BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH

Departament Inspekcji

Zestawienie wyników sprawdzeń zgodności przetwarzania danych z przepisami o ochronie danych osobowych, które zostały przeprowadzone przez administratorów bezpieczeństwa informacji w bankach w zakresie marketingu kierowanego do klientów oraz osób niebędących klientami banków

Warszawa 2017 r.

1. Wprowadzenie

Generalny Inspektor Ochrony Danych Osobowych zwrócił się, na podstawie art. 19b ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922), zwanej dalej „ustawą" o ochronie danych osobowych, do administratorów bezpieczeństwa informacji w 20 bankach, w tym w 9 bankach spółdzielczych, o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą o ochronie danych osobowych, w tych podmiotach.

Zakresem sprawdzeń objęto przetwarzanie danych osobowych przez banki w zakresie marketingu kierowanego do klientów oraz osób nie będących klientami banku, w szczególności ustalenie:

1. W jaki sposób są przetwarzane dane osobowe w celach marketingowych, w tym wskazanie:

1) poszczególnych form zbierania danych osobowych od osób, których danych dotyczą, lub podmiotów trzecich (np. pisemnie – w formie papierowej, elektronicznie, telefonicznie);

2) jakiej kategorii osób dane dotyczą (czy dane dotyczą klientów czy też innych osób);

3) czy dane są pozyskiwane od osób, których dotyczą czy też z innych źródeł;

4) w przypadku pozyskiwania danych z innych źródeł - od jakich podmiotów i na jakiej podstawie prawnej dane są pozyskiwane;

5) podstawy prawnej przetwarzania danych osobowych w celach marketingowych, tj. czy dane osobowe są przetwarzane na podstawie art. 23 ust. 1 pkt 5 ustawy, czy też osoby, których dane dotyczą, wyraziły zgodę na ich przetwarzanie przez bank, jako administratora danych, w celach marketingowych;

6) czy dane są przetwarzane w celu marketingu własnych produktów i usług, czy też w celu marketingu produktów i usług innych podmiotów;

7) zakresu przetwarzanych danych osobowych;

8) w jakim celu jest przetwarzana każda z ww. danych osobowych;

9) sposobu dopełnienia obowiązków administratora danych wynikających z art. 24 i art. 25 ustawy, tj. czy informacje, o których mowa w tych przepisach są przekazywane osobom, których dane osobowe dotyczą, w formie pisemnej, telefonicznie, na stronie internetowej;

10) w jakim zbiorze dane osobowe są przetwarzane;

11) po jakim czasie dane są usuwane;

12) w przypadku przetwarzania danych na podstawie art. 23 ust.1 pkt 5 ustawy - w jaki sposób są rozpatrywane sprzeciwy wobec przetwarzania danych w celach marketingowych, o których mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Czy Bank powierzył innym podmiotom przetwarzanie danych osobowych, zgodnie z art. 31 ust. 1 ustawy, w celach marketingowych, a jeżeli tak, to w jakim zakresie i celu.

3. Czy dane osobowe udostępniane są innym podmiotom, a jeżeli tak, to na jakiej podstawie prawnej, w jakim celu, zakresie i w jaki sposób.

Sprawdzenia zostały przeprowadzone przez administratorów bezpieczeństwa informacji w 2016 r.

2. Charakterystyka sposobów przetwarzania danych w bankach objętych sprawdzeniami

Na podstawie informacji zawartych w sprawozdaniach i w załączonych do nich dowodach stwierdzono, iż 14 z 20 banków przetwarza dane osobowe w celu marketingu własnych lub cudzych produktów, natomiast pozostałe 6 nie przetwarza danych osobowych w tym celu.

Banki, prowadząc działalność bankową, zazwyczaj decydują się również na prowadzenie marketingu mającego na celu pozyskanie nowych klientów bądź też nakłonienie swoich dotychczasowych klientów do skorzystania z określonego produktu oferowanego przez bank. Marketing może mieć formę bezpośrednią lub pośrednią. Marketing pośredni jest kierowany do niesprecyzowanej liczby osób i jest prowadzony m.in. poprzez zamieszczanie informacji o ofercie w mediach czy na tablicach ogłoszeniowych (billboardach), natomiast marketing bezpośredni polega na przedstawieniu konkretnej osobie oferty banku. Prowadzenie marketingu bezpośredniego wiąże się nierozłącznie z przetwarzaniem danych osobowych osób, do których jest on kierowany. Są to co najmniej dane kontaktowe, a w przypadku, gdy bank zdecyduje się na profilowanie takiej osoby w celu przedstawienia oferty produktu możliwie najlepiej odpowiadającego jej potrzebom, również inne dane osobowe niezbędne do dokonania takiego profilowania.

Marketing bezpośredni jest prowadzony poprzez przedstawienie oferty produktów banku za pośrednictwem poczty elektronicznej lub telefonicznie. Nie stwierdzono, aby którykolwiek z banków objętych sprawdzeniami przesyłał swoją ofertę pocztą tradycyjną.

