NR 11 (909) LISTOPAD 2018 CENA 39,00 ZŁ (W TYM 23% VAT) WWW.PGP.INFOR.PL

PORADNIK GAZETY PRAWNEJ

UKAZUJE SIĘ OD 1995 ROKU

RODO

W PRAKTYCE

- Na co skarżą się polskie firmy po wdrożeniu RODO
- Jak postępować w przypadku naruszenia ochrony danych osobowych
- Czy korzystanie z plików cookie zawsze wymaga zgody użytkownika

INFOR
Zał. R. Pieńkowski w 1987 r.

INDEKS 331783

ISSN 1234-5695

Partnerzy merytoryczni

KANCELARIA PRAWNA answer OSTAFI I PARTNERZY

INFORLEX

STREFA RODO 2018

INFORLEX RODO AKTUALIZOWANY SERWIS WWW
+ KSIĄŻKA **„RODO DLA KSIĘGOWYCH I BIUR RACHUNKOWYCH"**

INFORLEX RODO zawiera:

- ✓ **Przepisy** regulujące **rozporządzenie o ochronie danych osobowych,**
- ✓ **Aktywne wzory i druki**,
- ✓ **Artykuły** na temat **procedur** związanych z wdrożeniem polityki **ochrony danych osobowych w firmie/jednostce,**
- ✓ **Informacje o obowiązkach,** jakie należy wypełnić, oraz **jak uniknąć kar** za błędne wdrożenie nowych regulacji,
- ✓ **Bazę porad i odpowiedzi GIODO**,
- ✓ **Wideoszkolenia i wideoporady** o tematyce **RODO.**

KSIĄŻKA: „RODO dla księgowych i biur rachunkowych"

Prosty język, obejmuje całość zagadnienia, liczne przykłady, wzory dokumentów do wykorzystania w biurze rachunkowym i dziale księgowości. Wzory można w łatwy sposób wykorzystać w swojej działalności, ponieważ ich wersja elektroniczna zapisana na pendrive jest dołączona do książki.

Pakiet RODO w cenie od **198 zł**

INFOR
Zał. R. Pieńkowski w 1987 r.

sklep.infor.pl | 22 212 07 30, 801 626 666 | bok@infor.pl

Autorami rozdziałów 1–18 Poradnika są:

Kamila Kozera
Radca prawny
w Kancelarii Prawnej ANSWER Ostafi i Partnerzy.

Katarzyna Pośpiech-Białas
Radca prawny
w Kancelarii Prawnej ANSWER Ostafi i Partnerzy.

Piotr Ostafi
Adwokat, partner
w Kancelarii Prawnej ANSWER Ostafi i Partnerzy.

Bartosz Wojciechowski
Radca prawny, partner
w Kancelarii Prawnej ANSWER Ostafi i Partnerzy.

Więcej informacji o autorach na str. 97

Spis treści

RODO w praktyce

1. Wstęp

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 lub ogólne rozporządzenie o ochronie danych) określa ochronę osób fizycznych w związku z przetwarzaniem danych osobowych oraz stanowi o swobodnym przepływie danych osobowych. Oznacza to nałożenie na przetwarzających dane większej odpowiedzialności. To oni będą musieli wykazać, że zastosowane metody ochrony danych są skuteczne.

Kiedy 8 czerwca 2018 r. pod Nowym Targiem doszło do wypadku drogowego, w którym uczestniczył autokar wiozący dzieci wracające z wycieczki szkolnej, część poszkodowanych uczniów została niezwłocznie rozwieziona do okolicznych szpitali. Jak się jednak okazało, ich rodzice mieli olbrzymie problemy z ustaleniem, gdzie przebywają ranne dzieci. Odnalezienie małego pacjenta w konkretnym szpitalu lub otrzymanie choćby podstawowych informacji przez telefon było bardzo trudne albo w ogóle niemożliwe. Jak się okazało, powodem takiej wstrzemięźliwości pracowników służby zdrowia było unijne rozporządzenie o ochronie danych osobowych, które 25 maja tego roku, a więc niecały miesiąc wcześniej, weszło w życie także w Polsce. Niebezpieczną sytuację bardzo szybko skomentował Maciej Kawecki, dyrektor departamentu zarządzania danymi w Ministerstwie Cyfryzacji. Zapewnił on, że jego urząd uczuli jednostki zdrowia, by bardziej racjonalnie podchodziły do tematu ochrony danych osobowych.

