dr Jarosław Greser

# Zasady przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych

18

**Autor**
jest prawnikiem, adiunktem na Uniwersytecie im. Adama Mickiewicza w Poznaniu.

**Słowa kluczowe:**
ochrona danych osobowych, RODO, dane wrażliwe

**Keywords:**
personal data protection, GDPR, sensitive data

**DOI:**
10.26368/17332265-041-1-2018-1

**Abstrakt**
Wejście w życie reformy systemu ochrony danych osobowych jest wyzwaniem dla wszystkich podmiotów, które te dane przetwarzają, w tym organizacji pozarządowych – bez względu na wielkość czy cel działania. Nowe przepisy co do zasady nie różnicują obowiązków dla organizacji społecznych i przedsiębiorstw, dlatego konieczne jest przygotowanie się do wprowadzanych zmian. W artykule omówiono główne założenia reformy i jej cel, który jest podstawą interpretacji przepisów zawartych w aktach prawnych. Szczegółowej analizie poddano pojęcie danych osobowych i zasady przetwarzania danych sensytywnych przez organizacje pozarządowe. Opisano zakres przedmiotowy i podmiotowy obowiązywania ogólnego rozporządzenia o ochronie danych osobowych oraz pojęcie i zakres zgody na przetwarzanie danych.

**Abstract**
Entry into force of the reforms to Poland's personal data protection system poses a challenge for all entities whose operations include gathering and processing of personal data, non-governmental organisations (whatever their size or object of activities) included. The new laws, in general, do not differentiate between the duties imposed on social organisations and on business enterprises; accordingly, at least some preparation for their effective implementation will be necessary. This article summarises the main premises of this reform and its stated objectives, which are bound to be looked to for guidance as to how the legislative provisions should be interpreted in practice. Especial attention is devoted to the very concept of personal data and to the rules applicable to processing of sensitive data by NGOs, and also to the objective and subjective ambit of the general regulation concerning personal data protection as well as the concept, and scope, of permission for data processing.

Dwudziestego piątego maja 2018 roku wchodzi w życie reforma systemu ochrony danych osobowych. Jej celem jest ujednolicenie praw i obowiązków związanych z ochroną danych osobowych w całej Unii Europejskiej. Reforma obejmuje także organizacje pozarządowe, które w zasadzie muszą wdrożyć wszystkie jej regulacje.

Obecnie istniejące przepisy w zakresie danych osobowych opierają się na dyrektywie 95/46/WE[1], która została przyjęta w 1995 roku. Zawarte w niej rozwiązania są nieadekwatne do poziomu rozwoju technologii informacyjnych, a także nie uwzględniają powstania całego sektora biznesu opartego na przetwarzaniu informacji. W związku z tym organy Unii Europejskiej rozpoczęły prace nad reformą, której rezultatem jest przyjęcie przez Parlament Europejski i Radę Unii Europejskiej rozporządzenia 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), a także dodatkowych regulacji szczegółowych[2].

Wybór formy rozporządzenia nie jest przypadkowy. Na poziomie prawa unijnego jest to akt prawny bezpośrednio stosowalny – wywołuje natychmiastowe skutki prawne od momentu wejścia w życie na poziomie zarówno Unii Europejskiej, jak i państw członkowskich (Zawidzka-Łojek 2012, s. 29). Umożliwia również powołanie się na jego regulacje przed sądem krajowym. Ponadto ma pierwszeństwo w wypadku kolizji z prawem krajowym. W Polsce zgodnie z art. 91 ust. 3 Konstytucji Rzeczypospolitej Polskiej rozporządzenie unijne jest stosowane przed prawem wewnętrznym, o ile przepis taki znajduje się w ustawie lub akcie niższego rzędu.

Zabieg ten ma doprowadzić do powstania jednolitych zasad ochrony danych osobowych wszystkich osób przebywających na terenie Unii Europejskiej. Przewidziano jednak możliwość odrębnej regulacji niektórych spraw przez państwa członkowskie. Polska skorzystała z tej możliwości i zawarła modyfikacje w projektowanej ustawie o ochronie danych osobowych (Ustawa o ochronie danych osobowych, projekt nr UC101, wersja z 14 września 2017 roku [dalej: projekt UC101])[3]. Fundamentalna treść praw i obowiązków uregulowana w RODO będzie jednak wynikała bezpośrednio z przepisów unijnych. Ma to duże znaczenie na poziomie praktycznym. Dotychczas do określenia wymogów dotyczących danych osobowych wystarczyło posługiwanie się przepisami prawa polskiego. Od wejścia w życie RODO konieczna będzie znajomość przepisów unijnych, zasad ich wykładni i relacji do polskiego prawa.

Nawiązując do zasad wykładni RODO, wskazówek w tym zakresie dostarcza preambuła tego aktu (Morawska 2017, s. 34–39). W motywie pierwszym podkreślono, że prawo do ochrony danych należy do praw podstawowych Unii Europejskiej, chronionych Kartą praw podstawowych. Akt ten ma moc prawną równą Traktatowi o funkcjonowaniu Unii Europejskiej (Kawecki 2017, s. 93). Jednocześnie w literatu-

1 Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (DzU WE L 281).

2 Dyrektywy dotyczącej przetwarzania danych w postępowaniach karnych, dyrektywy o wykorzystaniu danych dotyczących przelotu pasażera oraz rozporządzenia w sprawie prywatności i łączności elektronicznej.