Zazwyczaj klienci banków podczas zawierania umowy z bankiem oraz w trakcie jej trwania mogą wyrazić zgodę na przetwarzanie danych osobowych w celach marketingu produktów i usług banku, a także innych podmiotów. Zaznaczyć w tym miejscu należy, iż wystarczającą podstawę przetwarzania danych klientów w celu marketingu produktów i usług administratora danych stanowi usprawiedliwiony cel administratora danych (art. 23 ust. 1 pkt 5 ustawy[1] w związku z art. 23 ust. 4 pkt 1 ustawy o ochronie danych[2]). Pozyskiwanie przez banki zgody w tych przypadkach jest zbędne, gdyż bank przetwarza dane osobowe w celu realizacji marketingu własnych usług. Banki często prowadzą marketing produktów i usług innych podmiotów,

[1] Art. 23 ust. 1 pkt 5. Przetwarzanie danych jest dopuszczalne wtedy, gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

[2] Art. 23 ust. 4 pkt 1. Za prawnie usprawiedliwiony cel, o którym mowa w art. 23 ust. 1 pkt 5, uważa się w szczególności marketing bezpośredni własnych produktów lub usług administratora danych.

najczęściej wchodzących w skład grupy kapitałowej (do której należy także i bank), takich jak inne banki czy towarzystwa ubezpieczeniowe.

Kierowana do klientów oferta jest najczęściej w odpowiedni sposób przygotowana (sprofilowana) w oparciu o dane, które są w posiadaniu banku.

3. Podsumowanie wyników sprawdzeń

3.1. Ogólna ocena kontrolowanej działalności

Inspektorzy, oceniając wyniki sprawdzeń przeprowadzonych przez ABI uznali, iż w zakresie objętym sprawdzeniami nieprawidłowości popełnione przez bank polegały na stosowaniu wadliwych klauzul zgód na przetwarzanie danych osobowych w celach marketingowych, a w jednym przypadku bank nie legitymował się podstawą prawną przetwarzania w tym celu danych osobowych osób nie będących jego klientami.

3.2. Synteza wyników sprawdzeń

1. Na podstawie informacji zawartych w sprawozdaniach ze sprawdzeń i załączonych do nich dowodów inspektorzy GIODO stwierdzili, iż osiem banków pozyskuje zgodę na przetwarzanie danych osobowych w celach marketingowych, stosując klauzule zawierające łącznie dwie lub więcej z następujących zgód:

- zgodę na przetwarzanie w celach marketingu własnych produktów lub usług;
- zgodę na przetwarzanie w celach marketingu produktów lub usług innych podmiotów;
- zgodę na używanie telekomunikacyjnych urządzeń końcowych w celu prowadzenia marketingu bezpośredniego, o której mowa w art. 172 ust. 1 ustawy[3] z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, z późn. zm.);
- zgodę na otrzymywanie informacji handlowej, o której mowa w art. 10 ustawy[4] z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2016 r. poz. 1030).

Zgoda na przetwarzanie danych osobowych powinna spełniać wymogi określone w art. 7 pkt 5 ustawy[5], czyli musi być sformułowana w sposób wyraźny i jednoznaczny oraz wyróżniać się spośród innych pochodzących od osoby ją wyrażającej informacji i oświadczeń woli. Niezbędne

[3] Art. 172 ust. 1 ustawy Prawo telekomunikacyjne. Zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę.

[4] Art. 10 ust. 1 ustawy o świadczeniu usług drogą elektroniczną. Zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny (art. 10 ust. 2 powołanej ustawy).

5 Art. 7 pkt 5. Ilekroć w ustawie mówi się o zgodzie osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

jest również umożliwienie tej osobie swobodnego wyrażenia woli w przedmiocie zgody na przetwarzanie jej danych, m.in. poprzez zapewnienie możliwości wyrażenia zgody niezależnie od innych oświadczeń woli.

Zawarcie kilku zgód w treści jednej klauzuli powoduje, iż osoba, która chciałaby wyrazić tylko jedną lub kilka spośród tych zgód, nie ma takiej możliwości, a zatem nie ma swobody w dysponowaniu swoimi danymi osobowymi.

Zgoda na przetwarzanie danych osobowych powinna być zatem wyodrębniona od innych zgód, również tych, które dotyczą używania telekomunikacyjnych urządzeń końcowych w celu prowadzenia marketingu bezpośredniego czy też otrzymywania informacji handlowych drogą elektroniczną. Przemawia za tym również fakt, iż zgodę na używanie telekomunikacyjnych urządzeń końcowych w celu prowadzenia marketingu bezpośredniego i zgodę na otrzymywanie informacji handlowej drogą elektroniczną regulują przepisy odrębne od przepisów ustawy o ochronie danych osobowych, tj. odpowiednio Prawo telekomunikacyjne i ustawa o świadczeniu usług drogą elektroniczną.

Stanowisko dotyczące konieczności wyodrębnienia zgody na przetwarzanie danych osobowych od innych oświadczeń woli podzielane jest również w orzecznictwie sądów administracyjnych. Jak wskazał Naczelny Sąd Administracyjny w wyroku z 10 stycznia 2013 r. (sygn. akt I OSK 2029/11), w orzecznictwie istnieje zgodność co do tego, że sposób pozyskiwania zgody na przetwarzanie danych umożliwiać powinien świadome i swobodne wyrażenie woli.

