[Artykuł recenzowany]

Jarosław Greser

Obowiązki organizacji pozarządowych jako administratorów danych osobowych w świetle RODO

20

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

SŁOWA KLUCZOWE:
ochrona danych osobowych, RODO, administrator danych osobowych

DOI
10.26368/17332265-042-2-2018-1

ABSTRAKT
W artykule skoncentrowano się na obowiązkach nałożonych na organizację pozarządową jako administratora danych osobowych w związku z wejściem w życie rozporządzenia ogólnego o ochronie danych (RODO). Punktem wyjścia jest przedstawienie nowego podejścia do ochrony danych osobowych, które jest zawarte w tym akcie prawnym, i wskazanie, że każde uprawnienie osób, których dane są przetwarzane, rodzi obowiązek po stronie administratora. W tekście omówiono instytucję analizy ryzyka przetwarzania danych jako podstawową czynność, którą administrator powinien wykonać przed podjęciem decyzji o tym, w jaki sposób i jakimi środkami będzie chronił dane. Ponadto poruszono problematykę oceny skutków planowanych operacji przetwarzania dla ochrony danych jako niezbędną do przeprowadzenia w wielu organizacjach pozarządowych, szczególnie tych, które przetwarzają dane wrażliwe. Wskazano również zakres informacji przekazywanych osobom, których dane są przetwarzane, i omówiono wybrane prawa tych osób. Zarysowano także problematykę pozostałych obowiązków administratorów, szczególnie prawa do zapomnienia i prawa do przeniesienia danych.

Przetwarzanie danych osobowych jest czynnością niezbędną do właściwego funkcjonowania organizacji pozarządowych niezależnie od ich wielkości i zakresu działania. Dlatego reforma systemu ochrony danych osobowych w Unii Europejskiej, nakładająca nowe obowiązki, wydaje się poważnym wyzwaniem dla wielu organizacji. W niniejszym artykule zostaną syntetycznie przedstawione obowiązki administratora danych, a więc podmiotu, który ponosi odpowiedzialność za wdrożenie nowych przepisów.

Nowe podejście do ochrony danych osobowych

Zmiana w systemie ochrony danych osobowych jest wynikiem przyjęcia przez Parlament Europejski i Radę Unii Europejskiej całej grupy nowych aktów prawnych, wśród których największe znaczenie ma Rozporządzenie w sprawie ochro-

ny osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO). Zmienia ono dotychczasowy paradygmat postępowania z danymi osobowymi. Dotychczas przepisy wskazywały minimalny zakres działań, jakie należało podjąć, aby zadośćuczynić wymaganiom prawnym. W Polsce przykładem takiej regulacji jest Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Jednym z głównych założeń reformy jest przyjęcie podejścia *risk based approach* (Litwiński 2017, s. 54). Zakłada ono, że wobec szybkości postępu technologicznego nie można przewidzieć, jakie środki będą adekwatne do skutecznej ochrony danych osobowych (Cwener 2017, s. 99). Obowiązek wyboru odpowiednich rozwiązań i ich skutecznego wdrożenia spoczywa na podmiocie, który bezpośrednio dysponuje danymi. RODO odchodzi więc od sztywno wyznaczonych zasad postępowania na rzecz elastycznego doboru środków ochrony. Jednocześnie zakłada ono, że w każdej sytuacji związanej z przetwarzaniem danych trzeba brać pod uwagę ryzyko, jakie takie działanie niesie dla prywatności osób, których dane są przetwarzane (Bielak-Jomaa 2017, s. 4). Takie rozwiązanie należy ocenić jako korzystne dla organizacji pozarządowych. Biorąc pod uwagę zróżnicowanie organizacji pod względem skali działania, grup odbiorców czy dostępu do zasobów, przyjęcie jednolitych kryteriów prowadziłoby do nakładania trudnych do realizacji obowiązków. Upraszczając nieco obraz, lokalne stowarzyszenie organizujące raz w roku dożynki będzie miało znacznie mniej obowiązków niż ogólnopolska fundacja wspierająca osoby z chorobami genetycznymi.

Punktem wyjścia ustalenia odpowiedzialności za wdrożenie przepisów RODO, a następnie ich realizacji, jest stwierdzenie, w jakiej sytuacji prawnej znajduje się dany podmiot. Zgodnie z przepisami są cztery możliwości: administrator, podmiot przetwarzający, współadministrator lub przedstawiciel.

Zgodnie z art. 4 pkt 7 RODO administrator to podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Definicja zawarta w tym przepisie wskazuje, że w wypadku organizacji pozarządowych administratorem najczęściej będzie osoba prawna: stowarzyszenie lub fundacja. Działający w jej imieniu organ, na przykład zarząd lub prezes, nie są administratorami, ponieważ nie działają w swoim imieniu i na swój rachunek. Obowiązków administratora nie można się zrzec ani przenieść na inny podmiot. Szczególnie nie zwalnia z nich powołanie inspektora ochrony danych, o którym mowa w art. 37 RODO. Nie można również mówić o zwolnieniu się z odpowiedzialności w wypadku zawarcia umowy ubezpieczenia od kar nakładanych przez organ nadzorczy. W takiej sytuacji możemy mówić jedynie o przejęciu

ryzyka przez podmiot trzeci – zakład ubezpieczeń – zapłacenia kary lub odszkodowań, gdyby stosowne przepisy zostały naruszone.