3 Projekt ustawy obejmuje między nimi modyfikacje dotyczące obniżenia kar za naruszenie przepisów o ochronie danych osobowych dla podmiotów publicznych Ponadto obniża wiek, w którym można wyrazić zgodę na przetwarzanie danych osobowych, do trzynastego roku życia. Z perspektywy organizacji pozarządowych proponowane zmiany mają marginalne znaczenie.

rze wskazuje się, że zobowiązane do jego stosowania są zarówno organy unijne, jak i organy państw członkowskich (Gajda 2014, s. 77). Prawodawca unijny przyznaje więc temu prawu do ochrony danych osobowych szczególny charakter. Dlatego prowadząc wykładnię przepisów, trzeba będzie uwzględnić odniesienia systemowe, szczególnie to, że naruszenie zasad ochrony danych osobowych może być również naruszeniem prawa do prywatności (Kozik 2017, s. 21).

Należy także zwrócić uwagę, że podstawą prawną wprowadzenia RODO jest art. 16 Traktatu o funkcjonowaniu Unii Europejskiej. Wskazuje on, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Należy się zgodzić z postulowanym w literaturze stanowiskiem, że wybranie tego przepisu jako podstawy prawnej powoduje, że w interpretacji RODO prymat ma cel efektywnej ochrony praw jednostki (Grzelak 2017, s. 19).

W motywie drugim RODO wskazano, że celem rozporządzenia jest działanie na rzecz „tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także do pomyślności ludzi". Cele zawarte w motywach pierwszym i drugim nie pozostają ze sobą w sprzeczności. Mogą jednak wchodzić w konflikt. W tej sytuacji interpretacja przepisów będzie wymagała uwzględnienia obu wskazanych wartości w najszerszy możliwy sposób przez ich wyważenie (por. Kordela 2012, s. 265). Jest to podkreślone w motywie czwartym, w którym wprost wskazuje się, że prawo do ochrony danych osobowych nie jest prawem bezwzględnym.

### Założenia reformy systemu ochrony danych osobowych

Znajomość założeń reformy systemu ochrony danych osobowych pozwala ujawnić założenia aksjologiczne prawodawcy, którymi kierował się w trakcie jej wdrażania. Ma to duże znaczenie w wymiarze wykładni celowościowej (Wronkowska, Ziembiński 1997, s. 40–42). Inaczej rzecz ujmując, dzięki znajomości założeń możemy wybrać tę interpretację, która pozwala najpełniej chronić stany pożądane przez prawodawcę.

Punktem wyjścia jest wskazane w motywie szóstym tło społeczne reformy. Wskazuje się w nim, że „skala zbierania i wymiany danych osobowych znacznie wzrosła", między innymi dzięki postępowi technologicznemu, ale także globalizacji. Nastąpiło przyspieszenie wymiany danych, znacznie zwiększyła się także szansa nadużyć czy przestępstw związanych z ich wykorzystywaniem. W tej sytuacji prawodawca postanowił wyważyć dwie wartości. Z jednej strony ułatwienie swobodnego przepływu danych osobowych i rozwój technologii powstałych na ich podstawie. Z drugiej strony – zapewnienie wysokiego stopnia ochrony tych danych.

Reforma zmienia całkowicie model systemu ochrony danych osobowych, gdyż RODO odchodzi od sztywno wyznaczonych zasad postępowania na rzecz *risk based approach* (Litwiński 2017, s. 54). Tym samym więc to na administratorze danych będzie spoczywał obowiązek oceny ryzyka ich przetwarzania i wyboru adekwatnych środków zapewnienia bezpieczeństwa przetwarzania danych. W polskich realiach wyrazem tego będzie uchylenie rozporządzeń ministerialnych, które wskazywały minimalną dokumentację dotyczącą przetwarzania danych osobowych, wymagania techniczne i organizacyjne oraz zakres działań administratorów bezpieczeństwa

informacji[4]. W dotychczasowej praktyce były one podstawą działań w zakresie danych osobowych dla wielu organizacji pozarządowych. Po wejściu w życie reformy nie będzie normatywnego odnośnika w tym zakresie. Nie oznacza to jednak, że przyjęte systemy ochrony czy dokumenty stracą moc. Jeśli analiza przeprowadzona w organizacji potwierdzi, że są wystarczające do ochrony przetwarzanych danych, z powodzeniem można je zaadaptować do wymogów RODO. Będzie to wymagało jednak zaplanowania i wdrożenia procesu oceny własnych działań w zakresie danych osobowych.

Kolejnym przejawem podejścia zakładającego odrzucenie nakazywania określonych zachowań jest brak konieczności rejestrowania zbiorów danych osobowych. Projekt UC101 nie przewiduje takiej możliwości, a nakaz takiego zachowania nie wynika z RODO. Zmiany będą dotyczyły również powoływania administratorów bezpieczeństwa informacji. Dotychczas polskie przepisy dawały administratorowi alternatywę: powołanie administratora bezpieczeństwa informacji lub rejestrację zbioru RODO nakłada obowiązek powołania inspektora ochrony danych w nielicznych wypadkach, głównie wobec podmiotów, których działalność koncentruje się na przetwarzaniu danych (art. 37 RODO). Z perspektywy organizacji pozarządowej sytuacja taka wystąpi bardzo rzadko.

