Dane cenniejsze niż złoto

Przekraczają granice szybciej niż ludzie. A zawierają istotne informacje. Na ich administratorze ciąży odpowiedzialność prawna związana z szeroko rozumianym przetwarzaniem danych. Za co konkretnie on odpowiada?

KATARZYNA ZAJĄCZKOWSKA - WEREMCZUK

Dane osobowe krążą pomiędzy bankami krajowymi a instytucjami kredytowymi, także prowadzącymi działalność w Polsce poprzez oddział, jak i transgranicznie. Zatem wszystko, co wiąże się z odpowiedzialnością prawną dotyczącą przekazywania danych osobowych należy rozpatrywać wielopłaszczyznowo. Przede wszystkim na gruncie „Prawa bankowego" i przepisów o ochronie danych osobowych. Nie sposób pominąć też przepisów Kodeksu cywilnego, w zakresie dotyczącym odpowiedzialności za szkodę.

KONWENCJA I DYREKTYWA NA STRAŻY

W standardach Rady Europy fundamentalną rolę w dziedzinie ochrony danych osobowych odgrywa Konwencja 108 RE z 1981 r., dotycząca ochrony osób w związku z automatycznym przetwarzaniem ich danych. Jest to *de facto* najstarsze narzędzie międzynarodowej ochrony danych osobowych. Zasadniczym celem Konwencji było jej ujednolicenie w krajach europejskich i zharmonizowanie z zasadą swobodnego przepływu danych między państwami członkowskimi. Zasada ta, uznana za regułę, mówi, że krajom członkowskim nie wolno zakazywać lub uzależniać od szczególnego zezwolenia, przekazywania danych osobowych na teren innego państwa – członka Wspólnoty. Ograniczenie takie może – według tego dokumentu – zostać wprowadzone w celu ochrony sfery osobistej. Wypracowany przez kraje członkowskie protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, dotyczący organów nadzoru i transgranicznych przepływów danych, zmierzał do zmniejszenia różnic między rozwiązaniami zawartymi w Konwencji 108 i Dyrektywie 95/46/EC.

Dyrektywa 95/46/EC Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych) zapewnić miała:

- jednolity minimalny poziom ochrony prywatności osób fizycznych w związku z przetwarzaniem danych osobowych zgromadzonych w zbiorach danych,
- możliwość swobodnego przepływu danych osobowych między państwami członkowskimi.

Dyrektywa jako zasadę traktuje swobodny przepływ danych między państwami członkowskimi: Art. 1 ust. 2. mówi o tym, że nie będą one ograniczać ani zakazywać swobodnego przepływu danych osobowych pomiędzy sobą ze względów związanych z ochroną przewidzianą w ust. 1.

Nieco inaczej przedstawia się kwestia dopuszczalności przekazywania danych osobowych do krajów trzecich, czyli innych niż państwa członkowskie (przy czym Dyrektywa nie definiuje, jakie to są kraje). Szczegółowe rozwiązania w tej mierze zostały przewidziane w Rozdziale IV Dyrektywy. Zgodnie z Art. 25 ust. 1, przekazywanie do kraju trzeciego danych osobowych jest możliwe tylko wtedy, gdy zapewnia on odpowiedni stopień ich ochrony.

Postanowienia Dyrektywy 95/46/EC Parlamentu Europejskiego i Rady konkretyzuje ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych. Nie precyzuje ona jednak zasad dopuszczalności przekazywania danych do państw członkowskich. Uznaje za pewne, iż jest to możliwe i wynika z Dyrektywy, zaś zasada swobodnego przepływu danych w ramach Unii Europejskiej obowiązuje wszystkich jej członków bez wyjątku.

JAKIE UPRAWNIENIA?

Osobie (a więc także klientowi banku), której dane dotyczą, przysługują uprawnienia przewidziane w Dyrektywie (Art. 11) i ustawie o ochronie danych osobowych (art. 25), zwłaszcza zaś prawo do informacji, które jest podstawowym prawem tego, kogo dane dotyczą. W jego zakres wchodzi prawo do uzyskania wiedzy o tym, kto jest administratorem danych, informacje o celu ich przetwarzania, o odbiorcach lub kategoriach odbiorców, wskazanie, czy zostały one podane dobrowolnie, czy też na podstawie obowiązku, o źródłach, z którego pochodzą oraz o prawie dostępu do treści swoich danych i ich poprawianiu.

Dopuszczalność przekazywania danych osobowych do państwa trzeciego wymaga spełnienia wymogów ustawy o ochronie danych osobowych, w szczególności przepisów Rozdziału 7. Składa się on tylko z dwóch artykułów, jednak o znacznej doniosłości dla omawianego tematu.

