Wydawanie decyzji administracyjnych w praktyce Prezesa Urzędu Ochrony Danych Osobowych

Marcin Lewoszewski
Radca prawny
Kobylańska Lewoszewski Mednis sp.j.

Po ponad roku stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L z 2016 r. Nr 119, str. 1 ze zm.), powszechnie określanego w Polsce jako RODO, doczekaliśmy się relatywnie bogatego dorobku polskiego organu nadzorczego. W omawianym okresie Prezes Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO) wydał ponad sto decyzji administracyjnych.

Wbrew obawom administratorów, podsycanym przez komunikaty o wysokości możliwych do nałożenia administracyjnych kar finansowych, które regularnie pojawiały się w mediach przed 25 maja ubiegłego roku, czyli datą rozpoczęcia stosowania przepisów RODO, jedynie kilka, spośród wydanych decyzji, zakończyło się wymierzeniem takiej kary administratorowi. Większość decyzji wydanych przez Prezesa UODO to decyzje umarzające postępowanie lub odmawiające uwzględnienia skargi złożonej na administratora przez osobę, której dane dotyczą. W niektórych przypadkach nawet wydanie decyzji nakazującej usunięcie stwierdzonego naruszenia i przyjęcie określonych środków naprawczych nie pociągało za sobą decyzji w sprawie dodatkowego nałożenia finansowej kary administracyjnej, co potwierdza, że organ rozważa w każdej sytuacji zasadność takiej sankcji i decyzja o jej nałożeniu nie jest ścisłą regułą.

Wśród wybranych przez nas decyzji merytorycznych, rozstrzygających władczo o sytuacji administratora, znajduje się jednak kilkanaście pozycji, które stanowią cenne źródło wiedzy o podejściu organu ochrony danych do różnych aspektów przetwarzania danych i sytuacji, które mogą stanowić naruszenie przepisów RODO. Adresatami opisanych poniżej decyzji są zarówno podmioty publiczne, jak i prywatne. Co ciekawe, stanowisko Prezesa UODO zawsze wzorowane jest na rozstrzygnięciach poprzednika, czyli Generalnego Inspektora Ochrony Danych Osobowych (dalej: GIODO). Wymaga to ciągłego monitorowania decyzji organu, kolejnych stanowisk czy przewodników wydanych przez Prezesa UODO.

Wśród omawianych decyzji nie ma jeszcze żadnych, będących wynikiem zastosowania mechanizmu spójności, tj. procedury przewidzianej w przepisach art. 60 RODO. Dla transgranicznego przetwarzania danych, tj. takiego, które w związku z działalnością administratora lub pod-

miotu przetwarzającego odbywa się w więcej, niż jednym państwie UE albo takiego, które znacznie wpływa lub może znacznie wpłynąć na podmioty danych, w więcej niż jednym państwie UE, wiodący organ nadzorczy wydaje decyzje w konsultacji z organami, których sprawa dotyczy. Niewątpliwie będą to jedne z bardziej interesujących rozstrzygnięć.

Jak jednak wspomniano na wstępie, Prezes UDOO jest aktywny w kontrolowaniu administratorów i podmiotów przetwarzających w kraju. W naszej ocenie już te pierwsze, omawiane i opisywane dalej decyzje Prezesa UODO zawierają ciekawe wskazówki interpretacyjne dla administratorów. Część z nich dotyczy jeszcze nieobowiązujących już przepisów ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.; dalej: OchrDanychU97), niemniej wciąż Prezes UODO dokonuje licznych rozstrzygnięć na tej podstawie, a niektóre wnioski w takich sprawach mogą mieć pośrednio zastosowanie do przetwarzania danych na podstawie przepisów RODO.

Udostępnienie i zakres przetwarzania danych osobowych

Wiele z opisanych poniżej decyzji **(decyzje nr 1–3 i 7–10)** dotyczy legalności przetwarzania danych osobowych, wyznaczenia odpowiedniego zakresu danych przetwarzanych dla określonego celu i podstaw ich udostępnienia administratorowi. Wydaje się, że wiele skarg wpływających do Prezesa UODO związanych jest z rosnącą świadomością znaczenia danych osobowych oraz konieczności ich chronienia przez administratorów, oraz świadomością samych podmiotów danych, dotyczącą wagi ochrony informacji na własny temat.