Kolejnym celem było – wzmiankowane wyżej – ujednolicenie praw i obowiązków podmiotów przetwarzających dane osobowe, a także wprowadzenie równorzędnych kar za naruszenia przepisów w państwach członkowskich (motywy jedenasty i trzynasty RODO). Sankcje te muszą być skuteczne, proporcjonalne i odstraszające (motyw sto pięćdziesiąty pierwszy i art. 83 RODO). Maksymalną granicą kary administracyjnej jest kwota 20 milionów euro. Przy wymiarze kary bierze się jednak pod uwagę nie tylko stopień naruszenia przepisów, ale także sytuację majątkową administratora danych.

Przygotowując reformę, zwrócono uwagę na różnicę w sytuacji faktycznej między korporacjami a małymi podmiotami. Co prawda przepisy przewidują nieliczne wyjątki od zastosowania samych przepisów, ale w motywie trzynastym wskazuje się, żeby „instytucje i organy Unii, państwa członkowskie i ich organy nadzorcze, [...] stosując niniejsze rozporządzenie, uwzględniały szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw". Sam przepis nie odnosi się bezpośrednio do organizacji pozarządowych, ale, jak się wydaje, będzie miał również do nich zastosowanie. Zgodnie z zaleceniem Komisji 2003/361/WE średnie przedsiębiorstwo zatrudnia mniej niż 250 osób. Biorąc pod uwagę realia trzeciego sektora, tylko w jednostkowych sytuacjach liczba ta będzie przekroczona. Jednocześnie postulat specjalnego traktowania należy rozciągnąć na organizacje nieprowadzące działalności gospodarczej. Celem zróżnicowania wskazanego w motywie trzynastym

4 W tym zakresie należy wskazać szczególnie dwa akty: Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU 2004, nr 100, poz. 1024); Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (DzU 2015, poz. 745).

była zakładana różnica w dostępności zasobów dla małych i dużych podmiotów. Organizacje nieprowadzące działalności gospodarczej, w zdecydowanej większości wypadków będące w gorszej sytuacji finansowej i organizacyjnej od firm porównywalnej wielkości, powinny być zatem traktowane szczególnie. Nie oznacza to jednak braku konieczności stosowania przepisów, a jedynie branie pod uwagę ograniczenia w możliwościach.

### Pojęcie danych osobowych

Omawiane rozporządzenie wprowadza definicję legalną danych osobowych. Zgodnie z nią dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Mogą to być zarówno pojedyncze informacje typu imię i nazwisko, jak i zestawienia informacji. W orzecznictwie wskazuje się, że dane osobowe obejmują nazwisko w zestawieniu z numerem telefonu lub informacjami dotyczącymi warunków pracy czy spędzania wolnego czasu (wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-101/01 Bodil Lindqvist przeciwko Szwecji). W tym zakresie definicja nie różni się od dotychczas stosowanej zarówno w ustawodawstwie, jak i w doktrynie czy orzecznictwie.

Doprecyzowano pojęcie „możliwa do zidentyfikowania osoba fizyczna". Przyjęto, że jest to osoba, którą można bezpośrednio lub pośrednio zidentyfikować. Forma tej identyfikacji jest dowolna, ale w RODO wymieniono przykładowe identyfikatory: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy. W dotychczasowej praktyce stosowania przepisów o ochronie danych osobowych zarysowały się dwa stanowiska w zakresie oceny możliwości identyfikacji. Pierwsze z nich – obiektywne – wskazywało, że danymi osobowymi są takie informacje, na podstawie których można zidentyfikować osobę fizyczną niezależnie od możliwości administratora. Na przykład posiadanie adresu IP internauty przez właściciela strony jest daną osobową, ponieważ po zestawieniu danych będących w posiadaniu dostawcy Internetu jest możliwe zidentyfikowanie osoby. Drugie stanowisko – koncepcja subiektywna – wskazywało, że możliwość identyfikacji musi nastąpić w ramach środków własnych administratora danych (Litwiński 2017, s. 51).

W literaturze wskazuje się, że w dyrektywie 95/46/WE i praktyce jej implementacji zastosowano stanowisko subiektywne (*ibidem*, s. 53). Jednocześnie orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej zmierza w kierunku koncepcji obiektywnej. W orzeczeniu C-582/14 Trybunał stwierdził, że dynamiczny adres IP należy do kategorii danych osobowych, gdy podmiot, który go przetwarza, dysponuje środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby odwiedzającej stronę internetową dzięki dodatkowym informacjom, jakimi dysponuje dostawca Internetu podmiotu, którego adres jest przetwarzany (wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-582/14 Patrick Breyer przeciwko Niemcom). Należy zwrócić uwagę, że w polskim systemie prawnym są takie możliwości. Ujawnienie przez operatora telekomunikacyjnego danych osoby posługującej się adresem IP może mieć podstawę w art. 23 ust. 1 pkt 5 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (dalej: ustawa z 1997 roku) i to mimo tego, że są chronione tajemnicą telekomunikacyjną (wyrok Naczelnego Sądu Admini-

stracyjnego z 19 maja 2011 roku, I OSK 1079/10). W pewnych sytuacjach podstawą ujawnienia jest postępowanie karne prowadzone w wypadku zniesławienia lub zniewagi (art. 212 i 216 Kodeksu karnego).

