Dane osobowe w chmurze

jak bezpiecznie przechowywać wrażliwe informacje?

experto24.pl

Spis treści

Wstęp 1
Nie ma generalnego zakazu 2
Rola Komisji Europejskiej 2
Privacy Shield 3
Alternatywne rozwiązania 5
Dostawca chmury jako procesor 6
Kto poniesie odpowiedzialność za naruszenia 7
Prawa poszkodowanego 8
Odpowiedzialność może ponieść też sam dostawca 8
W jakich przypadkach odpowiedzialność będzie wyłączona 10
Odpowiedzialność solidarna 11
Procesor może odpowiadać względem administratora 12
Prezes UODO może kontrolować prawidłowość przekazywania danych 12

Wstęp

Coraz częściej przedsiębiorcy w Polsce korzystają z usługi przechowywania danych w tzw. chmurze. Wielu dostawców tego typu usług ma swoje siedziby poza państwami Unii Europejskiej. Jakie ma to znaczenie w kontekście ochrony danych osobowych? Czy wolno przekazywać dane osobowe do chmury na serwerze takiego dostawcy? Jaka odpowiedzialność z tego tytułu ciąży na administratorze? Odpowiedzi na te pytania znajdziesz w niniejszej publikacji.

Nie ma generalnego zakazu

Na wstępie należy wskazać, że RODO nie zabrania przekazywania danych osobowych do państw trzecich. Co więcej, w motywie 101 RODO wskazano, że przepływ danych osobowych do państw spoza Unii i do organizacji międzynarodowych oraz z takich państw i z takich organizacji jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej. W takiej sytuacji konieczne jest jednak przestrzeganie przepisów RODO regulujących kwestie związane z przekazywaniem danych do państw spoza Unii Europejskiej, a także – szerzej, spoza Europejskiego Obszaru Gospodarczego.

Uwaga

RODO wskazuje na kilka, niezależnych od siebie sytuacji, w których możliwe jest przekazanie danych osobowych do państwa trzeciego. Oznacza to, że wystarczy, że wystąpi jedna z takich sytuacji, a możliwe będzie przekazanie danych do dostawcy usług chmurowych spoza UE.

Rola Komisji Europejskiej

Pierwszą z możliwości, kiedy dopuszczalne jest transferowanie danych do państwa spoza Unii Europejskiej, jest sytuacja gdy Komisja Europejska wydała wobec określonego państwa decyzję uznającą to państwo za zapewniające odpowiedni stopień ochrony. Oznacza to, że dane państwo, pomimo iż nie obowiązuje w nim RODO, uchwaliło przepisy, które regulują kwestie związane z przetwarzaniem danych osobowych w tym państwie i są one na tyle skuteczne, że zapewniają poziom bezpieczeństwa danych i ochronę praw obywateli na poziomie zbliżonym do tych, które wynikają z unijnych przepisów dotyczących ochrony danych osobowych.

Przed wydaniem wskazanej decyzji Komisja zobowiązana jest do oceny, czy dane państwo spełnia odpowiednie standardy związane z ochroną praw obywateli. Pod uwagę brane jest również istnienie niezależnego organu dot. ochrony danych osobowych, który funkcjonuje w danym państwie, jak również zaciągnięcie przez to państwo międzynarodowych zobowiązań w zakresie ochrony danych osobowych.

Uwaga

Dotychczas Komisja Europejska wydała takie decyzje w odniesieniu do następujących państw i terytoriów:

- Andora,
- Argentyna,
- Kanada (w pewnym zakresie),
- Wyspy Owcze,
- Guernsey,
- Izrael,
- Wyspa Man,
- Japonia,
- Jersey,
- Nowa Zelandia,
- Szwajcaria,
- Urugwaj.

Innymi słowy, przekazywanie danych osobowych do tych państw może odbywać się bez dodatkowych warunków. Wystarczające jest spełnianie ogólnych wymogów związanych z przetwarzaniem danych, wynikających z RODO, takich jak np. posiadanie odpowiedniej podstawy prawnej do przetwarzania danych, zawieranie umów powierzenia czy też realizowanie praw osób, których dane dotyczą.

