OCHRONA DANYCH OSOBOWYCH W OŚWIACIE

Poradnik dla administratorów oraz inspektorów ochrony danych

Anna Pielok, Piotr Sojka

DOBRE PRAKTYKI W OŚWIACIE

Wolters Kluwer

OCHRONA DANYCH OSOBOWYCH W OŚWIACIE

Poradnik dla administratorów oraz inspektorów ochrony danych

Anna Pielok, Piotr Sojka

DOBRE PRAKTYKI W OŚWIACIE

Wolters Kluwer

WARSZAWA 2020

Stan prawny na 15 maja 2020 r.

Wydawca serii
Elżbieta Piotrowska-Albin

Wydawca
Izabella Małecka

Redaktor prowadzący
Paulina Ambroży

Opracowanie redakcyjne
Joanna Ośka

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

ISBN 978-83-8187-874-6

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

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

PRZEDMOWA

Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych autorstwa Anny Pielok i Piotra Sojki to pierwsze tak obszerne opracowanie dotyczące problematyki ochrony danych osobowych w sektorze oświaty pod rządami RODO dostępne na rynku polskim.

Autorzy poradnika od wielu lat są związani z problematyką ochrony danych osobowych i informacji. Swoje doświadczenia zdobywali pierwotnie jako administratorzy bezpieczeństwa informacji, a następnie jako inspektorzy ochrony danych w samorządzie gminnym i jego jednostkach organizacyjnych. Wdrażając RODO w placówkach oświatowych, tworzyli dokumentację oraz procedury ochrony danych osobowych. Mając równocześnie dwudziestoletnie doświadczenie jako pracownicy samorządowi na różnych stanowiskach, poznali otoczenie prawne oświatowych administratorów.

Poradnik przechodzi przez obowiązki szkół i placówek oświatowych wynikające z RODO, osadzając je w kontekście sektora i działalności oświatowej. Autorzy podają liczne przykłady i odwołania do przepisów branżowych, w ten sposób ułatwiając skonkretyzowanie obowiązków leżących po stronie szkół, przedszkoli i innych placówek i organizacji prowadzących działalność oświatową, będących administratorami danych osobowych w rozumieniu RODO.

Poradnik omawia też obowiązki oraz rolę inspektora ochrony danych. Pozostanie zapewne tajemnicą autorów, dlaczego swojemu hipotetycznemu inspektorowi ochrony danych nadali imię i nazwisko

Piotr Czepialski. Oczywiście niejasne przede wszystkim pozostanie, czemu akurat Piotr.

Jak wskazują autorzy, Poradnik jest „sprzęgnięty" z rozwiązaniami zawartymi w projekcie Kodeksu postępowania przygotowanym przez autorów i opublikowanym na stronie rodo-w-oswiacie.pl. Dlatego jego użyteczność jest szersza niż to, co jest w nim bezpośrednio zawarte.

Zaletą Poradnika jest duża jednoznaczność stanowisk oraz rozwiązań omawianych i proponowanych przez autorów. Nie pozostawiając za wiele miejsca na wątpliwości, ułatwiają oni zastosowanie proponowanych rozwiązań.

Działalność oświatowa ze swojej natury wymaga przetwarzania danych osobowych. Poruszanie się w gąszczu przepisów branżowych oraz interpretacja syntetycznego aktu prawnego, jakim jest RODO, jest zadaniem trudnym i czasochłonnym nawet dla specjalistów. Dlatego Poradnik jest pozycją obowiązkową dla osób zajmujących się edukacją, i to nie tylko dla inspektorów ochrony danych. Pamiętać bowiem musimy, że za zgodność z ochroną danych odpowiada kierownictwo jednostki, kierownicy komórek organizacyjnych, a także konkretni pracownicy, a nie inspektor ochrony danych.

Książka skierowana jest do wszystkich, którzy pracują w oświacie i muszą podejmować decyzje dotyczące ochrony danych osobowych.