Regulacje RODO nie zawierają ograniczenia, znanego z polskiej ustawy, wyłączającego spod reżimu ochrony danych osobowych informacje, których wykorzystanie do określenia tożsamości osoby wymagałoby nadmiernych kosztów, czasu lub działań. Co prawda motyw dwudziesty pierwszy wskazuje, że przy stwierdzeniu, czy dana informacja może identyfikować osobę fizyczną, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania. Preambuła nie ma jednak charakteru normatywnego (por. wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-134/08 Hauptzollamt Bremen przeciwko J.E. Tyson Parketthandel GmbH), a jej zadaniem jest odtworzenie celów prawodawcy wykorzystywanych w czasie wykładni przepisów (Zieliński 2017, s. 297–300). Ponadto Trybunał Sprawiedliwości Unii Europejskiej wykazuje skłonność do odstępstwa od językowego znaczenia wykładni, jeśli jest to uzasadnione koniecznością osiągania celów Unii Europejskiej (Grzelak 2017, s. 13). Należy zatem ostrożnie traktować zastrzeżenie i w razie wątpliwości przyjmować koncepcję obiektywną (inaczej: Litwiński 2017, s. 54).

Z perspektywy organizacji pozarządowych duże znaczenie można przypisać identyfikacji opierającej się na jednym albo kilku szczególnych czynnikach określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Będą się w to wpisywać zarówno niepełnosprawność czy poglądy polityczne, jak i hobby lub pełnienie funkcji w organizacji. Na przykład stwierdzenie „prezes stowarzyszenia X" umożliwia łatwą identyfikację osoby fizycznej, odnosi się ono zatem do jej danych osobowych.

Jednocześnie wprowadzono definicje danych genetycznych, danych biometrycznych i danych dotyczących zdrowia. W praktyce funkcjonowania organizacji pozarządowych największe znaczenie będą miały te ostatnie. Są one rozumiane jako dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. Z tą kategorią danych są związane szczególnego rodzaju obowiązki w zakresie ich przetwarzania. Jednocześnie są one niezbędne w organizacjach o charakterze samopomocowym czy pacjenckim, jak i prowadzącym działalność gospodarczą w zakresie rehabilitacji.

Rozporządzenie RODO wprowadza również definicję przetwarzania danych osobowych. Jest to operacja lub zestaw operacji wykonywanych na danych osobowych albo zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. W zakres przetwarzania danych wchodzi ich zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Wskazane wyżej działania należy traktować jako przykłady. Możliwe, że wraz z rozwojem techniki powstaną inne formy przetwarzania danych, nieujęte w tym katalogu.

Definicja zawarta w RODO zastąpi stosowaną obecnie definicję z ustawy z 1997 roku. Należy zauważyć, że poza elementem dotyczącym identyfikacji nie

wprowadza ona nowości normatywnej. Należy ją traktować jako doprecyzowanie obecnie funkcjonujących ustaleń terminologicznych. W tym zakresie nie powinno to rodzić wątpliwości w stosowaniu przez organizacje pozarządowe.

Regulacja RODO wprowadza także własną definicję zbioru danych. Zgodnie z nią zbiorem tym jest uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy też rozproszony funkcjonalnie lub geograficznie (art. 4 pkt 6 RODO). Należy pamiętać, że kryteria wyszukiwania danych w zbiorze mogą mieć charakter osobowy, na przykład nazwisko lub PESEL, albo nieosobowy, na przykład sygnatura akt lub data odebrania korespondencji (por. Korga 2017, s. 51). W takim wypadku dane te stanowią jeden zbiór.

Przetwarzanie danych może następować w oddzielonych od siebie funkcjonalnie lub geograficznie oddziałach czy innych jednostkach organizacyjnych. Dane uczestników jednego projektu, które znajdują się w różnych biurach, będą więc stanowić ten sam zbiór. Ponieważ zarówno RODO, jak i projekt UC101 nie zakładają możliwości urzędowej rejestracji zbiorów, definicja ta będzie miała zastosowanie do ochrony danych. W ramach oceny ryzyka koniecznie będzie stwierdzenie, czy określone dane stanowią jeden zbiór, a w wypadku ich rozproszenia trzeba będzie podjąć adekwatne środki w zakresie ich ochrony.

### Zakres obowiązywania RODO

Aby osiągnąć cele wskazane wyżej, RODO wprowadza nowe uprawnienia dla osób, których dane są przetwarzane, i nakłada na administratorów nowe obowiązki. Z perspektywy organizacji pozarządowych podstawową kwestią jest stwierdzenie, czy nowe regulacje mają zastosowanie, a jeśli tak – to w jakim zakresie.

Rozporządzenie RODO wyróżnia dwa podmioty, których dotyczą obowiązki wskazane w tych przepisach. Pierwszym z nich jest administrator danych – rozumiany jako osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem mogą być zatem zarówno organizacje pozarządowe w rozumieniu art. 3 ust. 2 Ustawy o działalności pożytku publicznego i o wolontariacie (t.j.: DzU 2016, poz. 1817 ze zm.), jak i podmioty prowadzące działalność pożytku publicznego. W zakres tej definicji wchodzą również grupy nieformalne oraz jednostki organizacyjne niemające osobowości prawnej, jak stowarzyszenia zwykłe. Punktem wyjścia jest bowiem nie forma prawna, ale fakt wskazywania celów i sposobów przetwarzania danych. Należy pamiętać, że w wypadku osób prawnych administratorem będzie ta osoba, a nie członkowie organów działających w jej imieniu. Stąd administratorem jest fundacja lub stowarzyszenie, nie zaś prezes czy zarząd.

Podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. W tym wypadku organizacja nie decyduje o celach i sposobach przetwarzania danych, tylko prowadzi operacje na nich w zakresie wskazanym przez administratora. Podstawą bycia podmiotem przetwarzającym jest najczęściej umowa (por. motyw

pięćdziesiąty piąty oraz art. 22 ust. 3 i art. 29 RODO). Na przykład stowarzyszenie ma dane darczyńców i zleca ich analizę badaczowi pod kątem wyboru osób, które potencjalnie będą najlepszymi odbiorcami kolejnej kampanii. W tym wypadku stowarzyszenie jest administratorem, ponieważ ustala cel, którym są badania marketingowe, i sposób przetwarzania, czyli przeprowadzenie analiz przez zewnętrzny podmiot. Z kolei badacz będzie podmiotem przetwarzającym dane, ponieważ może prowadzić na nich operacje tylko w zakresie wskazanym w umowie. Nie ma tu znaczenia odpłatny czy nieodpłatny charakter umowy, istotny jest fakt powierzenia danych do przetwarzania. Możliwe jest również dalsze powierzenie danych przez podmiot, któremu dane powierzono. W literaturze wskazuje się, że będzie to wymagać zgody administratora danych (Żabówka 2017, s. 178). Należy się zgodzić z tym postulatem, ponieważ do oceny skutków prawnych umowy o powierzenie danych stosujemy przepisy o zleceniu (art. 750 Kodeksu cywilnego). Zgodnie zatem z art. 738 par. 1 Kodeksu cywilnego przyjmujący zlecenie może powierzyć wykonanie zlecenia osobie trzeciej w trzech wypadkach. Wtedy, gdy to wynika z umowy lub ze zwyczaju, albo gdy jest do tego zmuszony przez okoliczności. O ile pierwsza sytuacja nie budzi wątpliwości, o tyle dwie pozostałe nie mają zastosowania zważywszy na art. 29 RODO. Wskazuje on, że przetwarzanie może wystąpić wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii Europejskiej lub prawo państwa członkowskiego – jako *lex specialis* uchyla zatem przesłanki zwyczaju lub okoliczności.

Rozróżnienie między administratorem danych a podmiotem przetwarzającym ma podstawowe znaczenie z perspektywy odpowiedzialności i obowiązków nałożonych przez przepisy. Co do zasady głównym podmiotem odpowiedzialnym jest administrator. Odpowiedzialność podmiotu przetwarzającego wynika z poszczególnych przepisów – na przykład w zakresie ochrony danych – i z umowy zawartej z administratorem.

Kolejną kwestią jest zakres stosowania przepisów. Artykuł 2 RODO wskazuje, że będą one miały zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Jednocześnie od zakresu stosowania przewidziano tylko cztery wyjątki, a żaden z nich nie dotyczy organizacji pozarządowych.

W kwestii zakresu terytorialnego stosowania omawianej regulacji w art. 3 RODO wskazano dwie zasady. Pierwsza to obowiązek stosowania rozporządzenia do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii Europejskiej, niezależnie od tego, czy przetwarzanie odbywa się w Unii Europejskiej.

Druga dotyczy organów mających siedzibę poza Unią Europejską, jeżeli czynności przetwarzania wiążą się z oferowaniem towarów lub usług przebywających w Unii Europejskiej lub monitorowaniem ich zachowania, o ile do zachowania tego dochodzi na jej terenie. Z pierwszej zasady wynika, że nowe przepisy będą miały zastosowanie, w zasadzie bez wyjątku, do wszystkich organizacji pozarządowych działających w Polsce. Ponadto sam fakt, że działania odbywają się poza granicami Unii Europejskiej, nie zwalnia ze stosowania przepisów. Na przykład organizacja

projektu szkoleniowego na Ukrainie przez fundacje mającą siedzibę w Polsce będzie podlegała pod przepisy RODO w zakresie ochrony danych osobowych, niezależnie od konieczności spełnienia norm przewidzianych w przepisach ukraińskich.

Druga zasada dotyczy podmiotów mających siedzibę poza Unią Europejską. Formalnie pozostają one związane zakresem zobowiązania, ale w praktyce dochodzenie odpowiedzialności będzie trudne, ponieważ RODO nie zawiera norm w tym zakresie. Wskazuje się, że możliwe będzie przypisywanie odpowiedzialności pośrednikom lub podmiotom zależnym i wykorzystywanie mechanizmów współpracy między państwami (Wirska 2017, s. 73–75).

### Zgoda na przetwarzanie danych osobowych

Podstawowym założeniem przepisów dotyczących ochrony danych osobowych jest przyjęcie, że ich przetwarzanie wymaga zgody osoby, której dane dotyczą. Ma to dwojakie konsekwencje. Po pierwsze, należy przyjąć, że zgoda jest konieczna w każdej sytuacji, chyba że wyraźnie jest wskazany wyjątek – na przykład art. 9 ust. 2 RODO. Po drugie, wyjątków nie wolno interpretować rozszerzająco (Zieliński 2017, s. 241–242).

Rozporządzenie zawiera definicję legalną pojęcia zgody. W art. 4 pkt 11 RODO zapisano, że „zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, jakim osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych".

