Rzeczpospolita 12-03-2013

Wiążące reguły korporacyjne umożliwiają bezpieczny transfer danych

FIRMY | Jeżeli przedsiębiorca ma decyzję, że we wszystkich miejscach na świecie przetwarza dane osobowe zgodnie z prawem Unii Europejskiej, to jest to dobry sygnał dla jego klientów.

Nie ma żadnej taryfy ulgowej, naruszenie przepisów jest naruszeniem – tłumaczy **dr Wojciech Rafał Wiewiórowski,** generalny inspektor ochrony danych osobowych

: Przedsiębiorcy mogą zatwierdzić wiążące reguły korporacyjne w zakresie przetwarzania danych osobowych. Co to takiego i jakie daje korzyści?

WOJCIECH RAFAŁ WIEWIÓROWSKI: Tak zwane wiążące reguły korporacyjne (Binding Corporate Rules; BCR) to instrument, którego zastosowanie umożliwia bezpieczny transfer danych osobowych poza Europejski Obszar Gospodarczy (EOG). Dlatego najbardziej są nim zainteresowane międzynarodowe korporacje. Jeżeli korporacja przyjmie wiążące reguły korporacyjne, które zyskają akceptację organu ochrony danych osobowych, to można powiedzieć, że staje się czymś w rodzaju wirtualnego państwa, które gwarantuje na „swoim terenie" odpowiednią – zdaniem instytucji unijnych – ochronę danych osobowych. Tyle tylko, że „teren" ten nie jest obszarem jednostki w rozumieniu prawa międzynarodowego publicznego, lecz w rozumieniu prawa handlowego. Czyli na terenie całej korporacji obowiązują pewne zasady, które zostały uznane za adekwatne do poziomu ochrony, który jest wymagany w UE.

Gdzie powinien zwrócić się przedsiębiorca, który chce uzyskać zatwierdzenie wiążących reguł korporacyjnych w zakresie ochrony danych osobowych?

Przedsiębiorca, który chce na podstawie wiążących reguł korporacyjnych wymieniać się informacjami między swoimi oddziałami znajdującymi się na całym świecie – nie tylko w krajach UE – powinien się skontaktować z rzecznikiem ochrony danych osobowych w tym kraju, w którym ma swoją główną siedzibę albo – jeśli chodzi o podmioty mające siedzibę poza Unią – swoje główne przedstawicielstwo na terytorium Unii. Czyli w przypadku polskiego przedsiębiorcy, działającego w wielu państwach świata, właściwy będzie generalny inspektor ochrony danych osobowych. W przypadku np. francuskiej firmy będzie to francuska komisja zajmująca się tymi zagadnieniami, czyli CNIL (Commission nationale de l'informatique et des libertés). Taki organ rozpocznie procedurę zatwierdzania wiążących reguł korporacyjnych, która będzie dokonywana wspólnie z innymi organami ochrony danych osobowych w UE. Tutaj zaczynają się pewne problemy, jakie w niektórych krajach – np. w Polsce – mogą pojawić się na końcu takiej procedury.

Co to za problemy?

Polska obecnie nie jest w stanie przystąpić do systemu wzajemnego uznawania wiążących reguł korporacyjnych. Zatem, jeżeli międzynarodowa korporacja takie reguły przyjmie, to jako polski organ ochrony danych osobowych muszę i tak wydać niezależnie od decyzji moich odpowiedników w innych krajach Unii odrębną decyzję w tej sprawie. Gdy rzecznicy z innych krajów Unii Europejskiej zatwierdzili już takie reguły, mam ułatwione zadanie. Jednak nie mam możliwości podjęcia takiej decyzji bez przeprowadzania zwykłego postępowania administracyjnego w tym zakresie. Taka – nie bardzo logiczna w praktyce sytuacja – wynika z tego, że sama konstrukcja wiążących reguł korporacyjnych nie jest opisana ani w prawie polskim, ani w prawie UE.

Kiedy to się zmieni?

W tej chwili prowadzimy prace w ramach jednej z części ustawy deregulacyjnej, aby jak najszybciej wprowadzić przepisy dotyczące wiążących reguł korporacyjnych do polskiej ustawy o ochronie danych osobowych. Wiemy, że w nowym rozporządzeniu unijnym, które w najbliższym latach zostanie uchwalone przez UE, rozwiązania dotyczące BCR będą się również znajdowały. Od tego momentu Polska będzie w stanie rozpoznawać automatycznie te reguły korporacyjne, które zostały zatwierdzone przez rzeczników w innych państwach UE.

Jeżeli takie reguły zostaną wprowadzone w UE, to po co zmiany w polskim prawie?