Najważniejszym słowem w powyższej wypowiedzi urzędnika jest racjonalność, która jest kluczem do zrozumienia i zastosowania w życiu nowych regulacji prawnych. Racjonalne dostosowanie, elastyczność środków oraz otwarty katalog stosowanych metod, technik i regulacji wewnętrznych stanowią o innowacyjności i atrakcyjności nowych przepisów. Z tych samych powodów stanowią one jednak wyzwanie i zmuszają do zupełnie nowego spojrzenia na ochronę danych osobowych, tak by dostosowując się do nowych mechanizmów prawnych nie narazić się na odpowiedzialność prawną i finansową. Ci, którzy myślą, że doświadczenia nabyte w trakcie praktyki pod rządami wcześniejszych przepisów (w tym między innymi ustawy o ochronie danych osobowych) są wystarczające, by stawić czoła nowym przepisom, są w poważnym błędzie.

Należy przypomnieć, że na podstawie poprzednio obowiązującej ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: OchrDanychU) konieczne i zarazem wystarczające było sporządzenie dokumentacji w postaci Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemami Informatycznymi, których forma i treść były uregulowane rozporządzeniem wykonawczym. Ich sporządzenie było zatem wyłącznie niezbyt uciążliwą formalnością. Co więcej, kary finansowe przewidziane ustawą, niezależnie od ich niewielkiej wysokości, miały charakter wyłącznie przymuszający. Stosowane były dopiero wtedy, gdy kontrolowany podmiot nie dostosował się do zaleceń pokontrolnych organu. Te przyczyny spowodowały, że ochrona danych osobowych była jednym z tych zagadnień, o których przedsiębiorca pamiętał w ostatniej kolejności.

UWAGA
Doświadczenia nabyte w czasie obowiązywania OchrDanychU są istotne, jednak niewystarczające, by sprostać wymaganiom RODO.

O ochronie tych jakże wrażliwych danych pamiętał jednak europejski prawodawca. Zauważył on, że zmieniający się świat wymaga dostosowania do niego mechanizmów prawnych. Coraz powszechniejsze aplikacje mobilne, galopujący rozwój branży e-commerce, nowe technologie oraz postępująca wirtualizacja i digitalizacja

życia codziennego spowodowały, że stopniowo zaczęliśmy tracić kontrolę nad naszymi danymi osobowymi oraz informacjami o życiu prywatnym.

Unijne rozporządzenie o ochronie danych osobowych ma pozwolić nam tę kontrolę przywrócić. Nie tylko dla odzyskania jakże wygodnej i spokojnej prywatności, ale i dla zarządzania nią w racjonalny sposób, także z powodów czysto ekonomicznych. Dziś dane osobowe, pozwalające sprofilować i celnie dotrzeć do każdego konsumenta, mają bowiem określoną i wymierną wartość. A zatem jeśli mamy coś cennego, nie pozwólmy, by ktoś korzystał z tego wbrew naszej woli i bez naszej kontroli nad gromadzeniem, przetwarzaniem i przechowywaniem tego unikatowego dobra, jakim są dane osobowe.

Między innymi dlatego pojawiła się potrzeba stworzenia niniejszego Poradnika, który ma być mapą drogową zarówno dla podmiotów przetwarzających dane osobowe, jak i dla samych podmiotów tych danych. Jako schemat Poradnika przyjęto schemat unijnego rozporządzenia, którego układ i kolejność w czytelny sposób pozwalają poprowadzić Czytelnika po meandrach RODO. Pamiętajmy jednak, że sama mapa to nie terytorium, więc wędrówka po nim może być pełna pułapek.

