskiwał w dotychczasowych przepisach UODO, obecnie odnajdzie je również w RODO. Odpowiednie przygotowanie szkoły czy przedszkola w zakresie stosowania nowych przepisów dotyczących ochrony danych osobowych stanowi kontynuację ustawowej konieczności organizacyjno-technicznego zabezpieczenia najistotniejszej wartości, dzięki której placówka istnieje – danych osobowych.

Niniejsze opracowanie stanowi przegląd podstawowych terminów i pojęć oraz wybranych działań określanych atrybutami bezpieczeństwa informacji i cech mających wpływ na standaryzowanie procesów ochrony danych osobowych. Specyfikacji wybranych pojęć dokonano w oparciu o wyżej wymienione przepisy, a także o terminologię stosowaną w rozporządzeniu KRI[4]. Poznanie ich znaczenia, umiejętność ich użycia i zastosowania w tworzeniu procedur powinno ułatwić zaplanowanie i projektowanie poszczególnych etapów wprowadzania RODO w każdej placówce.

[4] Rozporządzenie Rady Ministrów z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247).

ADMINISTRATOR, AKTYWA, ADEKWATNOŚĆ

Pojęcie „administrator" pojawia się w niemal każdym rozdziale RODO. Warto zatem przeanalizować zakres działań i treść kryjącą się w przepisach RODO, z którymi spotka się dyrektor placówki w działalności służbowej w procesie przygotowania i wprowadzania nowej jakości zarządzania danymi osobowymi. Środki organizacyjne, techniczne i edukacyjne są obszarami odpowiedzialności zarówno dyrektora, jak i podmiotów przetwarzających w imieniu administratora, a przede wszystkim osób działających na polecenie tegoż administratora. Dane osobowe, na bazie których wykonywane są zadania pracodawcy i organu realizującego przepisy prawa oświatowego, to podstawowe aktywa[1] informacyjne placówki. Działania poprzedzające wprowadzenie RODO od maja 2016 r. warto oprzeć na wskazaniu zadań ADO i ABI po nowelizacji ustawy o ochronie danych osobowych dokonanej w 2015 r. Wypełnienie zadań ustawowego zarządzania i przetwarzania od 1.01.2015 r. do 30.06.2015 r., zgodnie z brzmieniem art. 36a ust. 1 lub art. 36b UODO, obligowało dyrektora do dokonania wyboru:

- powołać ABI lub
- zrezygnować z powołania.

[1] Aktywami według Polskich Norm są wszystkie ważne dla organizacji/placówki informacje, techniki i narzędzia, które w istotny sposób wpływają na stabilność procesów przetwarzania i zabezpieczenia informacji oraz danych osobowych (por. PN ISO/IEC 27005, s. 17).

Tak sformułowana nowelizacja w art. 36a wprowadziła możliwość powołania ABI placówki, natomiast w art. 36b zadania ABI powierzyła administratorowi danych. Rozwiązania przyjęte nowelizacją UODO z 2015 r. zakładały rozpoczęcie procesu przygotowania osób funkcyjnych i tym samym jednostki do wypełniania nowych regulacji RODO poprzez systematyczne nabywanie umiejętności, a także:

- organizacyjne przekształcenie struktury – podległość ABI administratorowi danych;
- zapewnienie badania zgodności przetwarzania danych;
- sprawne zarządzanie użytkownikami;
- umiejętność sprawowania nadzoru i weryfikację procedur;
- systematyzowanie kategorii przetwarzanych danych osobowych;
- aktualizację przepisów wewnętrznych;
- weryfikację umów na świadczenie usług.

Przepisy RODO wykluczają natomiast możliwość zastosowania podobnych do stosowanych w poprzednim porządku prawnym rozwiązań organizacyjnych i jednoznacznie wskazują na konieczność **autonomicznego wyznaczenia** inspektora ochrony danych osobowych (dalej: IODO) w organach i podmiotach publicznych. Podkreślenie autonomicznego charakteru znajduje umocowanie w polskich przepisach dotyczących ochrony danych osobowych, w których ustalono zadania administratora, m.in. zgłoszenie w określonym terminie wyznaczonego w placówce inspektora.