Obowiązki w zakresie ochrony danych osobowych spoczywają również na podmiocie przetwarzającym dane. W tym wypadku obowiązki te będą pochodną zakresu danych, które zostały przekazane do przetwarzania. Przykładem takiej sytuacji jest prowadzenie ewaluacji projektu wymagającej kontaktu z osobami w nim uczestniczącymi. Zgodnie z art. 29 RODO przetwarzanie odbywa się wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii Europejskiej lub prawo państwa członkowskiego. Dlatego najczęściej podstawą takiego przetwarzania są umowy o powierzeniu przetwarzania danych osobowych. Jest to umowa nienazwana, a więc granicą normowania stron jest zasada swobody umów. Za *essentialia negotii* należy uznać wskazanie, jakie dane są powierzone do przetwarzania i w jakim zakresie dane będą przetwarzane. Opierając się na treści tych uprawień, podmiot przetwarzający sam decyduje, jakie środki ma przedsięwziąć w celu należytego zabezpieczenia danych. Realizacja takiej umowy może być zabezpieczona karami umownymi. Odwołując się do przykładu – przy zlecaniu ewaluacji można wskazać, że wykorzystanie danych do innych celów niż ewaluacja, takich jak oferowanie własnych usług, będzie skutkowało nałożeniem kary określonej w umowie. Należy pamiętać, że podmiotami przetwarzającymi będą również osoby prowadzące własną działalność gospodarczą, z którymi współpracujemy. Na przykład fundacja zlecająca rehabilitację swoich podopiecznych fizjoterapeucie prowadzącemu działalność gospodarczą powinna zawrzeć z taką osobą umowę o powierzeniu danych osobowych.

Współadministratorami zgodnie z art. 26 RODO są podmioty, które są administratorami określonych danych i wspólnie ustalają cele i sposoby ich przetwarzania. Może się to zdarzyć na przykład przy realizacji projektu przez kilka organizacji w partnerstwie. Najczęściej takie porozumienie będzie formą umowy. W jej zakresie musi mieścić się jasny podział odpowiedzialności dotyczących wypełniania obowiązków nakładanych przepisami. Konstruując takie porozumienie, należy zwrócić szczególną uwagę na to, który ze współadministratorów będzie pełnił funkcje punktu kontaktowego dla osób, których dane są przetwarzane.

Zgodnie z art. 4 pkt 17 RODO przedstawiciel oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii Europejskiej, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia. Taka sytuacja może wystąpić na przykład przy wysyłaniu lub przyjmowaniu wolontariuszy z organizacji mającej siedzibę poza Unią Europejską. W tym wypadku przedstawicielem organizacji zagranicznej może być podmiot w Polsce. Wymaga to jednak uzgodnienia między stronami.

Z czterech sytuacji przedstawionych powyżej najczęściej będziemy mieli do czynienia z pierwszą, gdy organizacja będzie administratorem danych. Zakres obowiązków pozostałych podmiotów jest ograniczony przez odpowiednie ustalenia umowne, dlatego w dalszej części niniejszego artykułu skupię się na omawianiu pozycji administratora jako relewantnej dla pozostałych sytuacji.

Obowiązki administratora można podzielić na trzy grupy. Pierwszą jest obowiązek sporządzenia analizy ryzyka i na jej podstawie zdecydowanie o przyjęciu odpowiednich środków organizacyjnych lub technicznych mających na celu ochronę danych osobowych. Drugą są obowiązki będące korelatem praw osób, których dane są przetwarzane. Trzecią jest zaś respektowanie zasad przetwarzania danych osobowych. W dalszych rozważaniach skupię się na dwóch pierwszych grupach obowiązków, ponieważ tematyka zasad przetwarzania została przedstawiona w artykule *Zasady przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych* zamieszczonym w poprzednim numerze „Kwartalnika Trzeci Sektor" (Greser 2018).

Analiza ryzyka przetwarzania danych

Dotychczasowe regulacje prawne nakładały na wszystkich administratorów danych osobowych obowiązek przygotowania instrukcji zarządzania systemem informatycznym i opracowania polityki bezpieczeństwa. W zależności od zakresu działań administratora dokumenty mogły również obejmować ewidencję upoważnień, wnioski i decyzje w zakresie rejestracji zbiorów danych, raporty z audytów, wykaz osób którym powierzono przetwarzanie danych czy umowy o powierzeniu przetwarzania danych. Zgodnie z nowymi regulacjami co do zasady nie będzie żadnego wykazu dokumentów obligatoryjnych. RODO nie przewiduje również stosowania żadnych konkretnych rozwiązań lub procedur (Cwener 2017, s. 98; Bielak-Jomaa 2017, s. 4). Podstawą sporządzenia dokumentacji będzie analiza ryzyka. Na gruncie RODO jako analizę ryzyka należy rozumieć dokument poprzedzający wdrożenie odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 32 RODO.

Analizę taką będzie musiał przeprowadzić każdy podmiot, który przetwarza dane osobowe. Nie jest to zależne od formy prawnej, wielkości czy skali podejmowanych działań. Nie zwalania z tego obowiązku brak środków finansowych czy zasobów ludzkich (wyrok Naczelnego Sądu Administracyjnego z dnia 4 marca 2002 roku). Dlatego nawet organizacje nieosiągające żadnego przychodu powinny przeprowadzić taką analizę. Od tego obowiązku nie zwalnia również fakt działania wyłącznie na rzecz swoich członków, jak to się dzieje na przykład w stowarzyszeniach samopomocowych.