Poznamy zatem definicję danych osobowych i jej najważniejsze elementy kreacyjne, czyli zakres przedmiotowy informacji, możliwość identyfikacji podmiotu oraz odniesienie do konkretnej osoby fizycznej. Dowiemy się, czy numer telefonu zawsze należy do danych osobowych, i rozróżnimy dane na zwykłe, wrażliwe i te wynikające z wyroków skazujących i czynów zabronionych. Spróbujemy przekonać, że choć co do zasady wizerunek należy do danych osobowych zwykłych, jednak gdy jest przetwarzany coraz powszechniejszymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby, to będzie należał już do danych osobowych szczególnych kategorii jako dana biometryczna.

Zwrócimy uwagę na cienką granicę między administratorem danych osobowych a podmiotem przetwarzającym takie dane. A granica ta jest nie tylko cienka, ale i płynna, ponieważ to, co odróżnia administratora od innych podmiotów, to przede wszystkim możliwość decydowania o celach i sposobach przetwarzania.

Spróbujemy uporządkować też zasady przetwarzania danych osobowych, zwłaszcza że jest to regulacja nowatorska. Obowiązująca wcześniej OchrDanychU nie wskazywała wprost zasad ochrony danych osobowych, które były wywodzone z jej poszczególnych postanowień. Ustawodawca unijny postanowił jednak podnieść rangę tych zasad, wymieniając je wprost w treści rozporządzenia. A zrobił to nie bez powodu, ponieważ wszelkie procesy przetwarzania danych osobowych muszą być obecnie zgodne ze wszystkimi zasadami przetwarzania łącznie. Naruszenie choćby jednej z nich powoduje, że przetwarzanie danych osobowych będzie niezgodne z prawem. Warto więc je poznać i o nich pamiętać.

Tak samo opiszemy podstawy prawne przetwarzania danych osobowych. Jest to tym ważniejsze, że przedmiotowe podstawy stanowią zamknięty katalog, a administrator wypełni zasadę legalności, tylko jeżeli oprze proces przetwarzania danych osobowych choćby na jednej podstawie wskazanej w przepisie, i to tej właściwej. Trzeba zatem dobrze ją dobrać, by nie naruszyć praw osoby fizycznej.

Unijne rozporządzenie daje też zupełnie nowe i daleko idące prawa osobom, których dane są przetwarzane. Przede wszystkim europejski prawodawca zadbał o to, by osoby fizyczne miały większy dostęp do informacji o swoich danych i działaniach administratora, a także większy i faktyczny wpływ na proces przetwarzania tych danych. Prawo dostępu do danych, prawo do ich sprostowania, prawo do przenoszenia, ograniczenia przetwarzania czy prawo do sprzeciwu w wyraźny sposób stanowią też jasną i uporządkowaną analogię wobec katalogu praw właścicielskich chroniących własność w prawie cywilnym. Nowatorskie jest z kolei prawo do usunięcia danych i prawo do bycia zapomnianym. Osoba, której dane dotyczą, będzie mogła bowiem żądać od administratora danych ich usunięcia, jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, jeżeli osoba, której dane dotyczą, cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących albo jeśli przetwarzanie jej danych osobowych nie jest, z innego powodu, zgodne z rozporządzeniem. Uprawnienie to zostało zabezpieczone określonymi procedurami i sankcjami, a świadomość prawna w społeczeństwie sukcesywnie rośnie, wydaje się więc, że czeka nas fala wniosków o bycie zapomnianym.

UWAGA

RODO umożliwia osobom fizycznym większy dostęp do informacji o swoich danych i działaniach administratora, a także większy i faktyczny wpływ na proces przetwarzania tych danych.

Przeanalizujemy też wykorzystanie danych osobowych do zautomatyzowanego podejmowania decyzji, w tym profilowania. Działania takie odnajdujemy coraz częściej nie tylko w marketingu, ale i w wielu innych sektorach życia. Profilowanie jest coraz bardziej powszechną praktyką, a postęp technologiczny i dostępność do wielu narzędzi katalogowych i analitycznych (w tym choćby niewinne pliki cookies) ułatwiły tworzenie profili i podejmowanie zautomatyzowanych decyzji. Z jednej strony stanowi to praktyczne ułatwienie dla konsumentów, z drugiej jednak może też znacząco wpływać na prawa i wolności osób fizycznych, a także utrwalać stereotypy czy podważać swobodę wyboru produktów i usług. Nadmienić trzeba, że choć RODO nie wprowadza zakazu profilowania, jednak wprowadza przepisy mające na celu przeciwdziałanie zagrożeniom wynikającym z profilowania i automatycznego podejmowania decyzji. Administrator danych, realizując zasadę przejrzystości podczas zbierania danych, jest bowiem zobowiązany do poinformowania o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a konsument ma prawo sprzeciwić się takim działaniom.