Istotną zmianą jest wskazanie bezpośredniej podległości IODO dyrektorowi placówki – art. 38 ust. 3 RODO. Oznacza to konieczność wprowadzenia zmian w zapisach dokumentów wewnętrznych. Tym samym pierwsza z czynności wdrożeniowych/organizacyjnych administratora w okresie od maja 2016 do 24 maja 2018 r. to wprowadzenie odpowiednich zapisów do dokumentów wewnętrznych placówki (odpowiednio – statutu, regulaminu organizacyjnego lub schematu organizacyjnego).

Przykład zapisu w statucie [art. 10 ust. 5 UODO (każdy z tych podmiotów dokonuje zawiadomienia) w zw. z art. 38 ust. 3 RODO (podległość kierownikowi jednostki)]

Inspektor ochrony danych osobowych podlega bezpośrednio dyrektorowi szkoły/przedszkola.

Zadania IODO:

- zapoznawanie personelu placówki z przepisami RODO i regulacjami prawa oświatowego dotyczącymi ochrony danych osobowych [przykładem jest rekrutacja szkolna] oraz szkolenie go w tym zakresie;
- informowanie o potrzebie aktualizacji zapisów w dokumentacji dotyczącej przetwarzania i zabezpieczenia danych osobowych [zmiany zapisów np. zgód lub wniosków];
- bieżąca analiza i konsultacje wszelkich spraw związanych z przetwarzaniem danych [w tym przypadku można wskazać ocenę dokumentacji i CV kandydatów co do adekwatności podanych ilości informacji osobistych kandydata];
- ocena potencjalnych zagrożeń mogących mieć wpływ na dostęp do danych osobowych [wskazanie na sytuacje braku kontroli ze strony IODO, np. ze względu na długotrwałą absencję];
- metodologiczne prowadzenie wewnętrznych nadzorów audytowych [zgodnie z przepisami o informatyzacji zasady audytu wewnętrznego bezpieczeństwa informacji posiadają jednoznaczną metodykę ich realizacji i potrzebę posiadania przygotowania IODO do tego zakresu czynności];
- informowanie o naruszeniu lub utracie danych [szybkość reakcji];
- sygnalizowanie potrzeb wsparcia działań inspektora [analiza i prognoza potrzeb, zasobów i działań wspierających];
- inicjowanie podnoszenia poziomu świadomości pracowników w zróżnicowanych formach edukacyjnych.

Ochrona danych osobowych w oświacie

Jarosław Feliński – wykładowca wyższych uczelni; prekursor kształcenia ABI w Polsce; kierownik merytoryczny studiów podyplomowych z ochrony danych osobowych; twórca autorskiego programu podyplomowych studiów dla ABI i IODO; audytor wiodący ISO PN 27001; prezes Stowarzyszenia Inspektorów Ochrony Danych Osobowych w Polsce.

W publikacji opisano działania i procedury zabezpieczenia danych osobowych w placówkach oświatowych różnych typów, wraz z przykładami zastosowania nowych rozwiązań. Przewodnik objaśnia także podstawowe terminy i pojęcia z zakresu ochrony danych osobowych, co ułatwi przygotowanie szkoły i przedszkola do stosowania nowych regulacji wynikających z wejścia w życie RODO. Jego celem jest pomoc w zaplanowaniu i wdrożeniu poszczególnych obowiązków wynikających z RODO.

Czytelnik znajdzie w książce odpowiedzi m.in. na takie pytania, jak:

- jakie są nowe obowiązki nałożone na administratorów danych osobowych oraz jak przygotować się do ich wykonywania;
- jaki jest zakres odpowiedzialności dyrektora szkoły oraz jej pracowników w związku z nowymi przepisami;
- kto może przetwarzać dane osobowe w zakresie legalności obrotu;
- w jaki sposób osiągnąć minimum skuteczności i funkcjonalności wdrożonych rozwiązań;
- kiedy można rozpoznać zdarzenie jako naruszenie przepisów RODO oraz jak należy postąpić w takim przypadku.

Publikacja przeznaczona jest dla dyrektorów oraz pracowników placówek oświatowych odpowiedzialnych za wdrożenie stosowania nowych przepisów z zakresu ochrony danych osobowych. Zainteresuje także prawników praktyków i pracowników naukowych specjalizujących się w ochronie danych osobowych.

CENA 49 ZŁ (W TYM 5% VAT)

9788381248006 W01P01

ISBN 978-83-8124-800-6

9 788381 248006