Ważne

Warto pamiętać, że przepisy RODO nie są jedynymi, które należy zbadać przy ocenie legalności przetwarzania danych osobowych – podstawa do przetwarzania danych dla określonego celu czy podstawa ich przekazania może wynikać nie tylko z przepisów RODO, ale również z treści przepisów szczególnych. W opisywanych przez nas sprawach takimi przepisami szczególnymi były np. ustawy regulujące sektor zdrowia, egzekucyjne czy proceduralne.

Zatem wielokrotnie, pomimo wątpliwości czy sprzeciwu zgłaszanego przez podmiot danych w sprawie legalności przetwarzania, dalszego udostępnienia danych czy przetwarzania określonego zakresu danych, Prezes UODO musiał umorzyć postępowanie, gdyż właśnie przepisy szczególne wskazywały na obowiązek lub uprawnienie do przetwarzania i dalszego przekazania danych osobowych. Przepisy takie niekiedy wskazują też wprost na zakres danych, koniecznych dla wypełnienia określonego celu. W takich sytuacjach Prezes UODO nie kwestionuje ustalonego odgórnie katalogu kategorii danych, uznaje się bowiem, że ciężar zbadania zakresu pod kątem jego zgodności z zasadą minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c RODO spoczywa na prawodawcy. **Ewentualne wątpliwości w zakresie prawidłowości takiego ustalenia rozstrzygać powinny m.in. Trybunał Konstytucyjny czy Europejski Trybunał Praw Człowieka.** Nie można zatem odgórnie wykluczyć niezgodności wskazanych przez prawodawcę katalogów kategorii danych z zasadami przetwarzania danych, wyrażonymi w przepisach RODO.

Ważne

Zakres danych nie zawsze wynika z przepisów prawa, stąd należy pamiętać, że niezbędność przetwarzania określonych kategorii danych dla osiągnięcia zamierzonego celu musi wykazać sam administrator.

Należy także zauważyć, że pomimo pewnych wątpliwości doktrynalnych na temat dopuszczalności wskazania zakresu danych w aktach wykonawczych, Prezes UODO, analizując dopuszczalny zakres danych, wciąż bada nie tylko akty rangi ustawowej, lecz także akty wykonawcze, takie jak rozporządzenia wydane na podstawie ustawy. W swojej dotychczasowej praktyce Prezes UODO nie kwestionował uregulowania zakresu danych w aktach wykonawczych do ustaw i można przyjąć, że do czasu odpowiednich nowelizacji pozostają one źródłem regulacji w tym zakresie **(por. decyzja nr 6)**.

Wybór podstawy prawnej przetwarzania danych osobowych

W przepisach OchrDanychU97, jedną z wymienionych w art. 23 ust. 1 podstaw prawnych przetwarzania danych osobowych było ich przetwarzanie w przypadku niezbędności dla wypełnienia uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W art. 6 ust. 1 lit. c RODO przesłanka ta została zmodyfikowana i obecnie na jej podstawie możliwe jest jedynie przetwarzanie

danych dla wypełnienia **obowiązków wynikających z przepisów prawa** – zatem nie powinno się jej stosować w przypadku, kiedy mamy do czynienia z uprawnieniem administratora. Taka zmiana jest istotna dla wszystkich podmiotów zobowiązanych do wykonywania obowiązków wskazanych w powszechnie obowiązujących przepisach i powinna spowodować ich przeformułowanie przez usunięcie pojęcia „może" tak, aby nie było wątpliwości, że podmiot wykonujący zadania zgodnie z dyspozycją, legitymuje się właśnie przesłanką niezbędności przetwarzania dla wypełniania określonego obowiązku. Jeszcze w 2016 r. pojawiały się głosy, że w istocie intencją unijnego prawodawcy było dopuszczenie do przetwarzania danych na podstawie art. 6 ust. 1 lit. c RODO także w sytuacji, kiedy przetwarzanie danych byłoby wynikiem korzystania z uprawnienia administratora; nie każde też państwo członkowskie UE ma – analogiczne do polskich – problemy interpretacyjne ze zmianą treści tej przesłanki. Nieoficjalnie pojawiały się nawet głosy o możliwości sprostowania treści art. 6 ust. 1 lit. c RODO lub opublikowania stanowiska KE w tej sprawie. Jak jednak wiadomo, na razie takich planów nie zrealizowano i z ostrożności konieczne jest uwzględnienie literalnego brzmienia danego przepisu.