Gdy mówimy o administratorze danych osobowych, wspomnimy też o wygodnej instytucji współadministratorów, która pozwala ustalić wspólnie cele i sposoby przetwarzania danych przez dwa i więcej podmioty powiązane funkcjonalnie lub gospodarczo. Omówimy przy tym także status prawny, a zwłaszcza obowiązki, inspektora ochrony danych osobowych oraz trudne kwestie zarządzania danymi osobowymi, w szczególności powierzenie i udostępnienie tych danych, upoważnienie do ich przetwarzania, prowadzenie rejestrów czy wreszcie analizę ryzyka i zagrożeń, które spędzają obecnie sen z powiek administratorom i inspektorom danych. A jeśli mowa o zagrożeniach, to omówimy także rodzaje i wysokość sankcji oraz przebieg postępowania kontrolnego.

Staraliśmy się poruszyć i omówić jak najwięcej kwestii. Wierzymy, że Poradnik pozwoli w przyjazny sposób poruszać się po wciąż mało znanej krainie unijnego rozporządzenia o ochronie danych osobowych.

2. RODO a prawo krajowe

RODO wiąże w całości i jest bezpośrednio stosowane od 25 maja 2018 r. we wszystkich państwach członkowskich. Jest zatem częścią krajowych przepisów bez potrzeby dokonywania jakichkolwiek dodatkowych działań wprowadzających. Mimo bezpośredniego stosowania obok RODO muszą lub mogą obowiązywać przepisy krajowe dotyczące ochrony danych osobowych.

W wielu przepisach RODO znajdują się odwołania do przepisów krajowych. Przedmiotowe odwołania mogą określać obligatoryjny lub fakultatywny zakres regulacji do dostosowania prawa krajowego do RODO. Do obligatoryjnej regulacji należą między innymi przepisy dotyczące organów nadzorczych (np. Prezes Urzędu Ochrony Danych Osobowych w Polsce; dalej PUODO lub Prezes UODO) czy przepisy dotyczące środków ochrony prawnej (np. skarga do Prezesa UODO w Polsce). W wielu przepisach RODO także przewiduje możliwość fakultatywnej regulacji krajowej. W przypadku braku takiej regulacji krajowej konieczne jest stosowanie generalnych zasad wynikających z RODO.

Ważnym zadaniem każdego państwa członkowskiego było (lub nadal jest) wprowadzenie do krajowego systemu prawnego przepisów zapewniających skuteczne stosowanie RODO, w tym przejrzenie obowiązujących przepisów szczególnych (sektorowych) odnoszących się do ochrony danych osobowych w celu usunięcia wszelkich niespójności z RODO. Dlatego w Polsce 25 maja 2018 r. weszła w życie ustawa z 10 maja 2018 r. o ochronie danych osobowych (dalej: OchrDanychU2018). Zakres ustawy nie objął wszystkich zagadnień RODO, które na gruncie przepisów krajowych są uregulowane w przepisach szczególnych. Powstał projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (planowany dzień wejścia w życie to 1 stycznia 2019 r.). Przepisy zawarte we wspomnianym projekcie dotyczą wielu ustaw obowiązujących w Polsce, w tym między innymi ustaw sektora cyfryzacji, energii, infrastruktury i budownictwa, finansów, statystyki publicznej, pracy, sportu i turystyki, zdrowia czy sprawiedliwości.

RODO wymaga zmiany licznych aktów prawnych obowiązujących w Polsce. Cały system prawny w Polsce powinien bowiem zostać dostosowany do RODO. Jednak należy pamiętać, że mimo braku wielu przepisów zapewniających skuteczne stosowanie RODO w Polsce, polskie przedsiębiorstwa powinny stosować RODO od 25 maja 2018 r., a nie od dnia wejścia w życie poszczególnych zmian w prawie krajowym.