Privacy Shield

Interesująca regulacja związana z przetwarzaniem danych osobowych poza terenem UE dotyczy Stanów Zjednoczonych Ameryki. Ma to o tyle istotne znaczenie, że tak jak wskazano na wstępie, duża liczba podmiotów świadczących usługi chmurowe ma siedzibę właśnie w tym państwie. W przypadku USA Komisja Europejska wydała decyzję, która dotyczy tylko niektórych podmiotów, działających na

terenie USA. Chodzi o te przedsiębiorstwa, które dobrowolnie przystąpiły do tzw. programu Privacy Shield.

Uwaga

Privacy Shield to zawarta pomiędzy USA a Unią Europejską umowa, która umożliwia transfery danych osobowych z UE do podmiotów mających siedzibę w USA. Lista tych podmiotów prowadzona jest przez Departament Handlu USA i można się z nią zapoznać pod linkiem https://www.privacyshield.gov/list.

Należy podkreślić, że program Tarcza Prywatności ma gwarantować obywatelom, których dane są przetwarzane, możliwość złożenia skargi w przypadku ewentualnego niezgodnego z prawem przetwarzania danych. Ponadto porozumienie przewiduje możliwość skorzystania z mechanizmów polubownego rozstrzygania ewentualnych sporów. Departament Handlu USA zobowiązany jest do prowadzenia regularnych przeglądów i kontroli respektowania zasad wynikających z programu, tak aby zweryfikować, czy przedsiębiorstwa, które przystąpiły do programu, rzeczywiście ich przestrzegają. W razie negatywnej oceny działania określonego podmiotu Departament Handlu usuwa go z listy.

Uwaga

Wiele spośród podmiotów, które oferują usługi chmurowe, mających siedzibę w USA, takich jak Microsoft, Google czy Amazon, przystąpiło do wskazanego powyżej programu. Zapewnia to możliwość korzystania z ich usług w sposób zgodny z prawem.

Pomimo to program Tarcza Prywatności jest dość regularnie poddawany krytyce. Jego przeciwnicy wskazują, że nie zapewnia on realnej ochrony praw obywateli UE, w szczególności z uwagi na znaczną ingerencję w dane użytkowników usług chmurowych, prowadzoną przez amerykańskie służby wywiadowcze. Stąd też konieczne jest bieżące monitorowanie orzeczeń Trybunału Sprawiedliwości Unii Europejskiej i komunikatów Unii Europejskiej, które dotyczą programu Tarcza Prywatności.

Alternatywne rozwiązania

Opisane powyżej decyzje Komisji Europejskiej, wskazujące na istnienie adekwatnego stopnia ochrony danych w poszczególnych państwach trzecich (w tym decyzja zatwierdzająca program Tarcza Prywatności) są stosunkowo korzystnym rozwiązaniem z punktu widzenia podmiotów działających na terenie Unii Europejskiej, które chcą korzystać z usług chmurowych spoza UE. Nie wymagają bowiem podejmowania dodatkowych czynności przez usługobiorcę i oferują możliwość postępowania z danymi osobowymi w sposób zbliżony do tego, który dotyczy przetwarzania danych w ramach państw UE. Decyzje Komisji nie są jednak jedynym rozwiązaniem zapewniającym zgodne z prawem przekazywanie danych osobowych do państw poza UE. Możliwe jest bowiem również przekazywanie danych z tzw. zastrzeżeniem odpowiednich zabezpieczeń. Mogą one polegać np. na:

- zawarciu z podmiotem spoza UE odpowiedniej, dodatkowej umowy, która zawiera specjalne klauzule, przyjęte przez Komisję Europejską, mające zapewnić odpowiedni poziom zabezpieczenia danych osobowych,
- przestrzeganiu przez dany podmiot spoza UE zatwierdzonych kodeksów postępowania, dotyczących ochrony danych osobowych, zgodnych z RODO, lub posiadania odpowiedniego certyfikatu, wskazującego na przestrzeganie przepisów RODO,
- związaniu się przez podmiot spoza UE wiążącymi regułami korporacyjnymi – tzn. zasadami dotyczącymi przetwarzania danych osobowych w ramach powiązanych ze sobą grup przedsiębiorstw, z których część ma siedzibę na terenie Unii, a część poza. Reguły takie muszą być zatwierdzone przez organ nadzorczy,
- zawarciu innej, odpowiedniej umowy pomiędzy administratorem danych w UE a podmiotem z państwa trzeciego, która zostanie zatwierdzona przez organ nadzorczy.

