FUNDACJA PANOPTYKON

Warszawa, 27 czerwca 2018 r.

Uwagi Fundacji Panoptykon[1] do Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe[2]

Związek Banków Polskich (dalej: ZBP) zwrócił się do Fundacji z prośbą o konsultację Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe (dalej: Kodeks). 20 czerwca 2018 r. przedstawicielki Fundacji odbyły spotkanie z przedstawicielami ZBP, podczas którego przedyskutowane zostały najważniejsze wątpliwości Fundacji do Kodeksu. Niniejszy dokument stanowi podsumowanie najważniejszych zgłoszonych wątpliwości i ustaleń wynikających ze spotkania. Pozostałe uwagi, w tym uwagi dodatkowe, nieomówione na spotkaniu przekazujemy w formie zaznaczeń i komentarzy w treści Kodeksu stanowiącej załącznik do niniejszego pisma. W związku z zapowiedzią ZBP, że niektóre przepisy Kodeksu zostaną zmienione, zgłaszamy gotowość do skonsultowania wprowadzonych zmian.

1. Podstawa prawna do przetwarzania danych w celach marketingowych

Nasze wątpliwości budzą przyjęte przez autorów Kodeksu podstawy prawne do przetwarzania danych w celach marketingowych. Zgodnie z poczynionym przez autorów Kodeksu rozróżnieniem, dane mogą być wykorzystywane do trzech rodzajów marketingu: marketingu bezpośredniego banków, marketingu podmiotów z grupy kapitałowej oraz marketingu podmiotów trzecich. W dokumencie brak jest jednak spójności co do podstaw prawnych, na które banki będą się powoływać w przypadku poszczególnych rodzajów marketingu.

Załącznik nr 4 do Kodeksu, precyzując cele i podstawy prawne przetwarzania, wskazuje, że przy marketingu bezpośrednim banku oraz podmiotów z grupy kapitałowej podstawą prawną będzie **zgoda albo uzasadniony interes**. Autorzy Kodeksu nie podają jednak przykładów, w których banki będą mogły się powołać na taką a nie inną podstawę prawną. W rubryce Załącznika nr 4 dotyczącej uzasadnionych interesów banków jako jeden z przykładów takich interesów podano marketing bezpośredni banku i podmiotów z grupy kapitałowej. Nie jest w związku z tym jasne, czy i kiedy taki marketing może odbywać się w oparciu o zgodę, zwłaszcza, że w samej treści kodeksu ani razu nie pojawia się nawiązanie do zgody jako podstawy prawnej marketingu.

Załącznik nr 4 **pomija ponadto milczeniem podstawę prawną dla marketingu podmiotów trzecich**. Treść kodeksu wskazuje z kolei, że podstawą dla przetwarzania danych w celu marketingu podmiotów trzecich stanowić będzie uzasadniony interes. W szczególności pkt 11 części E wskazuje, że procesy marketingu podmiotów trzecich oparte na profilowaniu mogą stanowić prawnie uzasadniony interes banków wtedy, gdy odbywa się to w sposób, który nie powoduje nadmiernej ingerencji w prawo do prywatności i którego podmiot danych może się racjonalnie spodziewać. Autorzy Kodeksu nie podają jednak żadnych przykładów, w których marketingu podmiotów trzecich nie będzie można oprzeć na uzasadnionym interesie. **Uważamy, że to może doprowadzić do sytuacji, w której różne banki będą stosować różne**

[1] Stanowisko przygotowane przez Karolinę Iwańską i Katarzynę Szymielewicz.
[2] Wersja z 10 stycznia 2018 r.

standardy. Zadaniem Kodeksu powinno tymczasem być dążenie do ujednolicenia praktyk, szczególnie tych tak daleko ingerujących w prywatność jednostek.

W kontekście marketingu podmiotów z grup kapitałowych istotne jest zastrzeżenie, że taki marketing nie może w każdej sytuacji odbywać się w oparciu o uzasadniony interes banku. W skład grupy kapitałowej danego banku mogą bowiem wchodzić bardzo różne podmioty. Klienci banku mogą mieć podstawy do spodziewania się marketingu ze strony niektórych z nich (np. podmiotów oferujących ubezpieczenie kredytu), jednak w przypadku innych, niezwiązanych stricte z sektorem finansowo-ubezpieczeniowym, nie sposób zaakceptować takiego założenia.