Nie dokonano także kompleksowej zmiany polskich przepisów przez usunięcie słowa „może" z szeregu aktów prawnych (ewentualnie zastąpienia go wyrazem „musi" lub „ma obowiązek"). Poza wyzwaniami logistycznymi, taka modyfikacja mogłaby powodować sprzeczność przepisów w nowym brzemieniu z zasadą wyrażoną w art. 5 ust. 1 lit. c RODO (minimalizacja danych), gdyż zamiana uprawnienia na obowiązek może jednocześnie sugerować, że administrator jest zobowiązany do przetwarzania wszystkich informacji wymienionych w tak skonstruowanym przepisie, nawet jeśli w jednostkowej sprawie nie jest to konieczne. Tego typu wątpliwości wzbudza np. nowelizacja przepisu art. 22^1 ustawy z 26.6.1974 r. – Kodeks pracy (t.j. Dz.U. z 2019 r. poz. 1040 ze zm.), w którym użyto słowa „żąda".

Z tego względu na uwagę zasługuje szereg decyzji Prezesa UODO, zgodnie z którymi w sytuacji, w której w przepisach prawa użyto sformułowania „może", sugerującego uprawnienie, zdaniem Prezesa UODO oznacza to istnienie obowiązku prawnego i przetwarzanie danych na podstawie art. 6 ust. 1 lit. c RODO **(patrz decyzja nr 14 oraz inne, np. ZSPR.440.195.2018)**. Przyjęcie takiej interpretacji należy ocenić pozytywnie, gdyż pozwala na dość zdroworozsądkowe interpretowanie przepisów RODO – takie, które uwzględnia specyfikę polskiego prawa administracyjnego i nie stawia polskich administratorów w sytuacji gorszej od ich zagranicznych odpowiedników.

Obowiązki informacyjne

Jednym z najważniejszych problemów praktycznych związanych ze stosowaniem RODO, jak się okazuje, jest obecnie wykonywanie obowiązku informacyjnego. Dla przypomnienia: zgodnie z przepisem art. 13 RODO, w przypadku zebrania danych od podmiotu danych, administrator ma obowiązek podać podstawowe informacje związane z administratorem i operacjami przetwarzania danych, jak dane kontaktowe administratora, dane kontaktowe inspektora ochrony danych, cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania, okresy retencji, informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych czy informacje o prawie wniesienia skargi do organu nadzorczego itd. Obowiązek, o którym mowa w art. 13 RODO, aktualizuje się ponadto w momencie zmiany celu.

Zgodnie natomiast z art. 14 RODO, analogiczny obowiązek należy wykonać względem podmiotów danych w przypadku pozyskiwania danych od podmiotów trzecich, w takim wypadku należy dodatkowo określić źródło i zakres danych. Należy przy tym pamiętać, że w takiej sytuacji, RODO przewiduje pewne wyjątki, wskazane w przepisie art. 14 ust. 4. Konieczność wskazania wyjątków od obowiązków informacyjnych jest oczywista – nie zawsze ujawnienie informacji na temat przetwarzania jest możliwe lub pożądane, np. w przypadku prowadzenia postępowania przygotowawczego przez Policję.

W swojej dotychczasowej praktyce **(patrz decyzja nr 6)** Prezes UODO nie nakładał kar administracyjnych za drobne uchybienia w treści klauzul informacyjnych – tj. brak wskazania wszystkich odbiorców danych czy nieprecyzyjne określenie terminów retencji, co, jak się wydaje, należy ocenić pozytywnie.

Ważne

Nakładanie sankcji nie jest jedynym możliwym działaniem władczym i w sytuacjach, w których jest to możliwe, powinno być rozważone przede wszystkim nakazanie usunięcia uchybień.

Skuteczne wypełnienie obowiązków informacyjnych spowodowało ponadto wątpliwości dotyczące sposobu informowania podmiotów danych oraz możliwości ko-

rzystania z wyłączeń, określone w art. 14 ust. 5 RODO. Pierwsza, największa jak dotąd kara, została nałożona za niespełnienie tego obowiązku **(patrz decyzja nr 13)**. Kluczowe dla omawianej decyzji są dwa zagadnienia: kiedy można stosować wyjątek, o którym mowa w art. 14 ust. 5 lit. b RODO (udzielenie informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku) oraz w jaki sposób wypełniać obowiązek informacyjny i w jaki sposób udowodnić jego wypełnienie przed Prezesem UODO.