Niektóre z tych możliwości, które zostały wskazane powyżej, łączą się z koniecznością podjęcia przez administratora dodatkowych działań, przykładowo w zakresie podpisania z podmiotem przetwarzającym, oferującym usługi chmurowe i mającym siedzibę poza terenem UE, odpowiedniej umowy, zawierającej standardowe klauzule umowne. W innym przypadku obowiązek podjęcia wielu działań, np. uzyskania potwierdzenia przetwarzania danych zgodnie z przepisami RODO na podstawie zatwierdzonego kodeksu postępowania lub w ramach procesu certyfikacji, obowiązek podjęcia dodatkowych (dobrowolnych) działań obciążał będzie danego usługodawcę. Mając to na uwadze, należy podkreślić, że oparcie się na powyższych przesłankach przekazania danych osobowych nie będzie możliwe w każdym przypadku i z reguły będzie uzależnione od woli i chęci podporządkowania się określonym regułom przez podmiot świadczący usługi chmurowe.

Uwaga

Istnieją również szczególne wyjątki związane z przekazywaniem danych osobowych do państw trzecich, umożliwiające przekazanie danych np. po uzyskaniu na to zgody osoby, której dane dotyczą, czy w sytuacji gdy jest to niezbędne do wykonania umowy pomiędzy administratorem a osobą, której dane dotyczą. Powinny one jednak mieć charakter incydentalny, z uwagi na to, iż wymagają badania, czy dane osobowe konkretnej osoby mogą zostać przekazane z uwagi np. na podstawy przetwarzania lub cele, w jakich są przetwarzane dane. W konsekwencji mogłoby to znacznie utrudnić bieżące i łatwe korzystanie z usług chmurowych przez administratora i znajdzie ograniczone zastosowanie w odniesieniu do korzystania z usług chmurowych.

Dostawca chmury jako procesor

Przede wszystkim to administrator danych ponosi odpowiedzialność za prawidłowość przetwarzania danych i nie może jej przerzucić na swojego podwykonawcę (usługodawcę) w taki sposób aby wywarło to skutek względem np. osób, których dane dotyczą albo organów nadzorczych (w Polsce: Prezesa Urzędu Ochrony Danych Osobowych).

Ważne

Nawet jeżeli usługobiorca (np. polski przedsiębiorca) korzysta z usługi chmurowej, odpowiada za prawidłowość przetwarzania danych w ramach tej chmury przed osobami, których dane dotyczą oraz przez Prezesem Urzędu Ochrony Danych Osobowych. Dotyczy to także kwestii bezpieczeństwa.

W praktyce może dojść do sytuacji, w której uwagi na korzystanie z usługi chmurowej naruszone są przepisy RODO, np. gdy dochodzi do nieuprawnionego dostępu do danych, czyli kiedy osoba trzecia, niezwiązana w żaden sposób z administratorem i nieposiadająca upoważnienia do przetwarzania danych, może np. odczytywać i kopiować dane.

Kto poniesie odpowiedzialność za naruszenia

Analizując kwestię wstępnej odpowiedzialności administratora należy wskazać, że bez znaczenia jest tutaj przyczyna dostępu do danych. Może być tak, że osoba trzeba weszła w posiadanie dostępu np. podszywając się pod uprawnioną osobę i podając jej dane dostępowe (takie jak login lub hasło) albo np. wykorzystała lukę bezpieczeństwa, co umożliwiło jej skopiowanie danych na posiadane przez siebie urządzenie bez wiedzy i zgody administratora.

Wystąpienie obu tych sytuacji może być spowodowane błędami popełnionymi zarówno po stronie administratora (usługobiorcy) jak i podmiotu przetwarzającego (usługodawcy, który świadczy usługi chmurowe). Wstępnie nie ma to jednak znaczenia dla osoby, której dane dotyczą. Dla niej istotne jest bowiem to, że doszło do wycieku jej danych, a więc, że osoba nieuprawniona uzyskała dostęp do tych informacji.

Ważne

Osoba poszkodowana ma prawo uznać, że podmiotem, który względem niej jest odpowiedzialny za ewentualny wyciek danych jest administrator danych. To bowiem właśnie on zdecydował o celach i sposobach przetwarzania danych.

