



**BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH
Departament Orzecznictwa, Legislacji i Skarg**

DOLiS-035-136/16

Warszawa, dnia 22 lutego 2016r.

**Pan
L. L.**

W odpowiedzi na Pana pismo z dnia [...] stycznia 2016 r., które zostało przesłane do Biura Generalnego Inspektora Ochrony Danych Osobowych pocztą elektroniczną uprzejmie informuję, iż Generalny Inspektor Ochrony Danych Osobowych może się wypowiedzieć wiążąco w konkretnej sprawie, dotyczącej przetwarzania danych osobowych wyłącznie w decyzji administracyjnej, wydanej po przeprowadzeniu postępowania w sprawie, na podstawie poczynionych w jego toku ustaleń, z uwzględnieniem obowiązujących w dacie wydania decyzji, przepisów prawa. Generalny Inspektor nie jest natomiast w stanie wiążąco opiniować jakichkolwiek rozwiązań odnoszących się do przetwarzania danych osobowych wyłącznie na podstawie przesłanej korespondencji.

Odnosząc się do Pana zapytania, organ do spraw ochrony danych osobowych wskazuje, iż zgodnie z art. 27 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*Dz. U. z 2015 r. poz. 2135, z późn. zm.*) zwanej dalej ustawą, za tzw. dane wrażliwe uważa się dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Jest to katalog zamknięty rodzaju informacji, jakie mogą być uznane za dane szczególnie chronione. W związku z powyższym wskazane przez Pana pytanie dotyczące danych nie odnosi się do danych szczególnie chronionych na gruncie przepisów ustawy.

Ustawa o ochronie danych osobowych odsyła do przepisów szczególnych, regulujących działalność określonych podmiotów i instytucji, wskazujących w jakich przypadkach i w jakim zakresie mogą one przetwarzać dane osobowe, aby obowiązki

i uprawnienia nałożone na nie mocą tych przepisów mogły być realizowane. Zgodnie z powyższym banki, jako podmioty zobligowane do stosowania środków bezpieczeństwa finansowego działają na podstawie własnych przepisów m.in. ustawy z dnia 29 sierpnia 1997 roku – Prawo Bankowe (*Dz. U. z 2015 r. poz. 128, z późn. zm*), zwanej dalej ustawą Prawo bankowe i ustawy z dnia 16 listopada 2000 roku o przeciwdziałaniu praniu pieniędzy oraz o finansowaniu terroryzmu (*Dz. U. z 2014 r. poz. 455, z późn. zm*), zwanej dalej ustawą o przeciwdziałaniu praniu pieniędzy. Praktyka taka odbywa się na podstawie jednej z przesłanek legalizujących przetwarzanie danych osobowych (art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych – czyli na podstawie szczególnych przepisów prawa).

Nie wskazał Pan, w jakim celu bank zadaje Panu pytania weryfikacyjne (np. w celu przedstawienia spersonalizowanych ofert marketingowych, czy może w celu przeprowadzenia transakcji). Gdy mowa o przeprowadzeniu transakcji, to zgodnie z art. 8 ustawy o przeciwdziałaniu praniu pieniędzy - instytucja obowiązana (m.in. bank) - przeprowadzająca transakcję, której równowartość przekracza 15 000 euro ma obowiązek zarejestrować taką transakcję. Bank musi również zarejestrować taką transakcję, której okoliczności wskazują, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu bez względu na jej wartość i charakter. W takim przypadku weryfikacja danych polega na sprawdzeniu i potwierdzeniu danych, i następuje przed zawarciem umowy z klientem lub przed przeprowadzeniem transakcji. W przypadku osób fizycznych i ich przedstawicieli – identyfikacja następuje poprzez ustalenie i zapisanie cech dokumentu stwierdzającego na podstawie odrębnych przepisów tożsamość osoby, a także imienia, nazwiska, obywatelstwa oraz adresu osoby dokonującej transakcji, a ponadto numeru PESEL lub daty urodzenia w przypadku osoby nieposiadającej numeru PESEL, lub numeru dokumentu stwierdzającego tożsamość cudzoziemca, lub kod w kraju w przypadku przedstawienia paszportu.

Pojęcie danych osobowych klienta mieści się w pojęciu informacji i tajemnicy bankowej, które wskazane są w art. 104. ust. 1. ustawy prawo bankowe stanowiący, iż bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności *bankowe*, są obowiązane zachować tajemnicę *bankową*, która obejmuje wszystkie informacje dotyczące czynności *bankowej*, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje.

Proces weryfikacyjny to proces polegający na sprawdzeniu i potwierdzeniu danych uzyskanych we wcześniejszym procesie identyfikacji i powinien być wykonany przed nawiązaniem relacji biznesowej z klientem. W praktyce przeprowadza się ją najczęściej równolegle do procesu identyfikacji. W celu zapewnienia jakości informacji niezbędnej do

wykonania procesów stosowania środków bezpieczeństwa finansowego wobec Klienta, instytucja obowiązana powinna dołożyć starań, aby źródła informacji wykorzystywane do weryfikacji tożsamości klienta były wiarygodne oraz aby status dokumentów został odpowiednio potwierdzony tak, by mogły one służyć jako dowód, że identyfikacja i weryfikacja zostały przeprowadzone zgodnie z obowiązującymi przepisami prawa. Procedury instytucji obowiązanej powinny określać metody weryfikacji uzależnione od zidentyfikowanej klasy ryzyka. Instytucja obowiązana określa, kiedy stosuje weryfikację klienta przy użyciu metod opartych na dokumentach, kiedy stosuje nie dokumentowe metody weryfikacji, a kiedy kombinację obu tych metod.

Generalny Inspektor Ochrony Danych Osobowych wskazuje, iż zgodnie z art. 36 ust. 1 ustawy administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Podzielać można obawy, iż przekazywanie danych drogą telefoniczną może być uznane za nie w pełni bezpieczne, choćby ze względu na brak całkowitej pewności co do identyfikacji rozmówcy. W przypadku przeprowadzenia przez Bank weryfikacji w celach przedstawienia spersonalizowanej oferty marketingowej, może Pan w obawie o bezpieczeństwo ochrony danych, odmówić udzielenia odpowiedzi, bądź zrezygnować z usług marketingowych przedstawianych drogą telefoniczną.

Jak wynika z powyższego - banki - jako instytucje zobowiązane na podstawie ustaw odrębnych – mają obowiązek zarejestrować, a tym samym weryfikować dokumenty zawierające dane osobowe osoby, która chce przeprowadzić transakcję, której równowartość przekracza 15 000 euro oraz bez względu na kwotę w przypadku, gdy okoliczności takiej transakcji wskazują, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu bez względu na jej wartość i charakter, albo w celach realizacji dalszych postanowień umowy zawartej z bankiem.

Przedstawiając powyższe, informuję, że więcej informacji na temat zasad przetwarzania danych osobowych, treść obowiązujących w tym zakresie aktów prawnych, a także wskazówki co do ich stosowania w praktyce, znajduje się na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych (www.giodo.gov.pl) oraz w serwisie edugiodo.giodo.gov.pl.