Dlatego **postulujemy wyraźne uregulowanie podstaw prawnych do prowadzenia marketingu** (własnego, podmiotów z grupy kapitałowej i podmiotów trzecich). Uważamy, że marketing podmiotów z grupy kapitałowej niezwiązanych z sektorem finansowych i marketing podmiotów trzecich powinien być **oparty o zgodę** osoby, której dane dotyczą, ponieważ w większości przypadków osoba ta nie ma racjonalnych podstaw do spodziewania się, że dane przekazane przez nią bankowi będą wykorzystane do marketingu ze strony tych podmiotów. Jeśli w opinii banków istnieją wyjątki od tej reguły (tj. sytuacje, w których klienci oczekują marketingu podmiotów trzecich lub podmiotów z grupy kapitałowej i przesłanka uzasadnionego interesu znajdzie do nich zastosowanie), Kodeks jest tym miejscem, w którym warto je skazać i scharakteryzować.

2. Scoring a zautomatyzowane podejmowanie decyzji

Zagadnienie oceny punktowej klientów (scoringu) oraz podejmowania decyzji kredytowych było ważnym przedmiotem dyskusji podczas spotkania 20 czerwca. ZBP przekazał nam informację, że scoring traktowany jest przez banki jako zwykłe profilowanie, a nie jako zautomatyzowane podejmowanie decyzji. W związku z tym, dla samego scoringu nie są przewidywane gwarancje z art. 22 RODO. Banki przyjęły jednak jako dobrą praktykę wyższy standard przejrzystości i zamierzają informować klientów o zasadach dokonywania scoringu, ale tylko na poziomie generalnym (przekazywane będą zasady prowadzenia tego procesu dla wszystkich klientów, bez odniesienia do indywidualnych ocen punktowych). ZBP poinformował nas również, że na podstawie art. 13 i 14 RODO klient ma prawo dostępu do wszystkich danych, jakie bank bierze pod uwagę (przetwarza) w ramach scoringu i w procesie podejmowania decyzji kredytowej. **Co do zasady nie mamy zastrzeżeń do takiej oceny prawnej scoringu.**

W zakresie zautomatyzowanego podejmowania decyzji kredytowych obecne brzmienie pkt. 4 w części E nie uwzględnia gwarancji przewidywanych przez art. 22 ust. 3 RODO (prawo do uzyskania interwencji ludzkiej, do wyrażenia własnego stanowiska oraz do zakwestionowania decyzji).Zgodnie z zapewnieniami ZBP, spowodowane jest to faktem, że poddana konsultacjom wersja Kodeksu pochodzi ze stycznia 2018 r., kiedy to procedowany w Ministerstwie Cyfryzacji projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 zawierał podstawę prawną dla profilowania przez banki – zgodnie z art. 22 RODO w takim przypadku właściwe środki ochrony praw i wolności osób fizycznych powinny być ustanowione na poziomie ustawy, a nie przez konkretnego administratora. Obecna wersja projektu ustawy nie zawiera już jednak postanowień dotyczących profilowania w sektorze bankowym. W związku ze zgłoszonymi przez nas wątpliwościami ZBP uznał, że **sektor bankowy w pełni obowiązuje zatem reżim art. 22 RODO i zapowiedział uzupełnienie Kodeksu o gwarancje przewidywane w tym przepisie**.

Zgodnie z informacjami przekazanymi przez ZBP, w przypadku podejmowania decyzji kredytowych brane są pod uwagę następujące czynniki (w kolejności od najważniejszego): aktualna sytuacja finansowa, historia kredytowa (raport BIK) i wynik oceny punktowej (scoringu). Klient ma prawo dokładnego wyjaśnienia tego, w jaki sposób decyzja kredytowa została podjęta, kiedy w grę wchodzą kryteria finansowe (aktualna sytuacja finansowa i historia kredytowa). W tym zakresie bank nie może zataić żadnych danych ani czynników. Z kolei **adekwatność danych branych pod uwagę przy scoringu jest oceniania wyłącznie przez organy nadzorcze** (Prezesa Urzędu Ochrony Danych Osobowych i Komisję Nadzoru Finansowego). **Nawet na etapie decyzji kredytowej klient nie ma prawa do wyjaśnienia, w jaki sposób zostały „zważone" poszczególne czynniki, jakie wpłynęły na wynik scoringu.** Banki uważają, że ich ujawnienie naruszyłoby tajemnicę handlową (fakt posługiwania się przez poszczególne banki różnymi modelami i algorytmami może być – zdaniem ZBP – elementem przewagi konkurencyjnej).