Osoba poszkodowana powinna wiedzieć, jaki podmiot jest administratorem jej danych, ponieważ na administratorze ciąży obowiązek poinformowania osoby, której dane dotyczą o przetwarzaniu jej danych osobowych, stosownie do treści przepisu art. 13 lub 14 RODO. Tym samym osoba, której dane dotyczą, otrzymała od administratora informację o tym, że jej dane są przetwarzane, w jakim celu są one przetwarzane oraz opis innych kluczowych kwestii dotyczących samego przetwarzania. W treści obowiązku powinna również znaleźć się informacja o podmiotach, które przetwarzają dane jako podwykonawcy administratora (podmioty przetwarzające). Nie wpływa to jednak na kwestię odpowiedzialności administratora za same dane, z perspektywy osoby, której dane dotyczą. Administrator jest także odpowiedzialny za realizację praw osób, których dane dotyczą, stosownie do postanowień rozdziału III RODO, które mówią m.in. o prawie do dostępu do danych, możliwości żądania ich sprostowania czy też ograniczenia przetwarzania.

Ważne

W szczególnych sytuacjach to również administrator jest zobowiązany do zawiadomienia osoby, której dane dotyczą, bez zbędnej zwłoki, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych, stosownie do treści przepisu art. 34 ust. 1 RODO.

Prawa poszkodowanego

Jakie prawa przysługują osobie, która poniosła szkodę w związku z nieprawidłowym przetwarzaniem jej danych? Otóż z perspektywy osoby, której dane dotyczą to administrator danych jest podmiotem odpowiedzialnym za ewentualne naruszenia przepisów, które skutkują nieprawidłowym przetwarzaniem danych tej osoby. Przepisy RODO potwierdzają tego rodzaju rozumowanie, nie ograniczają się jednak do uznania, że tylko administrator jest odpowiedzialny za przetwarzanie danych danej osoby.

Ważne

Administrator jest odpowiedzialny również za niezgodne z przepisami RODO działania podmiotu przetwarzającego.

Odpowiedzialność może ponieść też sam dostawca

Przepis art. 82 ust. 1 RODO mówi bowiem o tym, że każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Innymi słowy, odpowiedzialność względem osoby, której dane dotyczą, nie jest ograniczona tylko do administratora. Jeżeli więc osoba, której dane dotyczą uważa, że doszło do naruszenia przepisów RODO przez podmiot, który przetwarzał dane w imieniu administratora (tzn. podmiotu, który zadecydował o celach i sposobach przetwarzania danych tej osoby) to ma prawo do:

- dochodzenia odszkodowania od administratora,

- dochodzenia odszkodowania bezpośrednio od podmiotu przetwarzającego.

Mając to na uwadze trzeba stwierdzić, że RODO dość szeroko zakreśla ramy odpowiedzialności administratora i podmiotu przetwarzającego. Celem tego rodzaju uregulowania jest zwiększenie możliwości poszukiwania ochrony swoich praw przez osobę, której dane dotyczą, w sytuacji gdy doszło do powstania po jej stronie szkody wynikającej z przetwarzania danych niezgodnie z RODO.

Przepis art. 82 ust. 2 RODO precyzuje, że każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym rozporządzenie. Z kolei podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. Tym samym przesądzono, że generalną odpowiedzialność za naruszenia przepisów RODO ponosi administrator danych. Odpowiedzialność podmiotu przetwarzającego jest natomiast ograniczona do sytuacji gdy:

- podmiot przetwarzający działał niezgodnie z tymi przepisami RODO, które nakładają obowiązki bezpośrednio na podmioty przetwarzające,
- podmiot przetwarzający działał niezgodnie z wytycznymi administratora (np. zawartymi w umowie powierzenia przetwarzania danych).

Przekładając to na realia korzystania z usług chmurowych trzeba wskazać, że osoba, której dane dotyczą, może skierować swoje roszczenia bezpośrednio do podmiotu przetwarzającego np. w sytuacji gdy usługodawca nie stosował odpowiednich zabezpieczeń danych w chmurze i z tej przyczyny dane te uległy wyciekowi. W takim przypadku podmiot przetwarzający nie spełnił bowiem wymogów nakładających na niego obowiązek wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa danych, stosownie do postanowień przepisu art. 32 ust. 1 RODO.

Podobnie, możliwość dochodzenia roszczeń bezpośrednio od podmiotu przetwarzającego zaktualizuje się gdy usługodawca, wbrew postanowieniom umowy powierzenia, która może zakazywać dalszego powierzania przetwarzania danych, skorzystał z usługi nierzetelnego podwykonawcy (który również nie wdrożył zabezpieczeń), w wyniku czego doszło do wycieku danych po stronie tego podwykonawcy. Stanowi to błąd podmiotu przetwarzającego, gdyż przetwarzał on dane niezgodnie z instrukcjami administratora.