Naczelny Sąd Administracyjny podkreślił, iż zgoda na przetwarzanie danych nie może mieć charakteru abstrakcyjnego, lecz winna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania. Strona nie może być przy tym wprowadzona w błąd. Jeżeli zatem oświadczenie woli dotyczyć ma istotnie różniących się celów przetwarzania, zgoda powinna być wyrażona wyraźnie pod każdym z tych celów przetwarzania.

Mając na uwadze powyższe stwierdzono, iż zastosowana przez banki forma pozyskiwania zgody na przetwarzanie danych osobowych w celach marketingowych, narusza przepisy ustawy o ochronie danych, bowiem decyzja w sprawie wyrażenia wskazanej zgody nie mogła zostać podjęta swobodnie i nie miała charakteru samodzielnego. Sprzeciwiało się to zatem art. 23 ust. 1 pkt 1 ustawy[6] w związku z art. 7 pkt 5 ustawy o ochronie danych osobowych.

Jeden z banków, mimo iż pozyskiwał od klientów zgodę na przetwarzanie danych osobowych w celach marketingowych w sposób, o którym mowa powyżej, nie przetwarzał danych

[6] Art. 23 ust. 1 pkt 1. Przetwarzanie danych jest dopuszczalne wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych

w tych celach. Wobec tego inspektorzy zwrócili się o podjęcie działań mających na celu modyfikację tej klauzuli.

Wobec pozostałych banków, w których stwierdzono stosowanie wadliwych klauzul zgód, wszczęto postępowania administracyjne. Cztery banki usunęły ww. uchybienie w toku prowadzonych postępowań administracyjnych i z tych względów postępowania te zostały umorzone. Wobec trzech innych banków Generalny Inspektor Ochrony Danych Osobowych wydał decyzje nakazujące usunięcie uchybienia poprzez zapewnienie swobody w przedmiocie złożenia przez klientów zgody na przetwarzanie danych osobowych w celach marketingu produktów banku.

2. Spośród 20 administratorów bezpieczeństwa informacji, którzy dokonali sprawdzenia przetwarzania danych osobowych przez banki w zakresie marketingu kierowanego do klientów oraz osób nie będących klientami banków, tylko jeden z nich stwierdził naruszenie przepisów o ochronie danych osobowych, mimo iż w wielu przypadkach ustalenia dokonane przez administratorów bezpieczeństwa informacji w toku sprawdzeń dawały podstawę do stwierdzenia takich uchybień.

Nieprawidłowości stwierdzone przez ABI polegały m.in. na zbyt rzadkim sprawdzaniu w systemie informatycznym, czy klient nie odwołał zgody na przetwarzanie danych osobowych do celów marketingowych[7] lub nie zgłosił sprzeciwu wobec przetwarzania danych osobowych w tych celach[8], co mogło skutkować skierowaniem telefonicznej oferty marketingowej do osoby, wobec której brak było podstawy prawnej do przetwarzania jej danych osobowych.

Powyższe naruszenia zostały usunięte w terminach określonych przez ABI w sprawozdaniu.

4. Uwagi dotyczące sporządzania sprawozdań przez ABI

Duża liczba otrzymywanych od ABI sprawozdań z ww. sprawdzeń nie zawierała wszystkich niezbędnych informacji i dowodów potwierdzających dokonane ustalenia. W związku z tym inspektorzy GIODO zwracali się na piśmie (często wielokrotne) do administratora bezpieczeństwa informacji o złożenie dodatkowych wyjaśnień i dowodów niezbędnych do stwierdzenia, czy przetwarzanie danych osobowych w zakresie objętym sprawdzeniem odbywa się zgodnie z przepisami o ochronie danych osobowych. Niekiedy sprawozdania, jak również wyjaśnienia, o których mowa powyżej, były przesyłane bezpośrednio przez ABI, a nie za pośrednictwem administratorów danych. W niektórych przypadkach w sprawozdaniach nie wskazano, które z załączonych dokumentów dotyczą poszczególnych ustaleń w nim zawartych. Uniemożliwiało to dokonanie przez inspektorów oceny przeprowadzonych przez ABI czynności i wymagało wystąpienia do ABI o przeprowadzenie dodatkowych czynności wyjaśniających.

[7] Zgodnie z art. 7 ust. 5 ustawy zgoda może być odwołana w każdym czasie.

[8] Zgodnie z art. 32 ust. 1 pkt 8 ustawy każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych;

Treść sprawozdań wskazywała także na niepełną wiedzę ABI w zakresie ochrony danych osobowych niezbędną do sporządzenia sprawozdania ze sprawdzenia, w szczególności w zakresie zgromadzenia adekwatnych dowodów w stosunku do istniejącego stanu faktycznego. ABI wskazywali w sprawozdaniach, iż nie stwierdzili nieprawidłowości w procesie przetwarzania danych osobowych, podczas gdy z analizy dokumentacji ze sprawdzeń wynikało, iż takie nieprawidłowości miały miejsce.