3. Najczęstsze problemy po wprowadzeniu RODO

Podczas wdrożenia RODO podmioty sektora prywatnego, jak i publicznego oczekiwały gotowych rozwiązań, które – wydaje się – jeszcze długo będą przedmiotem wszechobecnej dyskusji o nowych europejskich standardach. Swoboda, jaką dał ustawodawca unijny (choćby poprzez wprowadzenie zasad przetwarzania danych), z jednej strony przyczyniła się do poszukiwania nowych rozwiązań, ale z drugiej strony wprowadziła swego rodzaju niepewność i różnorodność w rozumieniu tych samych zagadnień. Podmioty zaś, których dane osobowe są przedmiotem tej dyskusji, w sposób masowy zaczęły korzystać z przysługujących im praw podmiotowych, nie znając jednak ograniczeń wynikających z unijnych przepisów.

Z informacji uzyskanych 26 października 2018 r. od Agnieszki Świątek-Druś, rzecznika prasowego Urzędu Ochrony Danych Osobowych, wynika, że w pierwszych trzech miesiącach stosowania przepisów RODO do Urzędu wpłynęło 2400 skarg, czyli mniej więcej tyle, ile w całym roku 2017 – liczba ta wynosiła bowiem 2950. Wiele skarg musiało zostać zwróconych ich adresatom z uwagi na braki formalne w postaci niezłożenia własnoręcznego podpisu pod skargą wnoszoną w formie tradycyjnej czy nieopatrzenia kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP w przypadku skargi składanej w formie elektronicznej. Braki dotyczyły także nieokreślenia żądania, tj. niewskazania, jakich działań skarżący oczekuje od organu ds. ochrony danych osobowych. Jak informuje Prezes, zgłoszenia dotyczyły m.in.: wymuszania przez podmioty zgód na przetwarzanie danych osobowych w celach marketingowych, nieuprawnionego udostępniania danych osobowych osobom trzecim, przesyłania przez firmy niechcianej korespondencji, stosowania monitoringu wizyjnego czy przetwarzanie danych biometrycznych pracowników. Taki stan rzeczy mógł być spowodowany nieumiejętnym wypełnianiem przez administratorów obowiązku informacyjnego. Skoro RODO wymusiło na administratorach konieczność poinformowania osób, których dane są przetwarzane, podmioty przetwarzające dane lawinowo zaczęły informować o sobie, o danych, jakie mogą „zbierać", o odbiorcach tych danych. Niestety, nie zawsze wskazywane przez te podmioty podstawy przetwarzania były właściwe. Podmioty przetwarzające dane zapominają, że zmiana celu, dla którego dane zostały pozyskane, wymaga każdorazowo wypełnienia obowiązku informacyjnego w stosunku do osób, których dane dotyczą. Niekiedy brak jednoznacznej interpretacji pojęciowej wprowadzał samych administratorów w błąd co do prowadzonych działań na danych, np. czy w ramach działalności dokonują profilowania czy nie, czy też przekazują dane poza Europejski Obszar Gospodarczy.

Opieszałość krajowego ustawodawcy w uregulowaniu stanu prawnego w obszarach ponad 100 ustaw sektorowych czy brak wyjaśnień nie ułatwia przetwarzającym realizacji przepisów o ochronie danych. Trudności dla podmiotów przetwarzających dane pojawiły się już na samym wstępie prac nad wdrożeniem wytycznych RODO w określeniu, jaką rolę pełni dany podmiot w całym systemie ochrony danych osobowych. To z kolei rodziło kolejne pytania w zakresie zasadności podpisywania umów powierzenia. Niektóre podmioty wprost odmawiały ich zawarcia, inne uzależniały jej podpisanie od odpłatności.