Naszym zdaniem takie podejście jest dyskusyjne, ale może zostać zaakceptowane, jeśli ocena punktowa rzeczywiście nie waży na całej decyzji kredytowej. Jeśli w konkretnych sytuacjach będą pojawiać się wątpliwości, ciężar dowodu co do tego, że zaważyły kryteria finansowe (a nie wynik scoringu) powinien spoczywać na banku. Rekomendujemy, żeby taką regułę wprost zapisać w Kodeksie. Ponadto podkreślamy, że kluczowe znaczenie dla ochrony praw podmiotów danych będzie miała ocena adekwatności danych wykorzystywanych do scoringu, nad którą powinny czuwać organy nadzorcze. Rozumiemy, że ze względu na wysokie ryzyko dla praw i wolności podmiotów danych, banki standardowo będą występowały do Prezesa UODO z wnioskiem o uprzednie konsultacje modelu (w tym zakresu danych osobowych) wykorzystywanego do scoringu. Rekomendujemy, aby taką wykładnię Art. 36 RODO wpisać do Kodeksu.

3. Inne przypadki profilowania

- **Profilowanie w ramach korzystania z systemu bankowości elektronicznej lub aplikacji mobilnej**

Nasze wątpliwości wzbudziło brzmienie pkt. 12 w części E, zgodnie z którym „zawarcie umowy, a tym samym przyjęcie regulaminu korzystania z systemu bankowości elektronicznej lub aplikacji mobilnej wykorzystującej profilowanie będzie stanowić podstawę prawną profilowania danych Klientów w celu świadczenia im usług/funkcjonalności opartych na profilowaniu danych oraz w celu przygotowania oraz prezentowania im dopasowanych/zindywidualizowanych ofert marketingowych". Sposób sformułowania tego przepisu sugeruje, że podstawą prawną dla profilowania w związku z korzystaniem przez klientów z systemu bankowości elektronicznej lub aplikacji mobilnej będzie niezbędność do wykonania umowy. W związku z tym niezrozumiałe są postanowienia Kodeksu dotyczące sprzeciwu wobec profilowania (pkt. 13). Na gruncie RODO sprzeciw przysługuje wobec przetwarzania danych w oparciu o uzasadniony interes administratora, a nie w oparciu o niezbędność do wykonania umowy.

Podczas spotkania 20 czerwca przedstawiciele ZBP przyznali, że sformułowanie pkt. 12 jest mylące i zadeklarowali jego zmianę. Dowiedzieliśmy się, że celem tego przepisu było jedynie nawiązanie do umowy ramowej, jaką klient zawiera z bankiem, a która zawiera postanowienia dotyczące korzystania z systemu bankowości elektronicznej i aplikacji mobilnej. Oba rodzaje profilowania, o których mowa w pkt. 12 (profilowanie w celu świadczenia usług/funkcjonalności oraz profilowanie w celach marketingowych) mają się z kolei odbywać **w**

oparciu o uzasadniony interes administratora. W tym kontekście postulujemy przeformułowanie i doprecyzowanie tego przepisu.

- **Zindywidualizowane oferty marketingowe**

Pkt 10 części E przewiduje, że „zindywidualizowane oferty marketingowe kierowane do Klientów, będące wynikiem profilowania, co do zasady nie są zautomatyzowanymi decyzjami, w zakresie w jakim nie wywołują wobec Klienta skutków prawnych lub w inny sposób istotnie nie wpływają na sytuację Klienta". **Uważamy za zasadne wskazanie przykładów sytuacji, w jakich przedstawienie klientom zindywidualizowanych ofert marketingowych będzie traktowane jak zautomatyzowana decyzja.** W przeciwnym razie w poszczególnych bankach mogą pojawić się różne standardy w tym zakresie.

Zadaniem Kodeksu powinno być dążenie do ujednolicenia praktyk, szczególnie tak daleko ingerujących w prywatność klientów i budzących uzasadnione kontrowersje. **Autorzy Kodeksu mogą zainspirować się wytycznymi Grupy Art. 29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania**[3], które podają konkretne przykłady, w których decyzja o przedstawieniu takiej a nie innej oferty (reklamy) będzie miała istotny wpływ na osoby, których dane dotyczą (np. jeśli reklama wykorzystuje wiedzę o słabościach danej osoby lub jest związana ze śledzeniem aktywności użytkowników na różnych stronach internetowych czy na różnych urządzeniach).

Mylące jest także drugie zdanie komentowanego przepisu – jego brzmienie sugeruje, że istotny wpływ na klienta wg Kodeksu ma wyłącznie taka zindywidualizowana oferta, która prowadzi do dyskryminacji lub nierównego traktowania opartego na nieobiektywnych kryteriach. Zgodnie z deklaracją przedstawicieli ZBP, celem tego postanowienia jest wprowadzenie zakazu stosowania dyskryminacyjnych ofert marketingowych. Jeśli tak, to treść Kodeksu powinna to odzwierciedlać.