Podmiot prowadzący analizę nie jest zobowiązany do zachowania żadnej określonej formy, ze względów dowodowych warto jednak, aby taka analiza była

utrwalona przynajmniej w formie elektronicznej. Nie ma również przyjętej lub zalecanej metodologii prowadzenia takiego działania. W literaturze wskazuje się, że koncepcja ochrony danych osobowych przyjęta w RODO jest oparta na normach z rodziny ISO/IEC[1] (Byczkowski 2017, s. 19), choć nie jest to jedyna dostępna metodologia (por. *Wytyczne*... 2017, s. 27). Można również stworzyć autorską metodę oceny ryzyka (por. *Nowa filozofia*... 2017, s. 10). Administrator będzie musiał jednak wykazać, dlaczego przyjął określoną metodę i czy rzeczywiście pozwala ona na obiektywne oszacowanie ryzyka[2].

Wskazówek dotyczących tego, co należy ująć w ramach analizy, dostarcza art. 32 RODO. Pierwszą przesłanką jest stan wiedzy technicznej, przez który należy rozumieć dostępność określonych rozwiązań. W ramach tego kryterium należy również zbadać, czy dana technologia odpowiada na współczesne wyzwania (czy nie jest przestarzała). W mojej ocenie nie można wywieść obowiązku używania wyłącznie najnowszych rozwiązań, szczególnie w sytuacji, gdy ich oddziaływanie nie jest jeszcze dostateczne przebadane. Tym bardziej że właśnie używanie nowoczesnych technologii bardzo często jest wskazywane jako zagrożenie dla prywatności osób fizycznych (*Wytyczne*... 2016, s. 11; Konarski 2017, s. 13). W praktyce funkcjonowania organizacji pozarządowych często są wykorzystywane technologie oparte na arkuszach kalkulacyjnych czy współdzieleniu plików w chmurze, jak Google Docs. Należy zauważyć, że można zwiększyć bezpieczeństwo zawartych tam danych przez wykorzystanie wbudowanych w te serwisy funkcji szyfrowania plików lub podwójnej weryfikacji dostępu. Jednocześnie RODO w art. 32 wskazuje przykłady rozwiązań do rozważenia – pseudoanonimizację i szyfrowanie danych osobowych czy wprowadzenie regularnego testowania, pomiaru i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Z przesłanką stanu wiedzy technicznej łączy się przesłanka kosztu wdrażania. Należy ją odnieść do możliwości finansowych określonego podmiotu. W wypadku organizacji pozarządowych budżet często nie pozwala na wdrażanie komercyjnych rozwiązań, tym bardziej w sytuacji, gdy organizacja jest dofinansowywana wyłącznie z grantów. Należy jednak zwrócić uwagę, że producenci oprogramowania często oferują specjalne zniżki dla podmiotów non profit lub udostępniają aplikacje w ramach inicjatyw takich jak Tech Soup, ponadto funkcjonują na rynku darmowe rozwiązania, które mogą być wystarczającą alternatywą. Trzeba również pamiętać, że zgodnie z orzecznictwem Naczelnego Sądu Administracyjnego względy natury finansowej nie powinny być traktowane jako podstawa sprzecznego z prawem przetwarzania danych osobowych (wyrok Naczelnego Sądu Administracyjnego z dnia 4 marca 2002 roku).

Kolejnymi przesłankami są charakter, zakres, uwarunkowania i cele przetwarzania. W ramach tego kryterium bada się między innymi: jakie dane i w jakiej skali są przetwarzane, szczególnie czy są to dane wrażliwe, w ilu lokaliza-

cjach są przetwarzane dane osobowe, ile osób ma do nich dostęp. Przesłanka ta ma zróżnicować podmioty, które dane osobowe przetwarzają w pewnym sensie obok swojej głównej działalności, od podmiotów, dla których jest to kluczowy zasób. W tym wymiarze korzystnie sytuują się organizacje pozarządowe, które bardzo często przetwarzają dane wrażliwe lub dane o charakterze wysoce osobistym – jak stan zdrowia fizycznego i psychicznego. Na przykład organizacja działająca na rzecz osób z rzadkimi chorobami genetycznymi będzie przetwarzała znacznie więcej danych niż organizacja, której celem jest propagowanie czytelnictwa, ponieważ ta druga nie musi przetwarzać danych genetycznych lub biometrycznych, aby wykonywać swoją misję. Jednocześnie inne będą uwarunkowania przetwarzania takich danych w wypadku organizacji i firmy farmaceutycznej, która analizuje dane pod kątem sprzedaży leków. Charakter komercyjny działalności stanowi inną okoliczność niż działanie o charakterze pomocowym i to pierwsze powinno być bardziej restrykcyjnie oceniane. Wymaga to jednak każdorazowego sprawdzenia w ramach analizy ryzyka.

