Rzeczpospolita 14-06-2011

Wywiad

# Bezpieczne obszary przetwarzania danych osobowych

**KORPORACJE |** Nasze dane, które dotyczą operacji bankowych, finansowych, ubezpieczeniowych, oraz te, które mają charakter marketingowy, są przekazywane przez firmy do ich oddziałów znajdujących się w krajach trzecich

**: Coraz częściej mówi się o konieczności zastąpienia części dzisiejszych regulacji prawnych w zakresie ochrony danych osobowych przez soft law, czyli wiążące reguły korporacyjne. Do czego one są potrzebne, co mają załatwić?**

WOJCIECH WIEWIÓRKOWSKI: Obowiązujące w Polsce przepisy dotyczące ochrony danych osobowych zostały przygotowane w połowie lat 90. Z tego samego okresu pochodzi większość europejskich norm prawnych. Wszystkie te akty prawne regulują ochronę danych osobowych, wiążąc ich przetwarzanie z terytorium, na którym to się odbywa.

**Co to oznacza?**

Przede wszystkim posługują się one pojęciem państwa, w którym dane są przetwarzane, oraz państwa, do którego są przekazywane.

Dzielą te państwa na takie, które zapewniają odpowiednią ochronę danych osobowych, i inne kraje. Do pierwszej grupy należą państwa członkowskie Unii Europejskiej i kraje, które chronią dane osobowe na takim samym poziomie jak UE. Drugą grupę stanowią tzw. państwa trzecie, do których dane osobowe mogą być przekazywane jedynie za zgodą rzecznika ochrony danych osobowych.

Takie rozwiązanie sprawdzało się, być może, 20 lat temu. Obecnie mamy do czynienia m.in. z automatycznym przekazywaniem danych osobowych pomiędzy instytucjami wchodzącymi w skład różnego rodzaju korporacji międzynarodowych.

Dzisiaj jesteśmy świadomi tego, że nasze dane, które dotyczą operacji bankowych, finansowych, ubezpieczeniowych, oraz te, które mają charakter marketingowy, są przekazywane przez firmy do ich oddziałów znajdujących się w krajach trzecich.

**Ale za zgodą ich klienta, który przekazał firmie dane?**

Zgoda klienta to za mało. Nawet za jego zgodą korporacje nie mogą przekazywać danych do krajów trzecich, jeśli nie uzyskają akceptacji rzecznika ochrony danych osobowych. Sądzę, że to trochę anachroniczne rozwiązanie. Sposobem wyjścia z tego impasu, jakim jest traktowanie każdego kraju jako oddzielnego terytorium, jest idea stworzenia tzw. wiążących reguł korporacyjnych (Binding Corporate Rules; BCR).

**Co to takiego jest?**

To przeniesienie do wewnętrznych standardów danej korporacji rozwiązań zgodnych z wymaganiami prawa europejskiego, czyli krótko mówiąc przeniesienie na poziom międzynarodowej organizacji tego, co w Europie uznawane jest za adekwatny poziom ochrony danych osobowych. Tak więc jeśli korporacja międzynarodowa stworzy takie wiążące reguły korporacyjne, które zostaną uznane przez rzeczników ochrony danych osobowych za adekwatne, to można byłoby uznać taką korporację za bezpieczny obszar przetwarzania danych osobowych. Stanowiłoby to odejście od pojęcia „terytorium" i uznanie, że korporacja jako całość jest obszarem, na którym dane osobowe są chronione w poprawny sposób.

Niezależnie od tego oddziały korporacji muszą mieć podstawę prawną uprawniającą je do przetwarzania danych osobowych, chociażby naszą zgodę.

Polska jest już włączona w procedurę tworzenia wiążących reguł korporacyjnych – mówi **Wojciech Rafał Wiewiórowski**, generalny inspektor ochrony danych osobowych

Jeśliby korporacja stosowała się do BCR, nie musiałaby każdorazowo uzyskiwać zgody rzeczników ochrony danych osobowych.