Wiele firm, w tym także podmiotów publicznych, nie było przygotowanych na zmiany kadrowe w postaci czy to zatrudnienia nowych osób posiadających wiedzę i doświadczenie w administrowaniu danymi osobowymi, czy przeprowadzenia szkoleń dla kadry już zatrudnionej. To z kolei przyczyniło się do generowania przez te podmioty dodatkowych kosztów. Konieczność poniesienia znacznych kosztów odnotować można w zakresie wyposażenia podmiotów w narzędzia informatyczne spełniające kryteria bezpieczeństwa. Stworzenie mechanizmów ochrony fizycznej, ale przede wszystkim stworzenie infrastruktury umożliwiającej realizację praw osób, których dane dotyczą, nie powodując paraliżu w funkcjonowaniu działalności, dla niektórych stało się wyzwaniem. Do chwili obecnej wiele firm uważa, że posiadanie polityk i regulaminów jest wystarczające dla uznania, że działanie przedsiębiorstwa jest bezpieczne i zgodne z RODO.

Podmioty, które nie do końca poradziły sobie z wdrożeniem RODO, nie wiedzą, jak odpowiadać na pytania wynikające z korzystania z prawa do bycia zapomnianym czy usunięcia danych. Realizowany przez administratorów obowiązek informacyjny ułatwił osobom fizycznym dotarcie do źródła przetwarzania ich danych. Jednocześnie osoby te, kierując żądania do przedsiębiorców oraz powołując się na przysługujące im prawa, nie są świadome, że prawa te nie są absolutne. Przykładem jest choćby prawo do bycia zapomnianym (o którym mowa w art. 17 RODO), z którego nie zawsze osoby te mogą skorzystać. Nie będzie ono przysługiwało, gdy przetwarzanie danych będzie niezbędne do wywiązania się przez administratora z obowiązku wynikającego z przepisów prawa czy do wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Wyzwań, z jakimi muszą zmierzyć się podmioty przetwarzające dane, jest wiele. Najważniejszym wydaje się zmiana świadomości w postrzeganiu istoty danych osobowych, co oznacza, że regulacje przewidziane przez RODO muszą na stałe wpisać się w działalność podmiotów stykających się z danymi osobowymi.

4. Jak należy rozumieć RODO

Pomimo że ochrona danych osobowych nie jest niczym nowym w polskim porządku prawnym, data 25 maja 2018 r. u wielu przedsiębiorców, i nie tylko, wzbudziła niepokój. W dużej mierze uzasadniony. Przyczyny takiego stanu rzeczy były różne, choćby obawa przed brakiem jednolitych reguł interpretacyjnych w zrozumieniu nomenklatury związanej z ochroną danych.

Po wejściu w życie RODO każdy przedsiębiorca stanął przed koniecznością dostosowania prowadzonej działalności, organizacji pracy do zgodności ze specyficznymi regułami, procedurami i mechanizmami nałożonymi przez unijnego ustawodawcę, których rozumienie może być zgoła odmienne przez różne podmioty. Niemniej jednak implementacja głównych motywów i założeń nowych przepisów bez unijnej standaryzacji pojęciowej w obszarze danych byłaby niemożliwa, a co najmniej dalece utrudniona.

§ Motyw 10 preambuły RODO[1]:
Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Jeżeli chodzi o przetwarzanie danych osobowych w celu wypełnienia obowiązku prawnego, w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, państwa członkowskie powinny móc zachować lub wprowadzić krajowe przepisy doprecyzowujące stosowanie przepisów niniejszego rozporządzenia […].

Unijny ustawodawca w art. 4 RODO stworzył kanon pojęć, które stosowane w obszarze danych osobowych mają kluczowe znaczenie, pozostając jednak neutralnymi dla poszczególnych ustawodawstw unijnych.

Obok interpretacji definicji danych osobowych (sformułowanych i bliżej przedstawionych w rozdziale 5) niemal zawsze pojawiającymi się, gdy mowa o danych osobowych, są pojęcia administratora, podmiotu przetwarzającego czy przetwarzania. Na potrzeby niniejszej publikacji poniżej omawiamy wybrane zagadnienia związane z ww. pojęciami, wskazując jednocześnie, że pełny katalog pojęciowy odnajdziemy w art. 4 RODO.