Ostatnią analizowaną przesłanką jest ryzyko naruszenia praw lub wolności osób fizycznych. Chodzi tutaj o prawa wynikające z Karty praw podstawowych Unii Europejskiej, w której prawo do ochrony danych jest bezpośrednio wskazane. Wynika to z motywu pierwszego RODO, stwierdzającego, że prawo do ochrony danych należy do praw podstawowych Unii Europejskiej i do praw człowieka. Wydaje się jednak, że zagadnienie to trzeba potraktować szerzej. Na gruncie polskiego prawa autonomia informacyjna jednostki jest chroniona w art. 51 ustawy zasadniczej. W literaturze podkreśla się, że norma zawarta w tym przepisie jest skierowana zarówno do organów państwa, jak i do podmiotów prywatnych (wyrok Trybunału Konstytucyjnego z dnia 19 lutego 2002 roku), i w życiu prywatnym, i w ramach stosunku pracy (Florek 2001, s. 76). Biorąc pod uwagę, że konstytucja jest stosowana bezpośrednio, można przyjąć, że przy interpretacji tej przesłanki trzeba wziąć pod uwagę również te regulacje. Ponadto prawo do prywatności jest jednym z praw chronionych przez Konwencję o ochronie praw człowieka i podstawowych wolności, na podstawie której orzeka Europejski Trybunał Praw Człowieka w Strasburgu. Jego orzecznictwo jest istotnym wskaźnikiem w zakresie granic praw człowieka. Na przykład w sprawie Bărbulescu przeciwko Rumunii dotyczy ono możliwości ingerencji pracodawcy w korespondencję prowadzoną przy użyciu komunikatorów internetowych (wyrok Europejskiego Trybunału Praw Człowieka z dnia 5 września 2017 roku).

Należy również zwrócić uwagę, że przesłanka ta nie dotyczy wyłącznie prawa do prywatności, ale wszystkich praw jednostki. Naruszanie przepisów dotyczących ochrony danych osobowych może na przykład doprowadzić do naruszenia także innych praw, takich jak wolność wypowiedzi artystycznej (Dąbrowski 2008, s. 417–423), wolność słowa, sumienia, wyznania i religii czy

swoboda przemieszczania się (Kalinowska, Litwiński 2017, s. 701). Dlatego analizę ryzyka należy przeprowadzić pod kątem możliwego naruszenia wszystkich praw, które są gwarantowane jednostce.

Ocena skutków planowanych operacji przetwarzania dla ochrony danych

Geneza procedury oceny skutków planowanych operacji przetwarzania dla ochrony danych (*data protection impact assessment*, DPIA) sięga lat dziewięćdziesiątych xx wieku (Kalinowska, Litwiński 2017, s. 695), ale swój normatywny charakter otrzymała dopiero w art. 35 RODO. Instytucja ta jest niezależna od oceny ryzyka, choć mocno z nią powiązana, między innymi przez obowiązek sporządzenia oceny skutków planowanych operacji, jeśli analiza ryzyka wykaże jego wysoki poziom, mogący zagrozić naruszeniem praw lub wolności osób fizycznych (por. *Jak stosować*... 2017, s. 33). Należy zgodzić się jednak ze stanowiskiem Grupy 29, która stwierdziła, że ocena skutków planowanych operacji przetwarzania dla ochrony danych stanowi narzędzie zarządzania ryzykiem naruszenia praw osób, których dane dotyczą, a zatem przy jej przeprowadzaniu przyjmuje się ich perspektywę, z kolei w wypadku zarządzania ryzykiem w pozostałych obszarach należy przyjąć perspektywę organizacji (*Wytyczne*... 2016, s. 21).

Nie istnieje definicja legalna DPIA, ale na podstawie analizy przepisów można wywnioskować, że jest to trzyczęściowy proces, który obejmuje: zdefiniowanie produktu lub procesu mającego wpływ na prywatność, wybór metodologii oceny tego wypływu, dobór adekwatnych środków do minimalizacji negatywnego oddziaływania.

Rozporządzenie zawiera pięć sytuacji, w których przeprowadzenie DPIA jest obowiązkowe. Pierwszą jest stwierdzenie, że dany rodzaj przetwarzania ze względu na swój charakter, zakres, uwarunkowania i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Druga sytuacja dotyczy zautomatyzowanego przetwarzania danych (bez udziału człowieka), gdy rezultatem takiego działania jest podjęcie decyzji wywołujących skutki prawne wobec osoby fizycznej lub w istotnie na nią wpływających. Przykładem może być automatyczna analiza badań pacjentów i kwalifikacja ich do leczenia lub ocena zdolności osoby szukającej pracy i przypisanie jej odpowiednich szkoleń. Trzecią sytuacją jest przetwarzanie danych pochodzących z systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie. Dotyczy to na przykład monitoringu miejskiego lub komunikacji publicznej. Będzie miała również zastosowanie wtedy, gdy monitorujemy komputery pracowników pod kątem sposobu ich używania bez informowania ich o tym. Czwartą jest przetwarzanie przez podmiot na dużą skalę danych wrażliwych, w tym danych o wyrokach skazujących. Przesłanka ta może mieć

zastosowanie w organizacjach działających na rzecz osób wykluczonych oraz podmiotach wspierających rodziny zastępcze lub osoby z określonymi schorzeniami. Piątą sytuacją jest sporządzenie przez organ nadzoru na podstawie art. 35 ust. 4 RODO wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych. Generalny Inspektor Ochrony Danych Osobowych zapowiedział wydanie takiego wykazu operacji i opublikowanie go na stronach urzędu przed 25 maja 2018 roku. W wersji zaprezentowanej do konsultacji publicznych (*Proponowany wykaz rodzajów przetwarzania*... 2018, s. 2) zwraca się uwagę, że analiza DPIA nie będzie wymagana, jeśli systemy monitoringu wizyjnego, w których obraz jest nagrywany, są wykorzystywane tylko na potrzebę analizy incydentów naruszenia prawa.

Jeśli organizacja spełnia którąś ze wskazanych wyżej przesłanek, powinna jak najszybciej przeprowadzić ocenę skutków. W literaturze postuluje się rozpoczynać ją na etapie projektowania operacji przetwarzania, nawet jeśli niektóre z tych operacji nie są jeszcze znane, i aktualizować je na bieżąco (Kalinowska, Litwiński 2017, s. 697).