Przepis art. 47 ust. 1 ustawy o ochronie danych osobowych (Art. 25 ust. 1 Dyrektywy) wprowadza zasadę, że przekazywanie danych osobowych do państwa trzeciego może nastąpić, jeżeli kraj docelowy daje przynajmniej takie gwarancje ochrony danych osobowych na swoim terytorium, jakie obowiązują na terytorium Rzeczypospolitej Polskiej. Sama ustawa o ochronie danych osobowych nie przesądza, jakie przesłanki decydują o ocenie, czy dane państwo trzecie daje takie gwarancje. Co najważniejsze, oceny takiej dokonać musi administrator danych, który zamierza transferować dane osobowe. Metodologii tej oceny szukać należy w art. 25 ust. 2 Dyrektywy.

ZA GRANICĄ JAK W POLSCE

Przepływ danych osobowych w obrębie Europejskiego Obszaru Gospodarczego jest traktowany tak samo, jak transfer danych na terytorium Polski. Dotyczy to wszystkich członków Unii Europejskiej oraz tych państw Europejskiego Obszaru Gospodarczego, które nie są członkami Wspólnoty (Norwegia, Islandia, Lichtenstein). Wobec tego przekazywanie danych osobowych do państw należących do Europejskiego Obszaru Gospodarczego podlega reżimowi ustawy o ochronie danych osobowych, z wyjątkiem przepisów Rozdziału 7. Zatem zarówno administrator danych (a takim jest także bank), który zamierza przekazywać dane osobowe, jak i administrator, który będzie ich odbiorcą i będzie je transferował, muszą spełnić jedną z przesłanek legalizujących ich przetwarzanie oraz zadbać o ich celowość i jakość. Obaj też zobowiązani są do ich zabezpieczenia.

Zgodnie z powołanym przepisem, oceny czy państwo trzecie daje wystarczające gwarancje ochrony danych osobowych należy dokonywać w świetle wszystkich okoliczności dotyczących operacji przekazywania danych lub zestawu takich operacji. Podkreślmy, że prace nad badaniem stopnia tej ochrony pojęła Grupa Robocza ds. ochrony danych osobowych powołana na mocy art. 29 Dyrektywy 95/46/WE.

ADMINISTRATOR NIEMAL JAK SAPER

Administrator, dokonując analizy, czy państwo trzecie gwarantuje wystarczającą ochronę danych osobowych, powinien uwzględnić przede wszystkim treść zasad dotyczących ich przetwarzania (celowość, jakość i adekwatność danych, zapewnienie spełnienia obowiązku informacyjnego, ich zabezpieczenie oraz realizacja prawa dostępu do nich osób, których dane dotyczą) oraz środki zapewniające skuteczne zastosowanie tych zasad. Przyjmuje się, że kraje, które ratyfikowały Konwencję 108 Rady Europy, spełniają wymóg gwarancji ochrony danych osobowych, o ile posiadają niezależny organ nadzorczy i są miejscem docelowym przekazania danych osobowych.
Dokonując tej oceny, administrator danych osobowych (a takim jest także bank) powinien działać wnikliwie, aby nie narazić się na zarzut nielegalnego ich przekazywania. Kontrola, czy transfer został dokonany do państwa trzeciego zapewniającego gwarancje ochrony, może zostać wykonana *ex post*, w ramach inspekcji wykonywanej przez Generalnego Inspektora Ochrony Danych Osobowych, na podstawie przepisu art. 12 ustawy o ochronie danych osobowych.
Według przepisu art. 12 pkt 1 ustawy o ochronie danych osobowych, do zadań Generalnego Inspektora w szczególności należy kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych. W razie ich naruszenia, Generalny Inspektor, na podstawie przepisu art. 18 ustawy o ochronie danych osobowych, może w drodze decyzji administracyjnej, nakazać przywrócenie stanu zgodnego z prawem, zwłaszcza:

- usunąć uchybienie,
- uzupełnić, uaktualnić, sprostować, udostępnić lub nieudostępniać danych osobowych,
- zastosować dodatkowe środki zabezpieczające zgromadzone dane osobowe,
- wstrzymać przekazywanie danych osobowych do państwa trzeciego,
- zabezpieczyć dane lub przekazać je innym podmiotom,
- usunąć dane osobowe.

Przekazanie danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora, pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.
Przekazywanie danych do takiego państwa trzeciego jest możliwe dopiero po wydaniu pozytywnej decyzji Generalnego Inspektora Ochrony Danych Osobowych. Decyzja nie wywołuje skutku *ex tunc* i nie legalizuje uprzedniego transferu danych osobowych.
Nieuzyskanie decyzji Generalnego Inspektora, zezwalającej na przekazanie danych osobowych, powoduje, że działalność administratora danych może zostać uznana za nielegalną i sprzeczną z prawem.