**Jak kształtuje się sama procedura tworzenia wiążących reguł korporacyjnych?**

Są one tworzone w samych korporacjach, a następnie podlegają ocenie rzeczników ochrony danych osobowych. Już w tej chwili przyjmowane są takie wiążące reguły korporacyjne. One w pewnym stopniu ułatwiają rzecznikom ochrony danych osobowych wydawanie takich decyzji w sprawie transferu danych do państwa trzeciego.

Jednak żeby w Polsce można było wydać decyzję na podstawie wiążących reguł korporacyjnych, to polski generalny inspektor ochrony danych osobowych musi uczestniczyć przynajmniej w procedurze ich uznawania, a czasami nawet w ich tworzeniu.

Polska jest już włączona w procedurę tworzenia wiążących reguł korporacyjnych. Następnym krokiem, do którego dąży Europa, będzie stworzenie zasady wzajemnego uznawania BCR.

**Jak to ma wyglądać?**

Jeżeli na przykład, kierując się ustalonymi europejskimi zasadami, irlandzki rzecznik ochrony danych osobowych przy pomocy szwedzkiego i maltańskiego rzecznika oceni, że wszystkie oddziały korporacji X, przetwarzając dane osobowe, stosują adekwatną ich ochronę, to na tej podstawie firma ta będzie mogła przekazywać dane z terytorium Polski do swoich oddziałów na całym świecie. Będzie to możliwe, gdyż polski GIODO będzie z zasady uznawał wiążące reguły korporacyjne, które pozytywnie zostały ocenione przez innych rzeczników.

Wydaje się, że to jest rozwiązanie bardzo probiznesowe. Narzuca też korporacjom stosowanie europejskich zasad ochrony danych osobowych w ich oddziałach poza terytorium naszego kontynentu.

Z jednej strony jest to ułatwienie dla biznesu, z drugiej upowszechnianie tych zasad, które uznajemy w Europie za poprawne dla przetwarzania danych, np. na Seszelach, Wyspie Guam czy w Wietnamie.

**Ile już korporacji w Europie przyjęło BCR?**

Obecnie w Europie jest 51 korporacji, które albo przyjęły wiążące reguły korporacyjne, albo właśnie oczekują na formalną akceptację. Część tych firm ma oddziały na terenie Polski. Jednak to, że stosują wiążące reguły korporacyjne, nie zwalnia ich od uzyskiwania pozwolenia na przekazanie danych do kraju trzeciego. GIODO traktuje istnienie BCR jako pewnego rodzaju ułatwienie przy dokonywaniu ustawowej oceny wniosku o przekazanie danych osobowych. Myślę jednak, że rozsądniejszym rozwiązaniem jest stopniowe odchodzenie od udzielania każdorazowej zgody na przekazanie danych.

**O przekazanie jakich danych osobowych najczęściej ubiegają się korporacje?**

Najczęściej chodzi o dane dotyczące operacji finansowych, których dokonują klienci korporacji. Firmy występują też o możliwość przekazania danych używanych w procedurach marketingowych. Zwykle są to firmy z tego samego sektora.

Przekazanie danych pomiędzy instytucją finansową a ubezpieczeniową nie jest już takie proste, ponieważ przy takiej czynności zmienia się zasadniczo cel przetwarzania danych. Jeśli tym celem jest obsługa operacji finansowych prowadzonych przez banki, która w każdym kraju wygląda podobnie, to sprawa jest stosunkowo prosta. Natomiast wykorzystanie danych pozyskanych w związku z wykonywaniem operacji finansowych do zawierania umów ubezpieczeń majątkowych czy życiowych to już zupełna zmiana celu ich przetwarzania.

Przypomnę, że w prawie europejskim istotny jest cel przetwarzania danych i to, by był on realizowany przy użyciu adekwatnych danych.

*—rozmawiał Jerzy Kowalski*