Należy podkreślić, że organ w swojej decyzji wskazał, iż z przepisów RODO nie wynika obowiązek wysyłania informacji do podmiotów danych przesyłką poleconą (listami poleconymi), o ile administrator może stosownymi dowodami wykazać, że obowiązek informacyjny został przez niego spełniony. Takie podejście organu byłoby zgodne z dotychczasową praktyką GIODO na gruncie OchrDanychU97. Należy jednak zwrócić uwagę, że w innej sprawie **(patrz decyzja nr 14)**, Prezes UODO wskazał, że w jego ocenie wartości dowodowej nie ma np. potwierdzenie w postaci wydruku aplikacji służącej do archiwizacji i zarządzania korespondencją. W tamtym postępowaniu wykazywano spełnienie obowiązków informacyjnych przez okazanie wydruku z ekstraktu z pliku wygenerowanego z aplikacji, w której archiwizowane są pliki dotyczące zawiadomień wysyłanych listem zwykłym przez bank. W decyzji zacytowano orzeczenie Wojewódzkiego Sądu Administracyjnego w Warszawie z 15.3.2017 r. (II SA/Wa 1695/16, Legalis), zgodnie z którym samo potwierdzenie komputerowe w prawym górnym rogu pism – „PRZESYŁKA NIESTEMPLOWANA, Data nadania ……", nie stanowi potwierdzenia wysłania pism. Prezes UODO przyjmuje za WSA, że tego typu wydruki nie mają wartości dowodowej, przynajmniej w kontekście ocenianych w omawianych postępowaniach przepisów ustawy z 29.8.1997 r. – Prawo bankowe (t.j. Dz.U. z 2018 r. poz. 2187 ze zm.; dalej: PrBank).

Istotne bowiem dla przedstawionych przez Prezesa UODO argumentów jest rozróżnienie pomiędzy sytuacją, w której przepisy szczególne, jak w tej sytuacji art. 105a ust. 3 PrBank wskazują na konieczność poinformowania o zamiarze przetwarzania danych osobowych, w przeciwieństwie do art. 13 ust. 1 RODO, który wskazuje jedynie na informowanie podmiotu danych o przetwarzaniu – co mogłoby sugerować istnienie różnego reżimu dowodowego dla sytuacji, w których prawodawca używa formy dokonanej lub niedokonanej czasownika.

Pozostawia to jednak administratorów w sytuacji, w której nie mają – na podstawie przytoczonych decyzji – pewności, co do sposobu dokumentowania wypełnienia jednego z podstawowych obowiązków, wynikających z przepisów RODO. Co więcej, trudno wskazać, dlaczego w ocenie Prezesa UODO określone osoby należy tylko „informować", a inne aż „poinformować", skoro wszystkim osobom fizycznym przysługiwać powinny takie same prawa.

Umowy powierzenia

W poprzednim stanie prawnym, tj. na mocy przepisów OchrDanychU97, GIODO w swoje praktyce wymagał od umów powierzenia przetwarzania, aby ponad polecenie przetwarzania danych zawierały postanowienia o możliwości lub braku możliwości dalszego powierzenia oraz o możliwości lub braku możliwości przekazywania danych poza EOG. Wymóg taki nie wynikał bezpośrednio z przepisów OchrDanychU97, GIODO traktował jednak takie postanowienia jako potwierdzenie odpowiedniego zabezpieczenia danych w związku z powierzeniem przetwarzania.

Obecnie podejście organu do umów powierzenia przetwarzania wydaje się być podobne i jednocześnie oparte o literalną wykładnię art. 28 RODO, zmierzającą do opisania wszystkich możliwych aspektów powierzenia w umowie i traktowanie jej postanowień jako dodatkowego zabezpieczenia danych. Poza *essentialia negotii* (zakres powierzonych danych, czas trwania przetwarzania, cele powierzenia) obowiązki podmiotu przetwarzającego wynikają wprost z przepisów samego RODO; stąd pojawiała się praktyczna wątpliwość, czy należy treść tych obowiązków powtarzać w tekście umów, czy ich źródło w przepisach powszechnie obowiązującego prawa powoduje, że ich powtórzenie w umowie jest bez znaczenia dla poprawności jej zawarcia. Prezes UODO zdaje się przyjmować, że dla potwierdzenia zawarcia wiążącej i spełniającej wymogi RODO umowy, konieczne jest potwierdzenie w jej tekście wszystkich obowiązków stron wynikających z art. 28 RODO. W **decyzji nr 6** Prezes UODO zweryfikował m.in. umowę z dostawcą usług w zakresie asysty technicznej i konserwacji oprogramowania. Prezes UODO stwierdził, że umowa ta nie spełniała wymogów określonych w art. 28 ust. 3 lit. e, f, h RODO, tj. obowiązków podmiotu przetwarzającego, związanych ze wsparciem administratora w zakresie odpowiadania na żądania podmiotów danych i wywiązywania się przez administratora z obowiązków, o których mowa w art. 32–36 RODO, jak również obowiązku udostępniania administratorowi wszelkich informacji niezbędnych mu na potrzeby rozliczalności, a także umożliwiania przeprowadzania audytów i inspekcji, i przyczyniania się do nich.