Informacje przekazywane osobom, których dane są przetwarzane

Rozporządzenie znacznie rozszerza katalog praw osób, których dane są przetwarzane. Jednocześnie doprecyzowuje istniejące uprawnienia. Z perspektywy administratora każde uprawnienie ma swoje odbicie w obowiązku, który trzeba zrealizować. Przekłada się to na wiele działań, które muszą być podjęte przez organizacje na etapie pozyskiwania zgody lub na żądanie osoby, której dane dotyczą.

Uprawnienia można podzielić na dwie kategorie: informacje i prawo do żądania określonych działań. W pierwszym wypadku zakres przekazywanych informacji różni się w zależności od tego, czy administrator pozyskał dane bezpośrednio od zainteresowanej osoby (art. 13 RODO) – na przykład po wypełnieniu przez nią zgłoszenia na szkolenie, czy też dane zostały pozyskane w inny sposób – na przykład w związku z zakupem bazy potencjalnych darczyńców (art. 14 RODO). Drugą sytuację, jako względnie rzadko występującą w praktyce, pozostawię poza przedmiotem rozważań zawartych w niniejszym artykule.

Informacje, które powinny być przekazane osobie, obejmują:

- tożsamość administratora i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
- dane kontaktowe inspektora ochrony danych, jeśli został on powołany,
- cele przetwarzania danych osobowych i podstawę prawną przetwarzania,
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją,
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, jeśli taki zamiar istnieje,

– okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
– informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania, albo o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
– jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
– informacje o prawie wniesienia skargi do organu nadzorczego,
– informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym albo warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
– informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Danych się nie podaje, jeśli określona osoba już nimi dysponuje. Będzie się tak działo najczęściej w sytuacji, w której przetwarzamy dane jakiejś osoby, ale zakres danych jest rozszerzany. Na przykład jeśli mamy imię i nazwisko podopiecznego, a dodajemy do nich adres mailowy i numer telefonu.

Jeśli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podaje wskazane informacje najpóźniej podczas pozyskiwania danych osobowych. Niezależnie od formy pozyskania informacje powinny być podane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie oraz jasnym i prostym językiem. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych wypadkach – elektronicznie (art. 12 ust. 1 RODO).

Trzeba pamiętać, że obowiązek informacyjny jest niezależny od zgody na przetwarzanie danych osobowych. Jeśli organizacja przetwarza dane na podstawie innej przesłanki niż zgoda osoba, której dane są przetwarzane, osoba taka musi być poinformowana o przysługujących jej prawach. Jako przykład można wskazać sytuację, w której prowadzony jest monitoring recepcji. Obowiązek informacyjny można wówczas zrealizować przez umieszczenie przy wejściu do budynku tablicy ze wskazanymi powyżej informacjami.

Prawa osób, których dane są przetwarzane

Wśród praw przysługujących osobie, której dane są przetwarzane na potrzeby działania organizacji pozarządowych, największe znaczenie mają: prawo dostępu do danych, prawo do sprostowania, prawo do bycia zapomnianym i prawo do przenoszenia danych. Wspólnym elementem wszystkich praw jest czas ich realizacji. Zgodnie z art. 12 ust. 3 RODO powinny być one realizowane niezwłocznie,

nie dłużej jednak niż w ciągu miesiąca od otrzymania żądania. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące ze względu na skomplikowany charakter żądania lub liczbę żądań.

Prawo dostępu do danych składa się z dwóch komponentów. Pierwszym jest prawo do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe. Jeśli do przetwarzania danych dochodzi, to osoba, której dane dotyczą, ma prawo do uzyskania dostępu i informacji w zakresie określonym w art. 15 ust. 1 RODO – na przykład rodzic dziecka, które uczestniczyło w zajęciach edukacyjnych prowadzonych przez organizację, chce się dowiedzieć, czy dane te są dalej przetwarzane. Trzeba pamiętać, że zgodnie z zasadą proporcjonalności dane powinny być przechowywane najkrócej jak to możliwe. O ile więc usługa edukacyjna została wykonana, a nie ma żadnych innych podstaw przetwarzania danych (na przykład przechowywanie dokumentacji ze względu na dofinansowanie usługi z grantu), wówczas danych tych nie należy przetwarzać. Jeśli jednak dane są przetwarzane, trzeba poinformować o tym uprawnionego na jego żądanie.

Drugim komponentem jest prawo do uzyskania kopii przetwarzanych danych osobowych podlegających przetwarzaniu. Jeśli osoba, której dane dotyczą, zwraca się elektronicznie o kopię – i nie zaznaczy inaczej – informacji udziela się powszechnie stosowanym kanałem elektronicznym. W innym wypadku kopia danych powinna być przekazana w formie pisemnej. Administrator jest uprawniony do odmowy wydania kopii danych, jeżeli może to niekorzystnie wpływać na prawa i wolności innych. Możliwe jest również pobranie opłaty za przekazaną kopię, nie może ona jednak przekroczyć kosztów administracyjnych i nie dotyczy pierwszego żądania. Ma to zapobiec nadużywaniu tego prawa, które w skrajnych sytuacjach może doprowadzić do paraliżu administratora. Prawo to nabiera szczególnego znaczenia w wypadku danych o stanie zdrowia. Na przykład prowadząc turnus rehabilitacyjny, na żądanie uprawnionego organizacja będzie musiała przekazać informacje na temat zabiegów, diety czy zmian w stanie zdrowia.

