

# Administrator danych

## – kto to taki?

**U**stawa z 29 sierpnia 1997 r. o ochronie danych osobowych (u.o.d.o.) posługuje się pojęciem „administratora danych”. Według jej art. 7 pkt 4, jest to organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych. Inaczej mówiąc, podmiot, który posiada wobec danych osobowych władztwo decyzyjne, tzn. decyduje np., jakie z nich gromadzi i przechowuje, na jakiej podstawie i komu je udostępnia oraz jakie stosuje wobec nich środki bezpieczeństwa.

Administratorem danych jest więc np. bank, urząd skarbowy, dyrektor szkoły, zakład ubezpieczeń społecznych, urząd gminy, spółdzielnia mieszkaniowa, spółka świadcząca usługi z zakresu zaopatrywania w wodę czy odbioru ścieków.

Niektóre podmioty mają problem z właściwym wskazaniem administratora danych, choć w przypadku jednostek publicznych jego rozwiązanie nierzadko znajduje się w przepisach prawa, stanowiących podstawę utworzenia zbioru, w którym przetwarzane są dane osobowe. Zazwyczaj wskazują one, kto jest odpowiedzialny za utworzenie i prowadzenie zbioru danych osobowych oraz na jakich zasadach winien to robić. Przykładowo, administratorem danych zawartych w zbiorach PESEL oraz ogólnokrajowej ewidencji wydanych i utraconych dowodów osobistych jest minister właściwy do spraw wewnętrznych (w myśl art. 44i ust. 3 Ustawy z 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych).

Z punktu widzenia u.o.d.o. ważne jest, aby każdy administrator danych wskazał podstawę prawną przetwarzania danych osobowych, a każda osoba, której dane są wykorzystywane, o tym wiedziała, była świadoma swoich praw z tym związanych oraz mogła je realizować. Jednak obowiązek wskazania podstawy prawnej przetwarzania danych jest tylko jednym z wielu, jakie u.o.d.o. nakłada na administratora. Spełnienie przez niego wszystkich obowiązków jest równoznaczne z respektowaniem zasad wynikających z u.o.d.o., w tym praw każdej osoby, której dane są przetwarzane.

### Uprawnienie do przetwarzania danych osobowych

Podstawowym obowiązkiem każdego administratora danych jest wskazanie podstawy prawnej do legalnego przetwarzania

danych osobowych. Są one wymienione w art. 23 ust. 1 u.o.d.o. – jeśli chodzi o przetwarzanie danych osobowych tzw. zwykłych – i w art. 27 ust. 2 – gdy chodzi o dane szczególnie chronione. Spełnienie przez administratora danych co najmniej jednego z wymienionych w tych przepisach warunków oznacza, że przetwarza on dane osobowe zgodnie z prawem. Przykładowo, bank przetwarza dane osobowe swoich kredytobiorców na podstawie i w zakresie wskazanym przede wszystkim w ustawie Prawo bankowe. Tym samym spełnia warunek z art. 23 ust. 1 pkt 2 u.o.d.o., w myśl którego przetwarzanie danych jest dopuszczalne, gdy zezwalają na to przepisy prawa.

### Obowiązek informacyjny

W zależności od tego, czy administrator pozyskuje dane bezpośrednio od osoby, której one dotyczą, czy też z innych źródeł, np. od osoby trzeciej, czy ze źródeł powszechnie dostępnych, ma on obowiązek poinformowania o tym każdą osobę, której dane gromadzi (chyba że ustawa zwalnia z tego obowiązku). Spełnienie obowiązku informacyjnego wiąże się z przekazaniem osobie, której dane dotyczą, pewnych informacji, aby mogła skorzystać z przysługujących jej uprawnień, np. prawa do wniesienia sprzeciwu wobec przetwarzania jej danych czy skargi na administratora danych.

A zatem w przypadku zbierania danych osobowych od osoby, której one dotyczą (art. 24 ust. 1 u.o.d.o.), administrator jest obowiązany poinformować ją o: adresie swojej siedziby i pełnej nazwie (imieniu, nazwisku, miejscu zamieszkania – w przypadku gdy jest osobą fizyczną), celu zbierania danych, a zwłaszcza o tym, komu zostaną one przekazane, prawie dostępu do treści swoich danych oraz ich poprawiania, dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. Administrator nie musi informować

osoby, od której dane pozyskał, jedynie wtedy, gdy posiada ona te informacje bądź gdy przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania (art. 24 ust. 2 ustawy).