Chcemy nieco wyprzedzić zmiany przepisów unijnych, zdając sobie sprawę z tego, że dziś wymagamy pewnej procedury tylko ze względów czysto formalnych. Przykładowo firma HP przyjęła niedawno wiążące reguły korporacyjne na poziomie międzynarodowym. Musiała jednak przejść całą polską procedurę, łącznie z tłumaczeniem na język polski tych wiążących reguł korporacyjnych tylko po to, by dostać decyzję GIODO. W przypadku istnienia takich norm w polskim prawie albo w prawie UE taką decyzję otrzymałaby automatycznie. Dążąc do usuwania barier administracyjnych, chcielibyśmy, żeby rozwiązanie dotyczące BCR jak najszybciej zaczęło działać w Polsce.

Jakie warunki musi spełnić przedsiębiorca, by uzyskać zatwierdzenie wiążących reguł korporacyjnych?

Są trzy rodzaje warunków, jakie muszą być spełnione. Pierwsze mają charakter merytoryczny, tzn., że zasady przetwarzania danych przyjęte przez przedsiębiorcę muszą być zgodne z prawem UE w zakresie ochrony danych osobowych i przestrzegane we wszystkich jego oddziałach, nie tylko na terenie Unii, ale i w Kanadzie, Wietnamie czy na Seszelach. Drugi warunek – wiążące reguły korporacyjne muszą być jednakowe w całej korporacji, co oznacza, że oddział np. w Wietnamie nie może ustalić własnych i zarazem innych reguł przetwarzania danych osobowych. Trzeci warunek dotyczy tego, że przedsiębiorca musi poddać się kontroli ze strony organów ochrony danych osobowych, którą objęte jest również przetwarzanie danych osobowych poza terenem UE. Zatem organy te muszą mieć możliwość sprawdzania, czy zasady dotyczące ochrony danych osobowych są stosowane w zagranicznych oddziałach danej korporacji.

A jak wygląda takie sprawdzenie? Czy np. inspektorzy GIODO muszą udać się za granicę?

Z reguły jest to możliwe do zrobienia wirtualnie, gdyż nawet przekazanie danych osobowych do zagranicznego oddziału nie polega na przesyłaniu dokumentów z danymi np. pocztą lotniczą, ale na współdzieleniu systemów teleinformatycznych. Większość obrotu dokumentów odbywa się drogą elektroniczną. Oczywiście nie ma możliwości, by inspektorzy udali się np. do Wietnamu na inspekcję. Nie mamy prawa działania na terenie państw trzecich. Możemy natomiast dokonać sprawdzenia np. przy pomocy zewnętrznej firmy audytorskiej, która przeprowadzi audyt na podstawie prawa państwa, w którym firma bądź jej oddział się znajduje.

Ile czasu trwa ocena, czy przedsiębiorca spełnia niezbędne warunki?

Trudno podać jedną odpowiedź. Kilka lat temu, gdy rozpoczynano prace w zakresie wiążących reguł korporacyjnych, procedura ta trwała nieraz nawet dwa lata. Zainteresowany podmiot nie był do końca pewien, w jaki sposób to zrobić, a jednocześnie organy ochrony danych osobowych nie miały dużego doświadczenia w ocenie tego typu spraw. Czasem pytały o rzeczy oczywiste albo próbowały wyjaśnić pewne kwestie, które budziły wątpliwości, choć tak naprawdę wątpliwości nie powinno być. Dziś przyspieszono procedury i zatwierdzenie BCR trwa kilka miesięcy. Liczy się też to, który organ ochrony danych prowadzi sprawę – jeżeli francuski czy niemiecki, które mają bardzo dużo inspektorów, to procedura trwa krócej. Gdy mamy do czynienia z organem na Cyprze, gdzie jest sześciu pracowników, sprawa może trwać dłużej. W Polsce staramy się, by inspektorzy GIODO już dziś szkolili się w zasadach pracy z wiążącymi regułami korporacyjnymi, mimo że na razie żadna polska firma nie wystąpiła do nas o zatwierdzenie takich reguł na poziomie międzynarodowym.

A co się zmieniło w ostatnim czasie w zakresie reguł BCR?

Szokujących zmian prawnych nie ma. Prawdą jest jednak, że od około pół roku przy wydawaniu przez GIODO decyzji sam fakt istnienia wiążących reguł korporacyjnych, zatwierdzanych przez rzeczników ochrony danych osobowych innych państw traktujemy jako świadectwo tego, że firma szanuje ochronę danych osobowych. Powoduje to, że w czasie postępowań dotyczących przekazywania danych do państw trzecich już sam fakt istnienia w danej firmie dokumentów typu BCR ułatwia nam wydawanie decyzji. Podstawy prawnej wciąż jednak nie ma. Jest dopiero przygotowywana.

A czy w Polsce ktoś już wystąpił o zatwierdzenie wiążących reguł korporacyjnych?