Maciej Gawroński

WSTĘP

Pierwsze, uwieńczone sukcesem, próby ujęcia w karby narastających problemów dotyczących bezpieczeństwa osób fizycznych w związku z tym, że dane na ich temat są przetwarzane przez różne podmioty, miało miejsce w 1995 r. Panowały wówczas warunki zupełnie odmienne od dzisiejszych. Internet dostępny był niewielkiej liczbie osób. Komputeryzacja dopiero nabierała rozpędu, a o czymś takim jak smartfon nikt nie słyszał. W miarę upływu czasu sytuacja ulegała ogromnym zmianom. Moce obliczeniowe maszyn wzrosły kilkaset milionów razy, dane osobowe – informacje, które zawsze miały wysoką wartość dla różnych podmiotów – zaczęły być przetwarzane na masową skalę z użyciem elektronicznych urządzeń. Stąd już tylko krok do łączenia informacji z różnych źródeł, profilowania lub określenia preferencji, na przykład zakupowych. Nagłośnione przypadki naruszeń bezpieczeństwa danych osobowych i w związku z tym rosnąca świadomość osób, których dane dotyczą, powoli rozpędzały lawinę, która w porę niewyhamowana, może przynieść skutki o trudnej do przewidzenia skali.

Dnia 27.04.2016 r. światło dzienne ujrzał akt, który miał pomóc w skanalizowaniu i uporządkowaniu tej lawiny. 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) (Dz.Urz. UE L 119, s. 1) – zwane potocznie RODO lub GDPR – weszło w życie 25.05.2018 r. i obowiązuje bezpośrednio wszystkie kraje w tzw. Europejskim Obszarze Gospodarczym.

Akt prawny dalej zwany RODO jest zbiorem przepisów nadrzędnych w stosunku do innych regulacji dotyczących bezpieczeństwa danych osobowych. Do jego stosowania zobowiązany jest każdy organ publiczny, w tym placówki oświatowe. W myśl definicji administratora, zawartej w art. 4 pkt 7 RODO, dyrektor szkoły jest administratorem danych osobowych uczniów, ich rodziców, pracowników, a także innych osób fizycznych, których dane przetwarza placówka w ramach swojej działalności, decydując o celach i środkach ich przetwarzania. Wdrożenie RODO w placówce oświatowej nie jest łatwe, gdyż jak pokazuje doświadczenie, dyrektorowi brak odpowiedniego personelu i funduszy na zapewnienie odpowiednich organizacyjnych środków ochrony, nie wspominając już o zabezpieczeniach w systemie informatycznym. Nic jednak nie zwalnia go od odpowiedzialności za przetwarzane dane osobowe. Obowiązek ochrony danych osobowych nakłada na dyrektora wprost art. 68 ust. 1 pkt 12 pr. ośw., wskazując iż jego zadaniem jest wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania danych osobowych przez szkołę lub placówkę zgodnie z przepisami o ochronie danych osobowych. Obowiązek ten jest równie ważny jak zapewnienie nadzoru pedagogicznego czy bezpiecznych i higienicznych warunków kształcenia. Tak więc, kwestię tę należy traktować z należytą powagą, choć jak pokazuje doświadczenie autorów, była ona do tej pory, delikatnie mówiąc, marginalizowana.

Celem opracowania niniejszego poradnika jest pomoc we wdrożeniu spójnych procedur, gwarantujących zgodne z przepisami prawa przetwarzanie danych osobowych w placówkach oświatowych. Opracowanie zawiera wzory procedur, które administrator danych – dyrektor szkoły – może wykorzystać w realizacji zadania zapewnienia bezpieczeństwa danych osobowych w swojej placówce.

Poradnik ten jest swego rodzaju *know-how* dla procedur i rozwiązań zaproponowanych w Kodeksie postępowania dla oświaty, opracowanego na podstawie art. 40 RODO, a opublikowanego na stronie internetowej: rodo-w-oswiacie.pl.