Prawo do sprostowania danych umożliwia żądanie niezwłocznego sprostowania lub uzupełnienia danych osobowych, które są nieprawidłowe. W takiej sytuacji administrator ma obowiązek powiadomienia o sprostowaniu każdego odbiorcy, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Obowiązek ten aktualizuje się również wtedy, gdy osoba skorzysta z prawa do bycia zapomnianym lub ograniczenia przetwarzania.

Prawo do bycia zapomnianym, nazywane również prawem do usunięcia danych, wyewoluowało z orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-131/12), ale w RODO uzyskało ono podstawę normatywną w art. 17. Nakłada on na administratora obowiązek usunięcia, z własnej inicjatywy, danych osobowych, jeśli:

– dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
– osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie,
– osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
– dane osobowe były przetwarzane niezgodnie z prawem,
– dane osobowe muszą być usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator.

W wypadku otrzymania żądania realizacji prawa do zapomnienia należy każdorazowo sprawdzić, czy zachodzą przesłanki wskazane powyżej. W praktyce organizacji pozarządowych poważnym utrudnieniem może być sytuacja, gdy z żądaniem wystąpi osoba, która brała udział w projekcie dofinansowanym ze środków publicznych, a po jego zakończeniu żąda, aby jej dane nie były przetwarzane. Najczęściej jednak organizacja będzie potrzebowała tych danych na wypadek kontroli. W tej sytuacji możemy mówić o nadrzędnej prawnie uzasadnionej podstawie przetwarzania, o której trzeba poinformować wnoszącego żądanie.

Ponadto w wypadku upublicznienia danych osobowych, na przykład na stronie internetowej, administrator ma obowiązek zażądania od innych administratorów przetwarzających te dane usunięcia ich kopii lub replikacji oraz łączy do nich prowadzących. Wymóg ten jest ograniczony kosztami i dostępną technologią. Innymi słowy – działania te muszą być możliwe do wykonania, a ich koszt nie może być nadmierny.

Nieco inny charakter ma prawo do przenoszenia danych zawarte w art. 20 RODO. Celem jego wprowadzenia jest zwiększenie mobilności elektronicznej i panowania przez użytkowników nad swoimi danymi (Wiewiórowski 2017, s. 24). Składa się ono z trzech niezależnych uprawnień (Czerniawski 2017, s. 31):
– prawa do otrzymania danych – czyli przekazania na żądanie osoby fizycznej zestawu danych zebranych przez administratora,
– prawo do przesłania danych bez utrudnień ze strony administratora,
– prawo do przesłania danych bezpośrednio między administratorami – to znaczy na żądanie osoby, której dane dotyczą, administrator ma obowiązek przesłać dane w interoperacyjnym formacie do wskazanego innego administratora.

Należy zwrócić uwagę, że prawo to przysługuje wyłącznie wtedy, kiedy dane są przetwarzane automatycznie i osoba, której dane dotyczą, sama je dostarczyła administratorowi. W praktyce dotyczy to na przykład wpisów na forach, wypełnionych ankiet lub przesłanych zdjęć (Czerniawski 2017, s. 30). Może to również dotyczyć wypełnianych przez uczestników ankiet oceniających wiedzę, preferencji żywieniowych lub kwalifikacji do leczenia. Uprawnienia

osoby, której dane dotyczą, ograniczają się wyłącznie do danych w formie dostarczonej. Dane przetworzone, na przykład stworzony na podstawie wpisu profil konsumencki, nie będą podlegać przesłaniu (Wiewiórowski 2017, s. 29). Podobnie należy ocenić informacje typu karta postępów dziecka w ramach zajęć edukacyjnych czy informacje dotyczące postępów w rehabilitacji.

Spory problem praktyczny powstaje w sytuacji uzyskania danych od innego administratora. Na przykład organizacja otrzymuje wyniki testów psychologicznych dotyczących zdolności swojego podopiecznego. Ponieważ nie może się z nimi zapoznać bez ich przetwarzania – a od tego momentu staje się za nie odpowiedzialna na podstawie przepisów RODO – pojawia się problem w zakresie przyjęcia tych informacji. Szczególnie że przesłane dane mogą zawierać informacje, których organizacja nie chce przetwarzać ze względu na prowadzoną przez siebie politykę. W literaturze wskazuje się, że administrator nie ma obowiązku przyjęcia przesłanych danych (Czerniawski 2017, s. 33). Należy podzielić to stanowisko i z ostrożnością podchodzić do danych przesłanych przez innych administratorów.

Pozostałe obowiązki administratora danych

Do nowych obowiązków należy zaliczyć konieczność uwzględniania ochrony danych w fazie projektowania (*privacy by design*) i domyślną ochronę danych (*privacy by default*). Obowiązek ten będzie miał szczególnie znaczenie w trakcie zamawiania lub wdrażania systemów informatycznych czy aplikacji mobilnych. W takim wypadku należy zawrzeć w umowie z wykonawcą obowiązek przeprowadzenia określonych analiz w związku ze zgodnością z RODO.

Ponadto administrator będzie miał obowiązek prowadzenia rejestru czynności przetwarzania. W literaturze wskazuje się, że rozwiązanie to ma trzy cele: ustalenie zakresu danych przetwarzanych przez administratora, weryfikację realizacji obowiązków wynikających z RODO, udowodnienie zgodności ich działań z przepisami o ochronie danych osobowych (Fajgielski 2017a, s. 36).