PRAWO DO ODSZKODOWANIA

Art. 23 Dyrektywy 95/46/EC przewiduje, że państwa członkowskie zapewnią, że każdej osobie, która poniosła szkodę wskutek niezgodnej z prawem operacji przetwarzania danych lub innej czynności niezgodnej z przepisami krajowymi przyjętymi na podstawie niniejszej dyrektywy, przysługuje od administratora danych odszkodowanie za poniesioną szkodę. Może być z tego zwolniony, w całości lub w części, jeżeli udowodni, że nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę. Rozwiązań szczegółowych szukać należy w krajowym porządku prawnym, przede wszystkim w przepisach kodeksu cywilnego.

Osoba, której dane zostałyby przekazane na terytorium RP i która poniosłaby szkodę w związku z ich przetwarzaniem przez polskiego administratora, będzie mogła skutecznie dochodzić od niego odszkodowania.
Dyrektywa nie precyzuje zasady odpowiedzialności administratora danych. Warto zatem rozważyć, co przewiduje prawo polskie (chodzi o przypadek, gdyby z roszczeniem o odszkodowanie wystąpiła osoba, której dane osobowe zostały przekazane do Polski przez zagranicznego administratora danych, a szkodę wyrządziłby polski administrator danych i od niego domagano by się zadośćuczynienia).
Polskie prawo cywilne w zakresie zasad odpowiedzialności wyróżnia: zasadę winy, zasadę ryzyka oraz zasadę słuszności.

• Zasada winy – to naczelna zasada w dziedzinie odpowiedzialności z tytułu czynów niedozwolonych; pojęcie winy nie zostało zdefiniowane w Kodeksie cywilnym. W sensie obiektywnym, wina oznacza bezprawność postępowania. W sensie subiektywnym, można wyróżnić stopnie winy: *dolus* – umyślność (zamierzone podjęcie działania sprzecznego z regułą lub regułami postępowania bądź powstrzymywanie się od działania, mimo istnienia obowiązku czynnego zachowania się) i *culpa* – niedbalstwo (sprawca wyobraża sobie skutek bezprawny, lecz bezpodstawnie przypuszcza, że go uniknie /to lekkomyślność/ oraz gdy sprawca w ogóle nie wyobraża sobie skutku bezprawności, choć może i powinien go sobie wyobrazić).
• Zasada ryzyka – ma charakter uzupełniający w odniesieniu do zasady winy. Wiąże się z odpowiedzialnością za sam skutek. Trudno tę zasadę wykluczyć w odniesieniu do odpowiedzialności administratora za szkody wyrządzone przez pracowników lub osoby, którymi się posłużył (ryzyko zwierzchnika, ryzyko przedsiębiorcy).
• Zasada słuszności – uzasadnia odpowiedzialność w przypadkach wyjątkowych, gdy ani na zasadzie winy, ani na zasadzie ryzyka odpowiedzialności przypisać nie można, jednak obciążenie kogoś odpowiedzialnością odszkodowawczą na rzecz poszkodowanego będzie usprawiedliwione ze względu na zasady współżycia społecznego.
W rozpatrywanym aspekcie najczęściej stosowana będzie zasada winy.

NAPRAWIENIE SZKODY

Do zaistnienia odpowiedzialności administratora danych musi powstać szkoda. Według przepisu art. 361 Kodeksu cywilnego, zobowiązany do odszkodowania ponosi odpowiedzialność tylko za normalne następstwa działania lub zaniechania, z którego szkoda wynikła. Tylko w tych granicach, w braku odmiennego przepisu ustawy lub postanowienia umowy, naprawienie szkody obejmuje straty (*damnum emergens*), które poszkodowany poniósł, oraz korzyści (*lucrum cessans*), które mógłby osiągnąć, gdyby szkody mu nie wyrządzono. Naprawienie szkody w ujęciu ww. przepisu ma zapewnić całkowitą kompensatę doznanego uszczerbku, nie dopuszczając do nieuzasadnionego wzbogacenia poszkodowanego. Odszkodowanie należy się, w ujęciu kodeksowym, tylko w granicach normalnego związku przyczynowego.
Zgodnie z ogólnymi regułami Kodeksu cywilnego (art. 6), szkodę i jej wysokość powinien wykazać poszkodowany. Niekiedy jednak wykazanie tego, zwłaszcza rozmiarów szkody, jest niemożliwe lub nader utrudnione. W takim przypadku, zgodnie z art. 322 Kodeksu postępowania cywilnego, sąd może w wyroku zasądzić odpowiednią sumę według swej oceny, opartej na rozważeniu wszystkich okoliczności sprawy.
Powołany powyżej przepis art. 23 Dyrektywy przesądza o sposobie naprawienia szkody w drodze odszkodowania.
Inaczej wynika z reguły przepisu art. 363 § 1 Kodeksu cywilnego, który stanowi, że naprawienie szkody powinno nastąpić według wyboru poszkodowanego, bądź przez przywrócenie stanu poprzedniego, bądź przez zapłatę odpowiedniej sumy pieniężnej.
Administrator danych będzie mógł się uwolnić od odpowiedzialności (eskulpować, egzonerować), jeżeli udowodni, że nie jest odpowiedzialny za zdarzenie, z którego wynikła szkoda. W tym zakresie *onus probandi* ciąży na administratorze danych, który nie będzie obciążony odpowiedzialnością, jeśli wykaże odpowiednimi dowodami, że szkoda została wywołana przez zdarzenie, które nie było ani jego działaniem, ani zaniechaniem i że nie pozostaje ono w jakimkolwiek związku przyczynowym z jego postępowaniem.