Unijna reforma ochrony danych osobowych została wprowadzona za pomocą narzędzia prawnego, jakim jest rozporządzenie. Zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 2016 r., s. 47) jest ono bezpośrednio stosowane we wszystkich państwach członkowskich. Zaletą, a zarazem źródłem trudności takiego rozwiązania jest daleko idąca ogólność i neutralność technologiczna. Ogólność pozwala administratorowi na własny dobór adekwatnych zabezpieczeń i wprowadzenie własnych rozwiązań. Jak na ironię, jest to również przekleństwo tego przepisu z powodu chaosu informacyjnego wywołanego przez media oraz kręgi mniej lub bardziej fachowe.

Oddając w Państwa ręce niniejszy poradnik, przedstawiamy własne propozycje rozwiązań i wzorów, których można, dokonując odpowiedniego dostosowania, użyć w każdej placówce oświatowej.

Rozdział I

ADMINISTRATOR, PODMIOT PRZETWARZAJĄCY I ODBIORCA DANYCH OSOBOWYCH W JEDNOSTKACH OŚWIATOWYCH

1. Administrator

Przetwarzanie danych osobowych zgodnie z RODO wymaga w pierwszej kolejności ustalenia, kto jest ich administratorem, w myśl definicji z art. 4 pkt 7 rozporządzenia 2016/679.

Zgodnie ze stanowiskiem Urzędu Ochrony Danych Osobowych „administratorem danych osobowych uczniów, ich rodziców, nauczycieli, pracowników szkoły jest ten, kto decyduje o celach i sposobach przetwarzania tych danych, czyli szkoła, którą reprezentuje dyrektor szkoły”[1].

Szkoła czy przedszkole są podmiotami publicznymi i przetwarzanie danych osobowych odbywa się na podstawie i w granicach prawa, tak więc decyzyjność dyrektora szkoły jest ograniczona właściwie do wyboru środków przetwarzania danych osobowych. Odnieśmy się tutaj do definicji przetwarzania danych osobowych, zawartej w art. 4 pkt 2 rozporządzenia 2016/679, gdzie przetwarzanie danych osobowych to

[1] Urząd Ochrony Danych Osobowych, Ministerstwo Edukacji Narodowej, *Poradnik RODO, Ochrona danych osobowych w szkołach i placówkach oświatowych,* sierpień 2018, s. 8.

wykonywanie na danych osobowych takich czynności jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnienie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. O środkach i zakresach tych czynności, wykonywanych na danych osobowych przetwarzanych przez jednostki oświatowe, zawsze będzie decydował ich dyrektor i to on będzie adresatem wszystkich obowiązków wynikających z RODO, a kierowanych do administratora danych osobowych.

To, na co należy zwrócić uwagę, to fakt, że jednostki oświatowe są najczęściej jednostkami organizacyjnymi organów administracji samorządowej. To, że zapewnienie edukacji jest zadaniem własnym gminy, nie czyni jej w żadnej mierze administratorem danych przetwarzanych przez jednostki oświatowe. Zarówno zadania gminy, jak i zadania szkoły w zakresie procesów opieki i kształcenia dzieci są ściśle uregulowane w przepisach prawa i przypisane osobno każdemu z nich. A zatem, każdorazowe, właściwe określenie relacji pomiędzy jednostką oświatową a jej organem prowadzącym co do ról w procesach przetwarzania danych osobowych jest konieczne do właściwego przypisania obowiązków i odpowiedzialności z tego wynikających.

Przetwarzając dane osobowe w ramach realizacji zadań wynikających z prawa oświatowego oraz funkcjonowaniem jednostki jako podmiotu publicznego, to dyrektor będzie administrował danymi. Odpowiedzialność za dane, oprócz przepisów RODO, wynikać będzie również z zacytowanego już we wstępnie art. 68 ust. 1 pkt 12 pr. ośw., na mocy którego wdraża on odpowiednie środki techniczne i organizacyjne zapewniające zgodność przetwarzania danych osobowych przez szkołę lub placówkę z przepisami o ochronie danych osobowych.