Dobrowolność zgody jest oceniana w wymiarze sytuacyjnym. Zwraca na to uwagę motyw czterdziesty trzeci RODO, w którym wskazuje się, że przy braku równowagi między osobą, której dane dotyczą, a administratorem należy szczególnie uważnie traktować kwestie dobrowolności. Na przykład dotyczy to sytuacji, w której uczestnictwo w projekcie jest warunkowe, to znaczy udział w projekcie zależy od udzielenia zgody na przetwarzanie danych dla celów marketingowych. W takim wypadku zgoda nie będzie uznawana za dobrowolną. Aby spełnić ten warunek, konieczne jest podzielenie zgody na dwie części: dotyczącą przetwarzania danych na potrzeby wykonania umowy oraz przetwarzania danych dla celów marketingowych, przy czym brak wyrażenia tej drugiej zgody nie może uniemożliwiać uczestnictwa w projekcie.

Jednoznaczność w składaniu oświadczenia woli wskazuje na utrzymanie zasady, że zgoda nie może być domniemana (por.: art. 7 pkt 5 ustawy z 1997 roku; Barta, Litwiński 2016, s. 227). Z kolei zgodnie z RODO może być ona złożona w innej formie niż pisemna, na przykład w formie dokumentowej (art. $77^3$ Kodeksu cywilnego). W jej zakres będą wchodzić zgody wyrażane mailem, wiadomościami tekstowymi czy komunikatorami, o ile można ustalić tożsamość osoby składającej oświadczenie (por. Chmieliński 2014).

W ramach wyraźnego działania potwierdzającego dopuszczalne jest wyrażenie zgody w formie ustnej. Przyjęcie takiego rozwiązania w praktyce będzie miało jednak charakter wyjątkowy. Po pierwsze, ze względu na konieczność wywiązania się z obowiązków informacyjnych. Zgodnie z art. 12 ust. 1 RODO informacje o prawach osoby mogą być udzielane ustnie, jeśli osoba, której dane dotyczą, tego zażąda,

o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Po drugie, obowiązek udowodnienia posiadania zgody na przetwarzanie danych spoczywa na administratorze (art. 7 ust. 1 RODO).

Pewne wątpliwości budzi zakwalifikowanie zgody jako oświadczenia woli. W obecnym stanie prawnym uznaje się ją za czynność zbliżoną do oświadczenia woli (Barta, Litwiński 2016, s. 228). Jednocześnie RODO nie daje żadnych wskazówek w tym zakresie (Kaczmarek-Templin 2016, s. 104–105). Ma to ogromne znaczenie praktyczne za względu na możliwość składania oświadczenia woli przez pełnomocnika czy stosowania przepisów o wadach oświadczenia woli. Wydaje się jednak, że treść normatywna RODO nie przekreśla stosowania dotychczas wypracowanej koncepcji.

Rozporządzenie RODO w art. 7 ust. 3 utrzymuje zasadę odwołania zgody w każdym momencie (por. art. 7 pkt 5 ustawy z 1997 roku). Złożenie takiego oświadczenia ma charakter *ex nunc*, to znaczy wywołuje skutki od chwili jego złożenia. Osoba wycofująca zgodę nie może więc kwestionować legalności przetwarzania danych w okresie między wyrażaniem zgody a jej wycofaniem.

Wycofania zgody nie można się zrzec. Za nieważną należy uznać również klauzulę nakładającą kary umowne za wycofanie zgody na przetwarzanie danych osobowych. Administrator nie może również utrudniać wycofywania zgody. Zgodnie z art. 7 ust. 3 RODO wycofanie zgody musi być równie łatwe jak jej wyrażenie. Nie oznacza to konieczności składania oświadczenia woli o wycofaniu w tej samej formie, co oświadczenia o zgodzie. Na przykład jeśli zgoda została złożona za pomocą formularza, to jej odwołanie może nastąpić przez kliknięcie w specjalny link. Przyjęcie zasady, że skuteczne odwołanie jest możliwe tylko w formie listu poleconego, byłoby jednak uznane za nakładające nadmierne obowiązki na osobę, której dane są przetwarzane.

Skutecznej zgody będzie mogła udzielić osoba z pełną zdolnością do czynności prawnej. W wypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku planowane polskie przepisy przewidują jednak możliwość udzielania zgody od trzynastego roku życia (por. Sibiga 2016). W wypadku osoby młodszej przetwarzanie danych osobowych ma być możliwe wyłącznie po uzyskaniu uprzedniej zgody jej przedstawiciela ustawowego albo po niezwłocznym potwierdzeniu przez przedstawiciela ustawowego zgody wyrażonej przez taką osobę (art. 3 projektu UC101).

W wymiarze zgody na przetwarzanie danych osobowych warto zwrócić uwagę na status już pozyskanych zgód. Co do zasady nie tracą one swojej ważności. To znaczy zgody pozyskane na podstawie dotychczasowych przepisów dalej obowiązują i możliwe jest przetwarzanie danych w zakresie w nich wskazanym. Nie będzie zatem konieczne uzyskiwanie nowych zgód lub weryfikowanie dawnych przy założeniu, że zostały one złożone zgodnie z przepisami obowiązującymi w chwili ich składania.