Natomiast w przypadku zbierania danych osobowych nie od osoby, której one dotyczą (art. 25 ust. 1 ustawy), administrator jest obowiązany poinformować ją, bezpośrednio po utrwaleniu zebranych danych – oprócz ww. elementów – również o źródle danych oraz uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8. Zalicza się do nich prawo do wniesienia pismennego, umotywowanego żądania zaprzestania przetwarzania danych osobowych ze względu na szczególną sytuację (pkt 7) oraz prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych (pkt 8).

Również w przypadku pozyskiwania danych osobowych z różnych źródeł administrator danych nie musi spełnić obowiązku informacyjnego wobec osoby, której dane dotyczą, jeśli – oprócz ww. okoliczności – dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania. Obowiązku informacyjnego nie muszą spełniać także podmioty publiczne lub wykonujące zadania publiczne na podstawie przepisów prawa. Przykładowo z obowiązku określonego w art. 25 ust. 1 u.o.d.o. zwolniony jest administrator danych (minister właściwy do spraw wewnętrznych), przetwarzający dane osobowe na potrzeby ewidencji pojazdów (zgodnie z art. 80b ust. 4 Ustawy z 20 czerwca 1997 r. – Prawo o ruchu drogowym). Dane osobowe bez wiedzy osoby, której dane dotyczą, mogą zbierać także detektywi – zezwala na to art. 8 ust. 4 Ustawy z 6 lipca 2001 r. o usługach detektywistycznych. Zgodnie z nim, detektyw przy przetwarzaniu danych osobowych jest obowiązany stosować przepisy u.o.d.o., z wyłączeniem m.in. art. 25 ust. 1.

### Szczególna staranność

Zgodnie z art. 26 ust. 1 ustawy, administrator przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których one doty-



czą, a zwłaszcza jest obowiązany zapewnić, aby były one przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, oraz przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Przetwarzanie danych zgodnie z prawem oznacza – jak wspomniano – że administrator danych legitymuje się co najmniej jedną przesłanką określoną w art. 23 ust. 1 lub w art. 27 ust. 2 ustawy (zasada legalności).

Obowiązek zbierania danych dla oznaczonych, zgodnych z prawem celów oznacza, że administrator może wykorzystywać dane tylko w tym celu, dla którego je pozyskał (zasada celowości). Przykładowo, uczelnia wyższa nie może wykorzystywać danych osobowych studentów dla celów marketingowych, jeśli gromadzi je dla przeprowadzenia procesu kształcenia. Ustawa o.d.o. dopuszcza jednak wykorzystywanie danych dla innych celów niż je pozyskano, a mianowicie dla celów badań naukowych, dydaktycznych, historycznych lub statystycznych, ale pod warunkiem, że nie naruszy to praw i wolności osoby, której one dotyczą (art. 26 ust. 2).

Administrator ma obowiązek przestrzegać, aby przetwarzane przez niego dane osobowe były merytorycznie poprawne (zasada merytorycznej poprawności) oraz adekwatne do celu ich przetwarzania (zasada adekwatności). Adekwatność danych oznacza, że gromadzone i wykorzystywane powinny być tylko dane niezbędne do określonego celu. Przykładowo przedsiębiorstwo wod-kan, zawierając z mieszkańcami umowy na dostawę wody, powinno gromadzić tylko dane niezbędne do ich realizacji. W przypadku żądania informacji, które budziłyby wątpliwości drugiej strony umowy, może ona zwrócić się o wskazanie podstawy prawnej żądania.

Administrator danych ma także obowiązek przechowywania ich nie dłużej, niż jest to konieczne dla realizacji celu, dla którego je zgromadził (zasada ograniczenia czasowego). Jeżeli zatem został osiągnięty cel przetwarzania danych, to należy je usunąć. Jednocześnie za niezgodną z u.o.d.o. należy uznać sytuację, gdy cel przetwarzania danych osobowych jest bliżej niesprecyzowany, a jego realizacja odległa w czasie. Przykładowo, dopuszczalne jest przechowywanie danych w tzw. księgach wejść i wyjść, tworzonych przez podmioty na potrzeby zapewnienia bezpieczeństwa osób pracujących w danym obiekcie, nie dłużej niż przez jeden rok.