2. Podmiot przetwarzający

Nie zawsze dyrektor szkoły jest w stanie zapewnić właściwe środki do przetwarzania danych osobowych, bazując wyłącznie na zasobach jednostki oświatowej. W takiej sytuacji dochodzi bardzo często do korzystania z usług podmiotu przetwarzającego, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO). W jednostkach oświatowych będą to na przykład firmy dostarczające usługę udostępniania oprogramowania do prowadzenia elektronicznego dziennika zajęć w formie *cloud computing*. Dane osobowe są przechowywane na serwerach podmiotu przetwarzającego i on też jest odpowiedzialny za ich zabezpieczenie, wykonywanie kopii zapasowych czy aktualizację oprogramowania służącego do ich przetwarzania. Z podobną sytuacją spotkamy się w przypadku obowiązku wydawania przez dyrektora szkoły nauczycielskich legitymacji służbowych. Zgodnie z przepisami, blankiet legitymacji wykonany jest z wielowarstwowej karty laminowanej. Aby móc wykonać taką legitymację, dyrektor szkoły zmuszony jest do korzystania z usług podmiotu zewnętrznego, który to względem powierzonych mu danych osobowych nauczycieli stanie się podmiotem przetwarzającym. Podmiotem przetwarzającym będzie także CUW, realizujący zadania dyrektora w zakresie prowadzenia rachunkowości czy obsługi kadrowo-płacowej. Z podmiotem przetwarzającym będziemy mieli również do czynienia w przypadku usługi elektronicznego monitorowania czasu przebywania dziecka w przedszkolu dla potrzeb naliczania opłat. Jeśli usługa ta będzie wykonywana w modelu *cloud computing*, to zaistnieje taka sytuacja jak w przypadku elektronicznego dziennika zajęć.

3. Inny administrator jako odbiorca danych

W procesach przetwarzania danych osobowych w jednostce oświatowej dochodzi do przekazywania danych osobowych innym administratorom. Wynika to przede wszystkim z przepisów prawa. Odbiorcy ci, którzy stają się administratorami przekazanych danych osobowych, realizują obowiązki przypisane im samym, a nie jednostce oświatowej. Odbiorcą danych będzie nie tylko podmiot przetwa-

rzający, ale również inny administrator[2]. Z taką sytuacją mamy do czynienia w przypadku przekazywania danych osobowych uczniów pielęgniarce szkolnej, sprawującej opiekę medyczną nad dziećmi w miejscu nauczania i wychowania. Po przekazaniu danych, w postaci imienia, nazwiska oraz numeru PESEL dziecka, to podmiot leczniczy, świadczący usługi w tym zakresie, staje się ich administratorem, przejmując także obowiązki wynikające z rozporządzenia 2016/679 i przetwarzając dane do zadań i celów jemu właściwych. Tak będzie też, gdy przekazywane są dane osobowe w arkuszach organizacyjnych do zatwierdzenia do organu prowadzącego, organu sprawującego nadzór pedagogiczny czy opiniujących go związków zawodowych. Każdy z tych organów ma swoje zadania związane z zatwierdzaniem arkusza organizacyjnego i dla przetwarzanych danych osobowych podczas ich realizacji jest administratorem danych osobowych tam zawartych. Analogicznie będzie, gdy przekazujemy dane osobowe do Ministerstwa Edukacji Narodowej za pośrednictwem Systemu Informacji Oświatowej oraz do Komisji Egzaminacyjnych za pośrednictwem Sytemu Informatycznego Obsługi Egzaminów Ogólnokształcących. Po przekazaniu tych danych ich administratorem stają się, odpowiednio, Minister Edukacji Narodowej oraz Okręgowe Komisje Egzaminacyjne w zakresie dziedziny ich działania (zasięgu terytorialnego).

