

PYTANIA DO EKSPERTA

Audyt najlepszą i najbardziej wiarygodną metodą weryfikacji

Czy stare umowy o powierzeniu przetwarzania danych (zawarte zgodnie z przepisami u.o.d.o.) mogą pozostać bez zmian po wejściu RODO, czy też wszystkie powinny być dostosowane do rozporządzenia przed 25 maja 2018 r.?

Nie ma na to pytanie jednoznacznej odpowiedzi, gdyż dotychczasowe umowy powierzenia przetwarzania danych zawarte zgodnie z wymaganiami określonymi w art. 31 ustawy o ochronie danych osobowych, oprócz elementów wprost wymienionych w tym przepisie jako niezbędne, mogły regulować również inne aspekty. Artykuł 31 u.o.d.o. obligatoryjnie wymagał jedynie, aby były zawierane na piśmie, a także aby został w nich określony zakres i cel przetwarzania danych (co wynika z ust. 2 powołanego przepisu, który stanowi, że podmiot, któremu powierzono przetwarzanie danych, może je przetwarzać wyłącznie w zakresie i celu przewidzianym w umowie). W umowach powierzenia zawieranych zgodnie z u.o.d.o. nie było natomiast potrzeby określania wymagań dotyczących sposobu zabezpieczenia danych ani innych wymagań dotyczących np. rozliczalności wykonywanych czynności, gdyż wynikały one bezpośrednio z ustawy. Artykuł 31 ust. 3 stanowił bowiem, że podmiot, któremu powierzono przetwarzanie, przed jego rozpoczęciem jest zobowiązany podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. Ustawa o ochronie danych osobowych wprost stanowi, że w przypadku powierzenia przetwarzania, odpowiedzialność za przestrzeganie wymagań w zakresie bezpieczeństwa danych i rozliczalność ponosi podmiot, któremu powierzono przetwarzanie. Nie było jednak przeszkód, aby w dotychczas zawieranych umowach powierzenia strony zobowiązały się dodatkowo do świadczenia innych usług, np. udzielania pomocy w wyjaśnieniach dotyczących stosowanych zabezpieczeń czy sposobu postępowania w przypadku zaistnienia incydentu bezpieczeństwa.

Natomiast art. 28 ust. 3 ogólnego rozporządzenia o ochronie danych (RODO) wprost wskazuje wiele innych, dodatkowych elementów, które obligatoryjnie umowa powierzenia ma zawierać. Należą do nich m.in. zobowiązania przetwarzającego do udzielania administratorowi danych pomocy (pełna lista – patrz ramka 1).

Zatem jeśli obecnie obowiązujące umowy powierzenia nie zawierają tych elemen-



DR ANDRZEJ KACZMAREK

dyrektor departamentu informatyki
w Biurze Generalnego Inspektora Ochrony
Danych Osobowych

tów, które zgodnie z RODO powinny być w nich uwzględnione, wówczas należy je odpowiednio zmodyfikować.

Jak administrator może sprawdzić, czy dany podmiot zapewnia zgodność przetwarzania z RODO?

Niewątpliwie najlepszą i najbardziej wiarygodną metodą jest przeprowadzenie audytu sprawdzającego, czy dany podmiot przestrzega zasad przetwarzania danych oraz czy zastosował procedury i środki bezpieczeństwa wymagane przepisami RODO. Weryfikacji powinny być poddane przede wszystkim metody i procedury stosowane przez podmiot przetwarzający w zakresie dotyczącym analizy ryzyka oraz oceny skutków, jakie mogą powodować zlecane przez administratora czynności przetwarzania danych w zakresie dotyczącym naruszenia prawa i wolności osób fizycznych. Potrzeba takiej weryfikacji podyktowana jest w RODO głównie tym, że jego przepisy nie określają katalogu zabezpieczeń, jakie należy zastosować w określonych przypadkach, ale ich wybór uzależniają od potrzeb wynikających z przeprowadzonych analiz oceny ryzyka oraz oceny skutków dla ochrony danych. Jak wskazują m.in. art. 24 i art. 32 RODO, administrator oraz podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób, których dane są przetwarzane. Podczas tych analiz, jak stanowi art. 32 RODO, należy uwzględnić stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania.

Inną metodą sprawdzenia jest skorzystanie z wyników weryfikacji dokonanych przez strony trzecie. Jeżeli przetwarzający posiada ważny certyfikat potwierdzający zgodność stosowanych procedur przetwarzania z RODO wydany przez akredytowany podmiot certyfikujący, należy wówczas przyjąć, że spełnia warunki.