### Przetwarzanie danych sensytywnych przez organizacje pozarządowe

Wśród danych osobowych wyróżnia się szczególną kategorię danych, nazywaną w doktrynie danymi sensytywnymi lub wrażliwymi. Obejmuje ona te informacje o jednostce, które istotnie wpływają na jej autonomię informacyjną. Zgodnie

z art. 9 ust. 1 RODO do tych danych zaliczymy informacje ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne oraz dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej albo danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Zarówno w obecnie obowiązujących przepisach, jak i w RODO jest wprowadzony wyraźny zakaz przetwarzania tego typu danych. Jednocześnie w praktyce organizacji pozarządowych wielokrotnie istnieje konieczność przetwarzania takich informacji. Dotyczy to organizacji działających na rzecz określonych grup (uchodźcy czy osoby chorujące na określone schorzenia), ale także podmiotów wspierających określone sprawy. Na przykład działanie w komitecie wspierającym określonego kandydata może ujawniać poglądy polityczne jego członków. Dlatego RODO w art. 9 ust. 2 lit. d przewiduje wyjątek w tym zakresie. Przepis ten stanowi, że przetwarzanie jest dozwolone, o ile dokonuje się go „w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą".

Zakres stosowania tego przepisu jest szerszy niż definicja organizacji pozarządowych w rozumieniu art. 3 ust. 2 Ustawy o działalności pożytku publicznego i o wolontariacie. Będzie on obejmował również grupy nieformalne, a także partie polityczne. Warunkiem jest działanie w ramach wskazanych w przepisie celów. Dlatego stosować tego przepisu nie mogą komitety działające na przykład na rzecz budowy kanalizacji w gminie. Zarówno w wypadku organizacji pozarządowych, jak i w wypadku innych podmiotów nie będzie miała znaczenia kwestia prowadzenia przez nie działalności gospodarczej. Analiza językowa nakazuje przy interpretacji terminu „niezarobkowy" odwołać się do tekstu angielskiego, w którym użyto sformułowania „not-for-profit". Będzie on zatem obejmował każdy podmiot, którego głównym celem nie jest działalność gospodarcza.

Kolejnym warunkiem jest przetwarzanie danych wyłącznie z określonego kręgu osób. O ile ustalenie członków lub byłych członków w wypadku stowarzyszeń nie jest problemem, o tyle w wypadku fundacji nie ma takiej kategorii pojęciowej. Wykładnia celowościowa wskazuje, że przepis ten należy stosować do członków organów fundacji. Zarówno tych, które podlegają ujawnieniu w Krajowym Rejestrze Sądowym, jak i tych, które są powoływane na podstawie statutu na przykład rady fundacji czy rady programowej.

Kategoria osób utrzymujących stałe kontakty w związku z celami podmiotu jest dość wąska. Będzie obejmowała na przykład rodziców dziecka, które jest objęte wsparciem danej organizacji. Przesłanka stałego kontaktu wymaga zachowania określonej częstotliwości. Nie jest ona sprecyzowana i w razie sporu będzie rozstrzygana przez sąd lub organ *ad casum*. Jednocześnie, o ile taka osoba nie jest członkiem, to po ustaniu kontaktu organizacja nie może przetwarzać jej danych sensytywnych.

Należy pamiętać, że administrator musi zachować wszystkie warunki w zakresie bezpieczeństwa danych oraz nie może ich udostępniać innym podmiotom. Wyjątkiem w zakresie drugiego warunku jest zgoda osoby, której dane dotyczą.

Brak spełnienia przesłanek wskazanych powyżej nie wyklucza możliwości przetwarzania danych sensytywnych przez organizacje. W praktyce znaczenie będą miały dwa wyjątki. Pierwszym jest art. 9 ust. 1 lit. a RODO, wskazujący, że dane takie mogą być przetwarzane, jeśli osoba, której dane dotyczą, wyraziła wyraźną zgodę na ich przetwarzanie w jednym lub kilku konkretnych celach. Cele te powinny być wskazane wprost i w sposób niepozostawiający wątpliwości co do zakresu przetwarzania. Drugim wyjątkiem jest przetwarzanie danych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą (art. 9 ust. 1 lit. e). Upublicznienie jest rozumiane jako przekazanie informacji kręgowi osób, który nie jest określony. W wypadku wątpliwości należy pamiętać, że ciężar dowodu spoczywa na administratorze.

***

Reforma systemu ochrony danych osobowych opiera się przede wszystkim na zmianie filozofii ich ochrony. Obecnie obwiązujące założenia, które koncentrują się na wyznaczaniu obowiązków przez organy władzy publicznej, zastąpiła większa odpowiedzialność administratora. Ma on szersze pole do wyboru środków i celów ochrony, ale spoczywa na nim większa odpowiedzialność, wyrażająca się między innymi w wysokości planowanych kar.

W zakresie zasad przetwarzania zmiany w stosunku do istniejącego stanu prawnego objęły głównie doprecyzowanie pojęć i wyjaśnienie wątpliwości pojawiających się w praktyce. Niemniej jednak otwartą kwestią pozostaje, czy przyjąć obiektywną, czy też subiektywną koncepcję identyfikacji osoby fizycznej. Na pochwałę zasługuje doprecyzowanie zagadnienia danych sensytywnych i wprowadzenie nowych kategorii danych. Z perspektywy organizacji pozarządowych duże znaczenie będzie miał wyjątek dotyczący możliwości przetwarzania danych sensytywnych przez niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych. Wątpliwości pojawiają się co do zakresu stosowania tego wyjątku w stosunku do fundacji i grup nieformalnych, ale wydaje się, że są one również objęte jego zakresem.