Właściwe określenie relacji pomiędzy podmiotami przetwarzającymi dane osobowe jest bardzo istotne, ponieważ wiąże się z różnymi obowiązkami oraz odpowiedzialnością za przetwarzanie danych osobowych. Powierzenie przetwarzania wcale nie zwalnia administratora z odpowiedzialności za powierzone dane, obciążając go obowiązkiem właściwego wyboru podmiotu przetwarzającego, uregulowaniem wszystkich istotnych kwestii przetwarzania w umowie powierzenia, a także kontrolowaniem bezpieczeństwa powierzonych danych. Przekazanie zaś danych osobowych innemu administratorowi będzie wiązało się również z przejęciem przez niego odpowiedzialności za przetwarzanie przekazanych mu danych osobowych.

[2] P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 227.

Rozdział II

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 5 rozporządzenia 2016/679, dane osobowe należy przetwarzać z zachowaniem odpowiednich zasad. Należą do nich zasady: zgodności z prawem, rzetelności i przejrzystości; ograniczenia celu; minimalizacji danych; prawidłowości; ograniczenia przechowywania; integralności i poufności; a także zasada rozliczalności.

Spróbujmy przeanalizować praktyczne zastosowanie wymienionych zasad na konkretnym przykładzie, jakim będzie przetwarzanie danych osobowych w procesie rekrutacji uczniów do placówki oświatowej.

1. Zasada zgodności z prawem, rzetelności i przejrzystości

Przetwarzając dane osobowe w procesie rekrutacji uczniów lub wychowanków do jednostki oświatowej, administrator danych pozyskuje je od rodzica bądź opiekuna prawnego dziecka lub od pełnoletniego kandydata. Chcąc przetwarzać dane osobowe z zachowaniem zasady zgodności z prawem, w pierwszej kolejności, dyrektor szkoły musi określić, na podstawie jakich przepisów prawa będzie dane osobowe przetwarzał, oraz odpowiedzieć sobie na pytanie, czy przetwarzanie to spełnia wymóg legalności przetwarzania danych określony w art. 6 i 9 rozporzą-

Celem poradnika jest pomoc we wdrożeniu i utrzymaniu spójnych procedur gwarantujących przetwarzanie danych osobowych w placówkach oświatowych, zgodne z przepisami prawa. Poradnik omawia obowiązki szkół i placówek oświatowych wynikające z RODO oraz wskazuje liczne przykłady i odwołania do przepisów branżowych.

Przybliżono w nim takie zagadnienia jak:

– administrator, inspektor ochrony danych oraz podmiot przetwarzający i odbiorca danych osobowych w jednostkach oświatowych;
– prawa osób, których dane dotyczą, upoważnienie do przetwarzania danych osobowych i oświadczenie o zachowaniu poufności;
– polityka bezpieczeństwa informacji;
– rejestr czynności i kategorii czynności przetwarzania danych osobowych;
– monitoring wizyjny w placówce oświatowej;
– szacowanie ryzyka naruszenia praw i wolności osób w związku z przetwarzaniem danych osobowych w placówce oświatowej oraz stałe monitorowanie wdrożonych zabezpieczeń;
– zarządzanie incydentami naruszenia ochrony danych osobowych;
– przepływ danych między placówką oświatową a organem prowadzącym i organem sprawującym nadzór pedagogiczny.

Opracowanie zawiera wzory procedur, które administrator danych – dyrektor szkoły może wykorzystać w realizacji zadania zapewnienia bezpieczeństwa danych osobowych w swojej placówce.

Publikacja przeznaczona jest dla dyrektorów, inspektorów ochrony danych oraz pracowników szkół, przedszkoli i innych placówek oświatowych, odpowiedzialnych za stosowanie przepisów z zakresu ochrony danych osobowych. Zainteresuje także prawników praktyków i pracowników naukowych specjalizujących się ochronie danych osobowych.

9788381878746 W01P01

ISBN 978-83-8187-874-6
9 788381 878746

CENA 59 ZŁ (W TYM 5% VAT)