Jeżeli chodzi o polskie firmy, to tego typu zgłoszenia nie było. Ale uczestniczyliśmy w przygotowywaniu i zatwierdzaniu BCR-ów, które zostały zgłoszone w innych krajach UE oraz rozpoznawaliśmy te reguły, które w innych krajach zostały przyjęte.

A ile polskich firm może być zainteresowanych zatwierdzeniem wewnętrznych reguł korporacyjnych?

Trudno powiedzieć. Przyznam, że gdy w maju 2011 roku organizowaliśmy konferencję dotyczącą wiążących reguł korporacyjnych, to spodziewaliśmy się, że zainteresuje ona około 20 prawników i traktowaliśmy ją jako małe warsztaty. Dużym zaskoczeniem dla nas był fakt, że do udziału w niej zgłosiło się około 140 różnego rodzaju podmiotów. Te małe warsztaty rozrosły się zatem w dużą konferencję. Zainteresowania tematem nie przekładałbym jednak na fakt, że wszystkie te firmy chcą przygotować wiążące reguły korporacyjne. Na pewno rozpoznają one rynek i badają, na ile takie rozwiązanie może być dla nich korzystne. W Polsce działają bardzo różne firmy – od polskich o charakterze międzynarodowym, które mają oddziały w wielu państwach świata – do przedsiębiorstw, które działają na terenie Polski, ale świadczą usługi outsourcingowe dla podmiotów z zewnątrz. Dlatego i one są zainteresowane kwestią BCR-ów. Mają swoich przedstawicieli za granicą, którzy uczestniczą w przetwarzaniu danych. Tymczasem Polska od kilku lat jest takim centrum outsourcingowym dla firm zajmujących się rachunkowością czy podmiotów przetwarzających dane finansowe. Bardzo często są to dane osobowe, nierzadko zawierające sensytywne informacje dotyczące osób. Stąd nie do końca mamy w Polsce rozpoznany rynek i nie wiemy, jak wiele firm może być zainteresowanych BCR.

Jeżeli jakiś polski przedsiębiorca wystąpi o zatwierdzenie jego reguł korporacyjnych, to czy przekazanie danych osobowych do jego oddziału w państwie trzecim nie będzie już wymagało angażowania GIODO?

Taki jest model docelowy. W momencie wprowadzania odpowiednich przepisów do prawa polskiego bądź europejskiego ten przedsiębiorca stanie się czymś w rodzaju wirtualnego państwa. Dla GIODO przestanie mieć znaczenie fakt, że jego oddział jest w Peru czy na Ukrainie.

A jaką korzyść mogą mieć klienci firmy, która uzyska zatwierdzenie wewnętrznych reguł korporacyjnych w zakresie przetwarzania danych osobowych?

Dla nich oznacza to tyle, że jest system kontroli nad tym, w jaki sposób ich dane osobowe są przetwarzane przez tę firmę. Można więc przyjąć założenie, że taki podmiot, który uzyskał decyzję dotyczącą wiążących reguł korporacyjnych, jest tym, który z założenia przetwarza dane bezpieczniej niż inni. To można wykorzystać w walce konkurencyjnej między przedsiębiorstwami. Jeżeli ktoś ma decyzję, że we wszystkich miejscach na świecie przetwarza dane osobowe zgodnie z prawem Unii Europejskiej, to jest to dobry sygnał dla klientów. Zakres wymagań, jakie trzeba spełnić, aby wiążące reguły korporacyjne zostały przyjęte, wskazuje też na to, że takie firmy wiedzą, w jaki sposób sobie radzić z danymi osobowymi.

Jak będą wyglądały kontrole przedsiębiorcy spełniania warunków w zakresie wiążących reguł korporacyjnych?

Bardzo różnie. Z zasady prowadzimy trzy rodzaje kontroli. Po pierwsze, kontrole sektorowe, do których wybieramy podobne firmy i sprawdzamy, jak są w nich przetwarzane dane osobowe. Drugi rodzaj kontroli wiąże się z otrzymaniem skargi dotyczącej działania danego przedsiębiorcy. Wówczas dokonujemy kontroli częściowej, obejmującej to zagadnienie, które kwestionuje skarżący. Trzeci rodzaj kontroli to kontrole z urzędu, które wszczynamy celem sprawdzenia, co wydarzyło się w konkretnej sprawie, o której informację pozyskaliśmy z różnych źródeł, w tym z prasy, radia czy telewizji.

Czy taki przedsiębiorca z zatwierdzonymi regułami BCR będzie inaczej traktowany, gdy naruszy zasady przetwarzania danych osobowych?

Nie ma tu żadnej taryfy ulgowej. Naruszenie przepisów jest naruszeniem.

—rozmawiał: Łukasz Kuligowski