### Środki techniczne i organizacyjne

W myśl u.o.d.o. każdy administrator jest zobowiązany do dbałości o dane osobowe, a przepisy jej rozdziału 5 określają ogólne zasady ich zabezpieczania. Zgodnie z jej art. 36 ust. 1, administrator danych musi zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a zwłaszcza powinien zabezpieczyć je przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Wybór odpowiednich środków zabezpieczających pozostawia jednak do uznania konkretnemu administratorowi. Ważne jest, aby administrator danych zastosował takie instrumenty organizacyjne i techniczne, za pomocą których będzie w stanie wyeliminować zagrożenia utraty, zmiany czy zniszczenia danych osobowych.

Administrator ma obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz zastosowane przez niego środki techniczne i organizacyjne (art. 36 ust. 2 ustawy).

Stosownie do art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora. Tym samym to na nim spoczywa obowiązek za dbania, aby każdej osobie, która będzie wykonywała czynności związane z przetwarzaniem danych osobowych, zostało wydane stosowne upoważnienie. Przykładowo pracodawca ma obowiązek wydać takie upoważnienie kadrowej, gdyż jej praca wiąże się z przetwarzaniem danych innych pracowników, w tym z dostępem do różnego rodzaju informacji, np. o ich zarobkach. Ale musi wydać takie upoważnienie także innym, niezatrudnionym u niego osobom, jeśli w ramach pewnych czynności, np. naprawy sprzętu, będą oni mieli dostęp do danych osobowych jego pracowników.

Administrator ma obowiązek prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, która powinna zawierać imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres tego upoważnienia, a także identyfikator, jeśli dane są przetwarzane w systemie informatycznym (art. 39 ust. 1 ustawy).

Ponadto administrator musi zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 ustawy). Wszystkie czynności związane z bezpieczeństwem przetwarzanych informacji może on wykonywać sam bądź też wyznaczyć w tym celu tzw. administratora

bezpieczeństwa informacji (ABI), nadzorującego przestrzeganie zasad ochrony (art. 36 ust. 3 ustawy). Jest to osoba odpowiedzialna za nadzór nad procesem przetwarzania danych osobowych, powinna więc posiadać niezbędną wiedzę w zakresie ich ochrony.

Szczegółowe warunki zabezpieczenia danych osobowych określone są w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Opisuje ono także środki bezpieczeństwa, jakie należy zastosować w celu ochrony danych. Ich dobór uzależniony jest od przyjętego dla danego zbioru poziomu bezpieczeństwa danych w systemie informatycznym (podstawowego, podwyższonego i wysokiego).

### Zgłoszenie zbioru do rejestracji

Na administratorze danych spoczywa wynikający z art. 40 ustawy obowiązek zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO). Nie dotyczy to jednak administratorów tych danych, które u.o.d.o. wymienia w art. 43 ust. 1. Każdy administrator przed zgłoszeniem zbioru powinien sprawdzić, czy nie podlega on zwolnieniu z rejestracji. Zgłoszenia takiego zbioru do rejestracji GIODO należy dokonać poprzez wypełnienie urzędowego formularza zgłoszenia, którego wzór określa załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji GIODO. Do przedstawienia innych dokumentów, które mogą mieć znaczenie w procesie rejestracji, administrator może zostać wezwany jako strona postępowania administracyjnego, prowadzonego w celu rejestracji zgłoszonego zbioru (rejestracji można dokonać także przez Internet za pomocą elektronicznej platformy e-GIODO).

Jeśli administrator zgłasza do rejestracji zbiór zawierający tzw. dane zwykłe, może rozpocząć ich przetwarzanie od momentu zgłoszenia tego zbioru. Wówczas, po zarejestrowaniu, GIODO może, na wniosek takiego administratora, wydać mu zaświadczenie o zarejestrowaniu zbioru. Natomiast gromadzenie danych szczególnie chronionych administrator może rozpocząć dopiero po zarejestrowaniu zbioru – zaświadczenie GIODO jest tu wydawane obligatoryjnie, po zarejestrowaniu zbioru.

Michał Serzycki,  
Generalny Inspektor Ochrony  
Danych Osobowych