W jakich przypadkach odpowiedzialność będzie wyłączona

Podmiot przetwarzający (dostawca usługi chmurowej) nie będzie natomiast odpowiedzialny za te kwestie, które są związane z obowiązkami nałożonymi wyłącznie na administratora. Przykładowo może być to np. niespełnienie wobec osoby obowiązku informacyjnego, czyli nie poinformowanie jej przez administratora o przetwarzaniu jej danych osobowych, stosownie do treści przepisu art. 13 lub 14 RODO. Inną tego rodzaju sytuacją będzie np. nierespektowanie praw osoby, której dane dotyczą m.in. w zakresie usunięcia jej danych na żądanie lub nieuwzględnienie sprzeciwu względem przetwarzania danych w celu marketingowym, w związku z istnieniem prawnie uzasadnionego interesu administratora. W takiej sytuacji podmiotem wyłącznie odpowiedzialnym będzie administrator danych i to do niego osoba, której dane dotyczą, powinna skierować ewentualne roszczenia. Ewentualne skierowanie roszczenia w tym zakresie wobec podmiotu przetwarzającego najprawdopodobniej skutkowałoby oddaleniem roszczenia przez sąd.

Jak wskazałem wyżej, z punktu widzenia osoby, której dane dotyczą podmiotem odpowiedzialnym za przetwarzanie jej danych osobowych jest głownie administrator, chociażby z uwagi na otrzymanie przez osobę informacji o przetwarzaniu danych wraz z nazwą i danymi kontaktowymi administratora. W związku z tym z reguły osoba, której dane dotyczą będzie kierowała swoje roszczenia przede wszystkim do administratora. Stąd też trzeba zastanowić się, czy administrator ponosi odpowiedzialność za ewentualne naruszenia przepisów RODO, które wystąpią po stronie podmiotu przetwarzającego.

Analiza przepisów RODO nie wyklucza takiej możliwości. Istnieje wprawdzie przepis art. 82 ust. 3 RODO, który stanowi, że administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności (...), jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Tym samym można uznać, że jeżeli wyciek nastąpił po stronie dostawcy usługi chmurowej, to administrator (usługobiorca) nie odpowiada za to zdarzenie. Należy jednak pamiętać, że administrator odpowiedzialny jest za wybór podmiotu przetwarzającego, stosownie do treści przepisu art. 28 ust. 1 RODO, który mówi, że administrator (...) korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą.

W konsekwencji można uznać, że administrator może być odpowiedzialny za wyciek danych, który zaistniał po stronie dostawcy usługi chmurowej (podmiotu przetwarzającego), w szczególności w sytuacji gdy nie zweryfikował stopnia bezpieczeństwa danych przechowywanych w chmurze (zarówno

przed zawarciem umowy albo ignorował tę kwestię w trakcie jej obowiązywania) albo nie zadbał o zawarcie w umowie powierzenia przetwarzania danych odpowiednich zapisów dotyczących bezpieczeństwa, nakładających obowiązki w tym zakresie na dostawcę usługi chmurowej. W skrajnych sytuacjach można też sobie wyobrazić, że administrator świadomie ignoruje kwestie związane z bezpieczeństwem danych w chmurze bo np. zależy mu na wyborze najtańszego dostawcy.

Odpowiedzialność solidarna

Powyższe wnioski potwierdza treść przepisu art. 82 ust. 4 RODO, który stanowi, że jeżeli w tym samym przetwarzaniu uczestniczy zarówno administrator jak i podmiot przetwarzający i odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

Ważne

Osoba, której dane dotyczą może dochodzić odszkodowania od któregokolwiek z tych podmiotów.

W tym miejscu warto przypomnieć, że jednym z elementów umowy powierzenia przetwarzania danych (tzn. umowy dotyczącej ochrony danych osobowych, zawartej pomiędzy dostawcą usługi chmurowej a usługobiorcą) powinno być uregulowanie dotyczące kwestii bezpieczeństwa. Przepis art. 28 ust. 3 RODO wskazuje m.in., że umowa powierzenia przetwarzania danych (...) powinna nakładać na podmiot przetwarzający obowiązek w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, przy uwzględnieniu stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania. Brak tego rodzaju uregulowań w umowie powierzenia lub brak prawidłowo zawartej umowy powierzenia w ogóle, w sytuacji gdy jest ona wymagana, z całą pewnością obciąża administratora.