Zakres terytorialny obowiązywania RODO może budzić problemy w stosowaniu przepisów w praktyce. Co do zasady należy przyjąć, że organizacja pozarządowa mająca siedzibę w Polsce będzie podlegała jego przepisom niezależnie od miejsca prowadzenia działalności.

Wprowadzone przepisy w zakresie zgody na przetwarzanie danych osobowych czynią zadość postulatom precyzyjnej regulacji w tym zakresie. Szczególnie ważne jest wskazanie konieczności świadomości w zakresie udzielenia zgody oraz możliwości łatwego jej wycofania. Uwagę zwraca obniżenie wieku, w którym można skutecznie zgodzić się na przetwarzanie danych osobowych w Internecie. Dla organizacji pracujących z młodzieżą będzie to znaczne ułatwienie, niemniej jednak rodzi się obawa nadużyć ze strony nieuczciwych podmiotów rynkowych.

Ogólnie reformę można ocenić pozytywnie. Jest to krok do dostosowania przepisów do zmieniającej się rzeczywistości społecznej. Będzie ona jednak wymagała od organizacji pozarządowych, tak jak od wszystkich innych podmiotów, podjęcia proaktywnej postawy w zakresie ochrony danych osobowych. Ze względu na ograniczone zasoby może to być problemem zwłaszcza dla mniejszych organizacji.

**Bibliografia**


Barta Paweł, Litwiński Paweł, 2016, *Ustawa o ochronie danych osobowych. Komentarz*, C.H. Beck, Warszawa.

Chmieliński Piotr, 2014, *Ustnie, pisemnie, elektronicznie. Prawo elektroniczne jako nowa gałąź prawa,* „Palestra", nr 5–6, s. 290–298.

Gajda Anastazja, 2014, *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomicznego-Społecznego »Studia i Prace«", nr 4.

Grzelak Agnieszka, 2017, *Główne cele ogólnego rozporządzenia o ochronie danych*, [w:] Maciej Kawecki, Tomasz Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, C.H. Beck, Warszawa.

Kaczmarek-Templin Berenika, 2016, *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia,* [w:] Edyta Bielak-Jomaa, Dominik Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Wolters Kluwer, Warszawa.

Kawecki Maciej, 2017, *Reforma ochrony danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych,* Wolters Kluwer, Warszawa.

Kordela Marzena, 2012, *Zasady prawa. Studium teoretycznoprawne, Wydawnictwo Naukowe Uniwersytetu Adama Mickiewicza,* Poznań.

Korga Magdalena, 2017, *Ochrona danych osobowych – od czego zacząć, jak opracować i utrzymać system oraz na czym polega ochrona danych w praktyce,* [w:] Magdalena Korga, Katarzyna Matelowska-Tatoj, Jarosław Żabówka, *Przygotowanie organizacji do stosowania RODO. Ochrona danych w procesie przejściowym i po wejściu przepisów w życie,* Presscom, Wrocław.

Litwiński Paweł, 2017, *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału sprawiedliwości z 19.10.2016 w sprawie c-582/14 Patrick Breyer*, „Europejski Przegląd Sądowy", nr 5.

Morawska Katarzyna, 2017, [w:] Maciej Kawecki, Tomasz Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia,* C.H. Beck, Warszawa.

Sibiga Grzegorz, 2016, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia,* „Monitor Prawniczy – dodatek", nr 20.

Wirska Paulina, 2017, *Rozszerzenie zakresu stosowania unijnych przepisów na administratorów danych i podmioty przetwarzające państw trzecich,* [w:] Maciej Kawecki, Tomasz Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia,* C.H. Beck, Warszawa.

Wronkowska Sławomira, Ziembiński Zygmunt, 1997, *Zarys teorii prawa,* Ars boni et aequi, Poznań.

Zieliński Maciej, 2017, *Wykładnia prawa. Zasady – reguły – wskazówki,* Wolters Kluwer, Warszawa.

Żabówka Jarosław, 2017, *Elementy systemu ochrony danych osobowych,* [w:] Magdalena Korga, Katarzyna Matelowska-Tatoj, Jarosław Żabówka, *Przygotowanie organizacji do stosowania rodo. Ochrona danych w procesie przejściowym i po wejściu przepisów w życie,* Presscom, Wrocław.

**Akty prawne i dokumenty**

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania, DzU WE L 281/31.
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, DzU UE 2016 L 119.
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 roku w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, DzU UE 2016 L 119.
Projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final 2017/0003 (COD).
Projekt ustawy o ochronie danych osobowych, nr UC101, wersja z 14 września 2017 roku.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), DzU UE 2016 L 119.
Ustawa z dnia 24 kwietnia 2003 roku o działalności pożytku publicznego i o wolontariacie, t.j.: DzU 2016, poz. 1817 ze zm.
Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, t.j.: DzU 2016, poz. 922.
Zalecenie Komisji z dnia 6 maja 2003 roku dotyczące definicji przedsiębiorstw mikro, małych i średnich, 2003/361/WE.

**Orzeczenia**

Wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-582/14 Patrick Breyer przeciwko Niemcom.
Wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-134/08 HauptzollamtBremen przeciwko J.E. Tyson Parketthandel GmbH.
Wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-101/01 BodilLindqvist przeciwko Szwecji.
Wyrok Naczelnego Sądu Administracyjnego z 19 maja 2011 roku, I OSK 1079/10.