Jest to istotne rozstrzygnięcie dla wszystkich administratorów, którzy umowy zawierali pobieżnie lub korzystali z innych instrumentów prawnych, o których mowa w przepisie art. 28 ust. 3 RODO, np. regulaminów korzystania z usług, które nie zawsze zawierają wszystkie elementy, o których mowa w tym przepisie.

Zabezpieczenie danych

Niektóre z decyzji nakładających pieniężną karę administracyjną dotyczą zabezpieczenia danych. Często wspólnym mianownikiem wydanych decyzji jest stwierdzenie naruszenia przepisów art. 32 i art. 5 ust. 1 lit. f RODO, tj. zasady poufności danych i obowiązku odpowiedniego zabezpieczenia danych **(patrz decyzje nr 12 i 15)**.

W obu przytoczonych decyzjach stwierdzono naruszenie obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych, po tym jak doszło do incydentu bezpieczeństwa. Jest to zdecydowanie bardziej typowa sytuacja, gdyż w przypadku, w którym już doszło do incydentu, ryzyko braku wykonania obowiązków wskazanych w art. 32 RODO wydaje się większe.

Praktyka Prezesa UODO w tego typu sytuacjach i sposób uzasadnienia decyzji nie odbiega od przykładów zagranicznych – czego ilustracją może być decyzja nr SAN-2019-005 z 28.5.2019 r., w której francuski CNIL (*Commission nationale de l'informatique et des libertés*, odpowiednik Prezesa UODO) nałożył sankcję za niezapewnienie odpowiednich zabezpieczeń danych, które doprowadziło do umożliwienia dostępu do tych danych osobom postronnym. W tym postępowaniu administrator podnosił, że dostęp ten mogła uzyskać jedynie osoba posiadająca specjalistyczną wiedzę techniczną. CNIL podkreślił jednak, że brak kontroli nad dostępem do danych jest jedną z podstawowych luk bezpieczeństwa i wydano wiele kar za tego typu naruszenia.

W przypadku praktyki Prezesa UODO, o ile w pierwszej z omawianych poniżej decyzji **(nr 12)** stwierdzone naruszenie było jawne i polegało na celowym umieszczeniu danych na stronie internetowej w sposób umożliwiający dostęp do danych nieograniczonemu gronu odbiorców, to druga decyzja **(nr 15)** dotyczy przypadku, w którym administrator podnosił w czasie postępowania, że przyjęte przez niego środki techniczne i organizacyjne były adekwatne do rozpoznanych ryzyk i dodatkowo jego działania były zgodne ze znanymi mu standardami rynkowymi.

W uzasadnieniu decyzji Prezes UODO przytoczył treść szeregu norm i standardów, których – jego zdaniem – administrator nie uwzględnił, projektując swoje zabezpieczenia.

Brak przepisów technicznych, których przestrzeganie mogłoby być obiektywnie i bezpośrednio zweryfikowane (np. przyjęcie określonej długości hasła) oraz narzucenie przez unijnego prawodawcę użycia środków zabezpieczenia danych, które w danym przypadku są odpowiednie, wpływa na pojawienie się szeregu wątpliwości interpretacyjnych, dotyczących konieczności stosowania komercyjnych norm bezpieczeństwa oraz tego, jakiego typu ryzyka administrator musi brać pod uwagę projektując swoje zabezpieczenia. Otwartym pozostaje pytanie, czy administrator, co do zasady, powinien przyjmować komercyjne standardy, typu normy ISO/IEC. Należy bowiem pamiętać, że choć administrator, w przypadku wykrycia oraz zgłoszenia naruszenia ochrony danych, może powoływać się na stosowanie określonych standardów, nie w każdej sprawie muszą one być wystarczające.

Ważne

Możliwe są sytuacje, w których pomimo przyjęcia określonych, uznanych standardów, Prezes UODO nie uzna ich stosowania za dowód na to, że ich przyjęcie stanowiło wywiązanie się z obowiązku odpowiedniego zabezpieczenia danych.