Procesor może odpowiadać względem administratora

Konieczne jest jednak podkreślenie, że dostawca usługi chmurowej (podmiot przetwarzający) może ponosić odpowiedzialność nie tylko względem osoby, której dane dotyczą, ale także względem usługobiorcy, czyli administratora danych. Może się bowiem zdarzyć tak, że administrator zobowiązany jest do wypłaty odszkodowania na rzecz osoby, która poniosła szkodę w związku z nieprawidłowym (niezgodnym z RODO) przetwarzaniem jej danych osobowych, a szkoda ta wyniknęła z przetwarzania danych osobowych przez podmiot przetwarzający, np. z uwagi na niewystarczające zabezpieczenie danych w chmurze.

W takiej sytuacji administrator ma dalsze roszczenie względem podmiotu przetwarzającego, co oznacza, że może dochodzić od niego kwoty odszkodowania, którą wcześniej wypłacił pokrzywdzonej osobie. Roszczenie tego rodzaju powinno być dochodzone stosownie do postanowień umowy powierzenia przetwarzania danych. W praktyce bowiem w tego rodzaju umowach regulowane są kwestie związane z poszerzeniem lub ograniczeniem odpowiedzialności podmiotów przetwarzających, jak również zawierane są w nich ustalenia dotyczące sposobu, terminów lub warunków wypłaty równowartości kwoty takiego odszkodowania.

Niekiedy uregulowania te ograniczają odpowiedzialność podmiotu przetwarzającego do określonej kwoty. W takiej sytuacji należy pamiętać, że takie ustalenia mają skutek względem stron umowy powierzenia (administratora i podmiotu przetwarzającego) a nie względem osób, których dotyczą dane przetwarzane w ramach chmury.

Prezes UODO może kontrolować prawidłowość przekazywania danych

Należy również pamiętać o tym, ze zgodnie z RODO, podmioty uczestniczące w procesie przetwarzania danych (zarówno administrator jak i podmiot przetwarzający) odpowiadają nie tylko przed osobami, których dane dotyczą, ale również przed organem nadzorczym, którym w Polsce jest Prezes Urzędu Ochrony Danych Osobowych. Może on dokonywać kontroli prawidłowości przetwarzania danych osobowych i nakładać administracyjne kary pieniężne w sytuacji gdy uzna, że przetwarzanie danych odbywa się niezgodnie z przepisami RODO.

Tego rodzaju kary mogą być również nakładane w przypadkach opisanych powyżej. Jeżeli więc organ nadzorczy uzna, że naruszenie przepisów wystąpiło po stronie podmiotu przetwarzającego, ma prawo nałożyć karę na podmiot przetwarzający. Jeżeli organ uzna przy tym, że w związku z naruszeniem powstałym po stronie podmiotu przetwarzającego doszło także do nieprawidłowości po stronie administratora, będzie uprawniony do nałożenia kary również na administratora danych. Dotyczy to w szczególności sytuacji gdy administrator korzystałby z usług takich podmiotów przetwarzających, które nie zapewniają odpowiednich warunków bezpieczeństwa względem przetwarzanych danych. Inną sytuacją, która umożliwia nałożenie na administratora kary finansowej przez organ nadzorczy w związku z korzystaniem z usług chmurowych jest nieodpowiednie skonstruowanie umowy powierzenia przetwarzania danych z podmiotem przetwarzającym, która nie zawiera wszystkich elementów wymaganych przez przepisy RODO. W takiej sytuacji organ nadzorczy może korzystać z przewidzianych w przepisach prawa uprawnień, w tym również tych odnoszących się do karania finansowo podmiotów uczestniczących w przetwarzaniu danych.

Podstawa prawna:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1) – art. 13, art. 14, art. 28, art. 32, art. 34, art. 44–49, art. 82

Stopka redakcyjna

Redaktor:	Michał Kowalski
ISBN:	978-83-269-8594-2
E-book nr:	2HH0946
Firma:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł, Nr rejestrowy BDO: 000008579
Copyright by:	Wiedza i Praktyka sp. z o.o. Warszawa 2019