4. Anonimizacja

W pkt. 4 części D autorzy Kodeksu piszą, że „usunięcie danych osobowych osób, których dane dotyczą, następuje np. poprzez ich zniszczenie lub anonimizację". Te dwa procesy – zniszczenie danych oraz anonimizacja – nie są jednak tożsame. Anonimizacja sama w sobie stanowi dalsze przetwarzanie danych[4]. Ta wątpliwość została poruszona podczas spotkania przedstawicieli ZBP z przedstawicielkami Fundacji. ZBP uwzględnił zasadność tej uwagi i zapowiedział dodanie w Kodeksie odrębnego punktu dotyczącego warunków, jakie powinien spełniać proces anonimizacji, oraz sytuacji, w których jest rekomendowany.

5. Przetwarzanie danych po upływie pierwotnego okresu przetwarzania

Mylące jest brzmienie pkt. 3 w części D, który wymienia sytuacje, w których dopuszczalne jest „dalsze przetwarzanie danych" na podstawie prawnie uzasadnionego interesu administratora. Punkt poprzedzający reguluje dopuszczalny okres przechowywania danych w sytuacji, gdy pierwotne cele przetwarzania zostały już osiągnięte. Można zatem odnieść wrażenie, że katalog z pkt. 3 wprowadza nowe cele i podstawy przetwarzania w stosunku do danych, które nie mogą już być przetwarzane ani w oparciu o pierwotną podstawę prawną (np. niezbędność do wykonania umowy), ani w oparciu o przepis prawa (np. prawo o rachunkowości) .

[3] Wytyczne WP 251, dostępne pod adresem: https://uodo.gov.pl/data/filemanager_pl/19.pdf
[4] Por. Opinia Grupy Art. 29 5/2014 w sprawie technik anonimizacji, WP 216, dostępna pod adresem: https://giodo.gov.pl/pl/1520203/7808 .

Po poruszeniu tej wątpliwości na spotkaniu z przedstawicielami ZBP rozumiemy, że intencją tego przepisu było wskazanie typowych sytuacji, w których banki mogą przetwarzać dane w oparciu o swój uzasadniony interes (niezależnie od istnienia lub nie innych podstaw prawnych), w szczególności w ramach realizowania rekomendacji organów nadzorczych (głównie Komisji Nadzoru Finansowego). **W związku z tym, sygnalizujemy, że ten przepis wymaga doprecyzowania**.

Niezależnie od powyższego, uważamy, że **również w przypadku wypełniania rekomendacji organów nadzorczych przetwarzanie nie może być bezterminowe**. Dlatego postulujemy wprowadzenie ram czasowych dla usuwania danych, o których mowa w poszczególnych punktach tego przepisu.

6. Żądanie przeniesienia części danych

W części regulującej standardy przenoszenia danych (część C, rozdział VIIIa, pkt 8) Kodeks przewiduje, że klient, który składa wniosek o przeniesienie danych jest zobowiązany wskazać, jakie konkretnie dane osobowe objęte są jego żądaniem. Takie sformułowanie sugeruje, że klient każdorazowo musi określić zakres danych, nawet jeśli nie ma świadomości, jakie dane na jego temat bank przetwarza. Ta wątpliwość została wyjaśniona na spotkaniu z przedstawicielami ZBP. Rozumiemy, że ten przepis ma dotyczyć tylko tych sytuacji, w których klient żąda przeniesienia części swoich danych. W celu uniknięcia wątpliwości interpretacyjnych, które mogą skutkować bezzasadnym ograniczeniem praw osób, których dane dotyczą, postulujemy doprecyzowanie tego przepisu.

7. Pozostałe uwagi

Pozostałe uwagi przekazujemy w formie zaznaczeń i komentarzy w treści Kodeksu. Uwagi te są, w dużej mierze, związane z naszymi wątpliwościami interpretacyjnymi lub nieścisłościami językowymi. Ponadto w kilku miejscach zwracamy uwagę na zasadność podania przykładów, które ułatwiłyby bankom interpretację poszczególnych postanowień. Wprowadzenie konkretnych przykładów realizowałoby zarazem cel Kodeksu, jakim jest doprecyzowanie zasad przetwarzania danych określonych w RODO i ujednolicenie praktyk stosowanych przez firmy z jednej branży. W przeciwnym razie obawiamy się, że klientom niektórych banków będą przysługiwać niższe gwarancje i standardy w zakresie ochrony danych osobowych.