W celu zapewnienia spójnego i zharmonizowanego podejścia interpretacyjnego na szczeblu europejskim Grupa Robocza Artykułu 29 RODO[2] wydała opinię (Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", WP 169) zawierającą wyjaśnienia odnoszące się do pojęć administratora danych i przetwarzającego dane. Praktyka stosowania przepisów o ochronie danych pokazała bowiem pojawiające się trudności w stosowaniu definicji administratora i podmiotu przetwarzającego. Trudności z interpretacją tych definicji pojawiają się zwłaszcza w złożonych okolicznościach, w których można przewidzieć wiele scenariuszy samodzielnego lub wspólnego funkcjonowania administratorów danych i przetwarzających o różnym stopniu autonomii i odpowiedzialności.

4.1. Administrator danych osobowych a podmiot przetwarzający dane osobowe

Status administratora danych osobowych może przysługiwać osobie fizycznej lub prawnej, organowi publicznemu, jednostce lub innemu podmiotowi. Jest to więc katalog otwarty. Administratorem może być zarówno podmiot prowadzący jednoosobową działalność gospodarczą, jak i podmiot działający w formie spółki z ograniczoną odpowiedzialnością. Dopiero precyzyjne określenie, czy dany podmiot jest administratorem danych, czy też nie, będzie się wiązało z podjęciem przez ten podmiot określonych działań w celu wypełnienia obowiązków wynikających z przepisów o ochronie danych osobowych.

---

[1] RODO jest aktem bardzo obszernym, zawiera bowiem 173 motywy oraz 99 artykułów. Dla prawidłowej wykładni RODO artykuły powinny być czytane łącznie z odpowiednimi motywami.

[2] Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy określa art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

SŁOWNICZEK
Administrator
Administrator oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
Artykuł 4 pkt 7 RODO

Jeżeli wymagania wobec poszczególnych podmiotów nie zostaną sprecyzowane w sposób wystarczająco jasny, istnieje ryzyko niepodjęcia przez te podmioty określonych działań, włącznie z brakiem zapewnienia gwarancji skutecznego stosowania prawa w praktyce.

Rozwój technologii informacyjno-komunikacyjnych, a także globalizacja przetwarzania danych powodują wzajemne przenikanie się ról administratora i podmiotu przetwarzającego, a tym samym trudności w płynnym określeniu pozycji podmiotu, który styka się z danymi osobowymi.

SŁOWNICZEK
Przetwarzanie
Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
Artykuł 4 pkt 2 RODO

Już samo gromadzenie przez określony podmiot danych osobowych klientów, kontrahentów, osób zatrudnionych sprawia, że spoczywa na nim obowiązek zapewnienia bezpieczeństwa administrowania takimi danymi. Administratorem danych osobowych możemy uczynić każdego pracodawcę wobec zatrudnionych pracowników. Będzie nim także operator sklepu internetowego (serwisu internetowego) w stosunku do użytkowników dokonujących zakupów z wykorzystaniem środków porozumiewania się na odległość czy świadczący usługę newsletter.

W praktyce przedsiębiorcy stają się administratorami wielu kategorii danych osobowych. Jest to uzależnione od charakteru prowadzonej działalności. Przedsiębiorcy są więc administratorami danych nie tylko w stosunku do swoich pracowników, współpracowników i klientów, ale również przedstawicieli dostawców, odwiedzających gości, podmiotów zgłaszających bądź odbierających produkty z reklamacji, kandydatów do pracy, potencjalnych klientów, którzy wysyłają zapytania ofertowe.

Grupa Robocza Artykułu 29 wyjaśnia, że posiadanie statusu administratora może wynikać z:
1) przyznanej podmiotowi przez przepisy prawa kompetencji do bycia administratorem,
2) kompetencji dorozumianych,
3) faktycznego wpływu podmiotu na dane osobowe.

Tabela 1. Status administratora – z czego wynika

Lp.	Status administratora wynika:	Komentarz
1	2	3
1.	Z przyznanej przez przepisy prawa kompetencji do bycia administratorem	Administrator danych lub szczegółowe kryteria potrzebne do jego wyznaczenia są określane przez przepisy prawa krajowego lub wspólnotowego. Niekiedy przepisy prawa, zamiast bezpośrednio wyznaczyć administratora danych lub określić kryteria jego wyznaczania, ustalają zadania lub nakładają na niego obowiązek gromadzenia i przetwarzania niektórych danych (np. banki, adwokaci).