W rejestrze tym zamieszcza się wszystkie następujące informacje[1]:

– imię i nazwisko lub nazwę oraz dane kontaktowe administratora i wszystkich współadministratorów, a także – gdy ma to zastosowanie – przedstawiciela administratora i inspektora ochrony danych,
– cele przetwarzania,
– opis kategorii osób, których dane dotyczą, i kategorii danych osobowych,
– kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
– przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
– planowane terminy usunięcia poszczególnych kategorii danych, o ile jest to możliwe,

– ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o ile jest to możliwe.

Obowiązek prowadzenia rejestru dotyczy wyłącznie podmiotów zatrudniających ponad dwieście pięćdziesiąt osób, chyba że przetwarzanie, jakiego dokonują, mogące powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje dane sensytywne. Jak się wskazuje w literaturze, spełnienie warunków, które zwalniają z prowadzenia rejestru, będzie w praktyce trudne (Fajgielski 2017a, s. 37), szczególnie w trzecim sektorze – z powodu przetwarzania danych wrażliwych przez wiele organizacji, głównie tych, które działają na rzecz osób niepełnosprawnych, integracji społecznej lub migrantów. Biorąc pod uwagę zasadę rozliczalności, należy rekomendować prowadzenie rejestru w wypadku wątpliwości co do konieczności jego prowadzenia.

Prowadzenie rejestru danych można powierzyć inspektorowi ochrony danych (*Wytyczne*... 2016, s. 19). Jednocześnie należy pamiętać, że nie ma obowiązku powoływania tego podmiotu. Jeśli jednak administrator zdecyduje się na to, powinien taki obowiązek wskazać w regulaminie pracy lub w umowie z osobą pełniącą tę funkcję (Sibiga, Syska 2017, s. 23). Ponadto będzie się to wiązało z dodatkowymi obowiązkami informacyjnymi i organizacyjnymi (por.: Chodorowski 2017; Fajgielski 2017b). Inspektorem ochrony danych może być osoba, która pełni swoją funkcję na podstawie umowy cywilnoprawnej, również w ramach prowadzonej przez siebie działalności gospodarczej[2]. Może być to także wolontariusz.

Kolejnym obowiązkiem wynikającym z RODO jest konieczność zgłaszania do organu nadzoru incydentów, które doprowadziły do naruszenia bezpieczeństwa danych osobowych. Obowiązek taki nie jest nowy, wprowadzono go już bowiem w 2013 roku, ale wyłącznie wobec operatorów telekomunikacyjnych (Soczyński 2017, s. 40). Zgodnie z RODO obowiązuje on wszystkich administratorów i powinien być wykonany, nie później jednak niż w siedemdziesiąt dwie godziny po stwierdzeniu naruszenia. Ponadto, jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Przewidziano jednak wyjątek od obowiązku zgłaszania. Zgodnie z art. 33 ust. 1 RODO ma on zastosowanie w sytuacji, gdy jest mało prawdopodobne, że naruszenie spowoduje zagrożenie dla praw i wolności osób fizycznych. Decyzja w tej sprawie należy do administratora, niemniej jednak trzeba pamiętać, że zgodnie z zasadą rozliczalności trzeba będzie udowodnić, na jakiej podstawie powziął on przekonanie, że wskazana wyżej przesłanka została spełniona.

***

Wśród obowiązków administratora na pierwszy plan wysuwa się ocena ryzyka naruszenia praw lub wolności osób fizycznych, która poprzedza wdrożenie

środków technicznych i organizacyjnych. Jest również podstawą przyjmowania dokumentów – polityki przetwarzania danych osobowych czy polityki tworzenia systemów bezpieczeństwa informacji. Z perspektywy organizacji pozarządowych, szczególnie mniejszych, można uznać to rozwiązanie za trafione. Odejście bowiem od jednakowego traktowania wszystkich podmiotów pozwala na uwzględnienie specyfiki trzeciego sektora. Jednocześnie jest to utrudnienie, ponieważ nie będzie się można powołać – jak obecnie – na akty wykonawcze do ustawy jako podstawę treści przyjmowanych dokumentów. Należy się zgodzić ze stwierdzeniem Generalnego Inspektora Ochrony Danych Osobowych, że „wprowadzone zasady mają zwiększać samodzielność, ale i odpowiedzialność administratorów danych" (Bielak-Jomaa 2017, s. 4).

Brak realizacji obowiązków może skutkować dotkliwymi sankcjami. Zgodnie z art. 83 RODO naruszanie przepisów rozporządzenia grozi karą grzywny wysokości do 20 milionów euro, a w wypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Ponadto w razie wyrządzenia szkody jest możliwe dochodzenie zadośćuczynienia w procedurze cywilnej na podstawie przepisów o ochronie dóbr osobistych (wyrok Sądu Apelacyjnego w Warszawie z dnia 16 grudnia 2016 roku). Należy jednak odnotować, że w projekcie ustawy ograniczono liczbę sankcji karnych, penalizując jako przestępstwa przetwarzanie danych wrażliwych, a jako wykroczenie – utrudnianie lub udaremnianie kontroli (Projekt ustawy... 2017).

Stan prawny na dzień 30 kwietnia 2018 roku.

PRZYPISY

1 Do wykorzystania są szczególnie normy dotyczące ochrony danych identyfikujących osobę (PII) – serii ISO/IEC 29100, normy dotyczące zarządzania bezpieczeństwem informacji – serii ISO/IEC 27000, normy dotyczące zarządzania ryzykiem – serii ISO 31000.