Dla ustalenia wysokości odszkodowania istotne znaczenie ma przepis art. 363 § 2 Kodeksu cywilnego. Zgodnie z nim, jeżeli naprawienie szkody ma nastąpić w pieniądzu, wysokość odszkodowania powinna być wymierzona według cen z daty ustalenia odszkodowania, chyba że szczególne okoliczności wymagają przyjęcia za podstawę cen istniejących w innej chwili.
Przyjmuje się, że wysokość odszkodowania pieniężnego zależna jest m.in. od miernika, jaki przyjmuje się dla określenia tej wysokości oraz od chwili, jaką uwzględnia się do przeprowadzenia wyliczenia. Ma to być chwila ustalenia odszkodowania, co oznacza datę orzekania przez sąd. Podkreślenia wymaga, że sąd tylko wyjątkowo może przyjąć za podstawę odszkodowania ceny istniejące w innej chwili – wtedy gdy przemawiają za tym szczególne okoliczności. W doktrynie i orzecznictwie przyjmuje się, że takie szczególne okoliczności zachodzą, jeśli przyjęcie cen z daty ustalenia odszkodowania powodowałoby pokrzywdzenie albo bezpodstawne wzbogacenie poszkodowanego oraz gdy poszkodowany samodzielnie usunął uszczerbek, dokonał naprawy.

WYPEŁNIANIE OBOWIĄZKU

Administrator danych osobowych (raz jeszcze przypomnijmy, że jest nim także bank), który otrzyma je w wyniku transferu, musi spełnić obowiązek informacyjny wynikający z przepisu art. 25 ustawy o ochronie danych osobowych. Otrzyma bowiem nowe informacje, a takie działanie z łatwością zakwalifikować można jako zbieranie danych osobowych nie od osoby, której one dotyczą.

> Jeżeli naprawienie szkody ma nastąpić w pieniądzu, wysokość odszkodowania powinna być wymierzona według cen z daty ustalenia odszkodowania.

Niedopełnienie obowiązku informacyjnego zagrożone jest sankcją karną, przewidzianą w przepisie art. 54 ustawy o ochronie danych osobowych karą grzywny, karą ograniczenia wolności albo pobawienia wolności do roku.
Na podstawie przepisu art. 32 ustawy o ochronie danych osobowych, każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych. Zauważyć należy, że zgodnie z art. 12 pkt 2 tejże ustawy, do zadań Generalnego Inspektora Danych Osobowych należy wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie tychże danych. Skutki wydania decyzji administracyjnej, w przypadku naruszenia przepisów o ochronie danych osobowych, precyzuje przepis art. 18. Mianowicie, w razie naruszenia przepisów o ochronie danych osobowych Generalny Inspektor może w drodze decyzji administracyjnej nakazać przywrócenie stanu zgodnego z prawem, a w szczególności:
• usunąć uchybienie,
• uzupełnić, uaktualnić, sprostować, udostępnić lub nieudostępniać danych osobowych,
• zastosować dodatkowe środki zabezpieczające zgromadzone dane osobowe,
• wstrzymać przekazywanie danych osobowych do państwa trzeciego,
• zabezpieczyć dane lub przekazać je innym podmiotom,
• usunąć dane osobowe.
Na zasadzie przepisu art. 105 ust. 5 Prawa bankowego bank (administrator danych) ponosi odpowiedzialność za szkody wynikające z ujawnienia tajemnicy bankowej i wykorzystania jej niezgodnie z przeznaczeniem.

Autorka jest radcą prawnym w Centrum Prawa Bankowego i Informacji Sp. z o.o. i w jednym z banków komercyjnych, doktorantką Instytutu Nauk Prawnych PAN