Administrator może się posłużyć również wynikami audytów podmiotu przetwarzającego, wykonanych przez niezależne firmy audytorskie. Pomocne mogą być ponadto informacje o przystąpieniu podmiotu przetwarzającego do zatwierdzonego kodeksu postępowania, stosowaniu wiążących reguł korporacyjnych czy standardowych klauzul ochrony danych przyjętych przez Komisję Europejską.

Czy pod rządami RODO utrudnione będzie korzystanie z usług podmiotów świadczących hosting w chmurze obliczeniowej (publicznej)? Jak sprawdzić, czy taki podmiot zapewnia zgodność przetwarzania z rozporządzeniem?

RODO, podobnie jak obecnie u.o.d.o., nie wyklucza korzystania z usług chmury obliczeniowej. Należy jednak pamiętać, że wówczas mamy do czynienia z instytucją powierzenia przetwarzania danych. Inaczej mówiąc, administrator, który chce wykorzystać możliwości obliczeniowe chmury i decyduje się na przetwarzanie danych przy użyciu tego instrumentu, co do zasady powierza tym samym proces przetwarzania danych usługodawcy świadczącemu tę usługę. Choć zakres takiego powierzenia może być bardzo zróżnicowany, począwszy od wypożyczenia odpowiedniej infrastruktury informatycznej, w której odpowiednimi narzędziami i procesami przetwarzania zarządza sam administrator, a skończywszy na wypożyczeniu całej kompletnej usługi przetwarzania, w której wszystkie czynności przetwarzania wykonywane są przez dostawcę chmury obliczeniowej.

Niezależnie od tego, jaki jest zakres powierzenia, ważne jest, by podpisując umowę powierzenia w rozumieniu art. 28 RODO (czy obecnie art. 31 u.o.d.o.) nie stracić kontroli nad danymi osobowymi. A więc nie wolno dopuścić do sytuacji, w której powierzone dane byłyby wykorzystywane w innym celu niż ten określony przez administratora bądź byłyby przetwarzane w sposób inny, niż wskazał administrator. Pamiętać więc należy, aby korzystać wyłącznie z usług podmiotów przetwarzają-

cych posiadających odpowiednią wiedzę fachową, wiarygodność i zasoby.

Zawierając umowę powierzenia przetwarzania danych z dostawcą usług chmurowych zgodnie z art. 28 RODO, należy pamiętać, że niezwykle ważną zmianą w stosunku do obecnie obowiązujących warunków określonych w u.o.d.o. jest to, iż na podmiocie przetwarzającym spoczywać będą bardzo podobne obowiązki w zakresie zabezpieczenia danych, jak na administratorze.

Jakie nowe obowiązki będzie miał podmiot przetwarzający?

Przede wszystkim on również musi wdrożyć środki techniczne i organizacyjne odpowiednie do ryzyka przetwarzania – tak, by to przetwarzanie odpowiadało wymogom rozporządzenia.

Powierzenie danych powinno być, jak dotąd, regulowane umową lub innym instrumentem prawnym. Przy czym te powinny określać przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą. Powinny również uwzględniać wszystkie nowe wymagania dotyczące umów powierzenia zobowiązujące przetwarzającego m.in. do informowania o naruszeniach i udzielania wsparcia administratorowi w kwalifikacji naruszeń, jeśli takie wystąpią oraz w wykonywaniu związanych z naruszeniem ochrony obowiązków. Dotyczy to głównie opisu charakteru naruszenia, jego skutków, środków zaradczych, jakie powinny być podjęte przez administratora, podmiot przetwarzający czy też osoby, których dane zostały naruszone. W tym ostatnim przypadku dotyczy to sytuacji, gdy charakter naruszenia może powodować wysokie ryzyko narażenia praw i wolności osób fizycznych. Wówczas art. 34 RODO wymaga, aby niezależnie od zgłoszenia naruszenia do organu nadzorczego, poinformować o nim osoby, których dane zostały naruszone, i o działaniach, jakie powinny one podjąć w celu zminimalizowania potencjalnych jego skutków.

Dlatego warto, aby podmioty korzystające z rozwiązań chmurowych już teraz dokonały przeglądu zawartych umów i upewniły się, że podmiot, któremu powierzyły dane, będzie spełniał wszystkie określone w rozporządzeniu wymagania, a umowa zawiera wszelkie niezbędne elementy.

Rozmawiała Joanna Pieńczykowska