2 Na marginesie warto podkreślić, że oferty przedsiębiorców oferujących „wzory analiz ryzyka", które chronią przed sankcjami ze stronu organu nadzoru, są wprowadzeniem w błąd. Warto zapoznać się ze stanowiskiem giodo w tym zakresie (por. https://giodo.gov.pl/pl/1520281/10484).

3 Generalny Inspektor Ochrony Danych Osobowych opublikował przykładowy szablon rejestru czynności przetwarzania. Jest on dostępny pod adresem: https://giodo.gov.pl/pl/1520281/10449.

4 Zgodnie ze stanowiskiem Naczelnej Rady Adwokackiej i Krajowej Rady Radców Prawnych funkcje inspektora ochrony danych mogą pełnić adwokaci i radcowie prawni. Por. https://www.giodo.gov.pl/pl/1520282/10461.

BIBLIOGRAFIA

Bielak-Jomaa, Edyta. 2017. Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych?. *Monitor Prawniczy*, 20: 3–7.

Byczkowski, Maciej. 2017. Znaczenie norm ISO we wdrażaniu bezpieczeństwa technicznego i organizacyjnego wymaganego w RODO. *Monitor Prawniczy*, 20: 17–25.

Chodorowski, Michał. 2017. *Nowe prawa i obowiązki administratorów bezpieczeństwa informacji (inspektorów ochrony danych) w świetle najnowszych opinii wydanych przez Grupę Roboczą Art. 29*, [w:] Maciej Kawecki, Tomasz Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa: Wydawnictwo C.H. Beck.

Cwener, Marcin. 2017. *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych*, [w:] Maciej Kawecki, Tomasz Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnieni*a, Warszawa: Wydawnictwo C.H. Beck.

Czerniawski, Michał. 2017. Obowiązki administratora danych wynikające z prawa do przenoszenia danych. *Monitor Prawniczy*, 20: 28–34.

Greser, Jarosław. 2018. Zasady przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych. *Kwartalnik Trzeci Sektor*, 41: 18–33.

Dąbrowski, Jakub. 2008. *Wolność wypowiedzi artystycznej w orzeczeniach Trybunału Praw Człowieka w Strasburgu*, [w:] Bartosz Guzik, Natalia Buchowska, Paweł Wiliński (red.), *Prawo wobec wyzwań współczesności*, t. 5, Poznań: Uni-Druk Wydawnictwo i Drukarnia.

Fajgielski, Paweł. 2017a. Rejestry czynności przetwarzania danych osobowych. *Monitor Prawniczy*, 20: 35–39.

Fajgielski, Paweł. 2017b. Informowanie o inspektorze ochrony danych. ABI *Expert*, 3.

Florek, Ludwik. 2001. *Konstytucyjne podstawy indywidualnego prawa pracy*, [w:] Mirosław Wyrzykowski, *Konstytucyjne podstawy systemu prawa*, Warszawa: Instytut Spraw Publicznych.

Kalinowska, Natalia, Litwiński, Paweł. 2017. Ocena skutków dla ochrony danych i uprzednie konsultacje – nowe obowiązki podmiotów przetwarzających dane osobowe. *Monitor Prawniczy*, 13: 694–702.

Konarski, Xawery. 2017. Rozporządzenie o e-Prywatności jako regulacja sektorowa względem ogólnego rozporządzenia o ochronie danych osobowych (RODO). *Monitor Prawniczy*, 20: 6–13.

Nowa filozofia w ochronie danych osobowych: od oceny ryzyka do spójnej strategii w organizacji. 2017. Oprac. Katarzyna Szymielewicz, Warszawa: Fundacja Panoptykon.

Sibiga, Grzegorz, Syska, Katarzyna. 2017. Działania organizacyjne i informacyjne związane z wyznaczeniem i wykonywaniem funkcji inspektora ochrony danych. *Monitor Prawniczy*, 20: 23–28.

Soczyński, Tomasz. 2017. Zgłaszanie naruszeń ochrony danych – nowy obowiązek administratorów danych. *Monitor Prawniczy*, 20: 40–47.

Wiewiórowski, Rafał Wojciech. 2017. Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych. *Europejski Przegląd Sądowy*, 5: 23–30.

Akty prawne i dokumenty

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) (Dz.U. UE z 2016 L 119).

Wytyczne dotyczące inspektorów ochrony danych ('DPO'), WP 243 rev. 01, 2016 [uaktualnione w dokumencie z 5 kwietnia 2017 roku].

Źródła internetowe

Jak można prowadzić rejestr czynności przetwarzania danych oraz rejestr kategorii czynności?. 2017. Generalny Inspektor Ochrony Danych Osobowych – https://giodo.gov.pl/pl/1520281/10449 [dostęp: 25 kwietnia 2018 roku].

Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków – https://www.giodo.gov.pl/pl/1520281/10430 [dostęp: 25 kwietnia 2018 roku].

Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, 2017 – http://www.giodo.gov.pl/pl/1520281/10303 [dostęp: 25 kwietnia 2018 roku].

Orzecznictwo

Wyrok Naczelnego Sądu Administracyjnego z dnia 4 marca 2002 roku (II SA 3144/01).
Wyrok Sądu Apelacyjnego w Warszawie z dnia 16 grudnia 2016 roku (VI ACa 1525/15).
Wyrok Trybunału Konstytucyjnego z dnia 19 lutego 2002 roku (U 3/01).
Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 w sprawie C-131/12 Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos.
Wyrok Europejskiego Trybunału Praw Człowieka z dnia 5 września 2017 roku Bărbulescu przeciwko Rumunii (skarga nr 61496/08).