Wdrażanie RODO w bankach na przykładzie „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe”[1]

dr *Tadeusz Białek*[2]
Damian Wyrzykowski[3]

Celem niniejszego opracowania jest prezentacja opracowanego przez Związek Banków Polskich projektu „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe” (dalej jako: Kodeks) jako przykładu działań wdrażających rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[4] w polskim sektorze bankowym oraz jego podmiotach. Aby umożliwić bezpośrednie odniesienie ww. zagadnienia do kontekstu legislacyjnego w postaci RODO, omówienie treści projektu Kodeksu zostanie poprzedzone ogólną charakterystyką instytucji kodeksu postępowania (*code of conduct*) na gruncie przepisów tego rozporządzenia.

Uwagi wstępne

Z dniem 25.5.2018 r. rozpoczęło się stosowanie RODO. Zakres oraz charakter zmian przewidzianych przez ten akt prawny jest na gruncie literatury często określany jako rewolucyjny[5], zwłaszcza w odniesieniu do zadań oraz obowiązków administratorów danych osobowych[6]. W tym też kontekście podnosi się, iż w ramach wprowadzanych przepisów na administratorów danych osobowych przeniesiony zostaje znacznie większy ciężar odpowiedzialności za przestrzeganie zasad i obowiązków wynikających z RODO[7].

Banki – jako podmioty, na których funkcjonowanie przepisy RODO wpływają w znaczący, wszechstronny sposób – już w momencie wejścia w życie RODO, tj. w maju 2016 r., prowadziły działania mające na celu pełne oraz skuteczne dostosowanie swojej działalności do nowych wymogów stawianych przez ten akt prawny. W szczególności należy zwrócić uwagę, iż Związek Banków Polskich – jako izba gospodarcza w rozumieniu ustawy z 30.5.1989 r. o izbach gospodarczych[8] – rozpoczął działania mające na celu informowanie podmiotów polskiego sektora bankowego o zmianach zakładanych przez RODO jeszcze przed wejściem jego przepisów w życie[9]. Mając więc na względzie kluczowe znaczenie dwuletniego okresu dostosowawczego do RODO, który rozpoczął się wraz z wejściem przedmiotowego rozporządzenia w życie[10], banki-członkowie Związku Banków Polskich przyjęły, że jednym z najistotniejszych aspektów pełnego dostosowania polskiego sektora bankowego do wymogów RODO jest opracowanie Kodeksu sektorowego mającego stanowić kodeks postępowania w rozumieniu art. 40 RODO.

Kodeks postępowania (*code of conduct*) jako instytucja przewidziana na gruncie RODO

W art. 40 RODO uregulowano instytucję kodeksów postępowania, która – choć była już znana oraz stosowana na dotychczasowym gruncie prawa ochrony danych[11]

[1] Niniejszy artykuł opiera się na brzmieniu projektu „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe” w wersji z 10.1.2018 r., która na chwilę pisania niniejszego artykułu jest jego najbardziej aktualną wersją. Autorzy zastrzegają możliwość zmiany brzmienia dotychczasowego projektu „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe” oraz zmiany stanu prawnego po dacie przekazania niniejszego artykułu redakcji.

[2] Radca prawny, doktor nauk prawnych, Dyrektor Zespołu Prawno-Legislacyjnego Związku Banków Polskich.

[3] Aplikant radcowski, doktorant na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, prawnik w Zespole Prawno-Legislacyjnym Związku Banków Polskich.

[4] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

[5] *M. Kawecki*, Prawo ochrony danych osobowych jako nowa dziedzina prawa, EPS 2017, Nr 5, s. 4.

[6] *P. Kozik*, Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego, EPS 2017, Nr 5, s. 17.

[7] *E. Bielak-Jomaa*, Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych?, dodatek MoP 2017, Nr 20, s. 3.

[8] T.j. Dz.U. z 2017 r. poz. 1218 ze zm.

[9] Zob. np. informację o zorganizowanej przez Związek Banków Polskich konferencji „Nowa regulacja przetwarzania danych osobowych – General Data Protection Regulation – skutki w sektorze finansowym”, która odbyła się 10.3.2016 r.: https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/marzec/nowa-regulacja-przetwarzania-danych-osobowych-general-data-protection-regulation-skutki-w-sektorze-finansowym (dostęp z 26.4.2018 r.).

[10] *E. Bielak-Jomaa*, Ogólne rozporządzenie…, s. 3.

[11] *P. Litwiński* (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2018, s. 596; *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, s. 821.

– wraz z przyjęciem RODO zyskuje nowy wymiar m.in. poprzez jej dalej idące sformalizowanie oraz wprowadzenie wielu domniemań prawnych łączących się z kodeksami postępowania[12]. W szczególności podkreśla się, że na gruncie RODO instytucja kodeksów postępowania zyskuje na znaczeniu ze względu na zwiększenie możliwości zastosowania mechanizmów wykazania zgodności prowadzonych operacji przetwarzania danych z obowiązującymi przepisami[13].

Zgodnie z art. 40 ust. 1 RODO państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja Europejska zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu RODO. Jak wskazuje przy tym przywołany przepis, kodeksy postępowania powinny być sporządzane z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania, jak również szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. W tym też kontekście podkreśla się, iż kodeksy postępowania mają charakter uregulowań sektorowych[14], stanowiąc instrument samoregulacyjny wspomagający oraz usprawniający proces wdrożenia przepisów RODO i krajowego ustawodawstwa przyjętego na podstawie RODO[15]. Stosowanie kodeksów postępowań ma więc istotne znaczenie dla sposobu realizacji zasad oraz obowiązków wynikających z RODO, jako że kodeksy postępowania wyjaśniają oraz dostosowują tak określone wymogi do konkretnych sektorów i związanej z nimi specyfiki[16]. W tym miejscu można również przywołać treść motywu 98 RODO, w myśl którego sporządzanie kodeksów postępowania ma ułatwiać skuteczne stosowanie RODO „z uwzględnieniem szczególnych cech przetwarzania prowadzonego w niektórych sektorach i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw", przy czym w kodeksach postępowania „można w szczególności dopasować obowiązki administratorów i podmiotów przetwarzających do ryzyka naruszenia praw lub wolności osób fizycznych, jakie może powodować przetwarzanie". W powyższym kontekście zwraca się więc również uwagę na korzyści płynące ze stosowania kodeksów postępowania, nie ograniczając ich przy tym wyłącznie do sfery zwiększenia poziomu przestrzegania wymogów RODO przy przetwarzaniu danych[17]. W tym też względzie wskazuje się, iż stosowanie kodeksów postępowań jest korzystne zarówno dla osób, których dane dotyczą, jak i samych administratorów oraz podmiotów przetwarzających[18].

Co ważne, choć kodeksy postępowania zalicza się do kategorii instrumentów prawa miękkiego (*soft law*)[19], na gruncie RODO pełnią one znaczącą funkcję niosącą ze sobą wiele istotnych implikacji. Kodeksów postępowania w rozumieniu art. 40 RODO nie należy więc traktować jako instrumentów o wyłącznie informacyjnym czy też wizerunkowym charakterze[20]. W szczególności zwraca się uwagę, że poprzez przyjęcie kodeksu postępowania członkowie określonego zrzeszenia (zob. uwagi niżej) zobowiązują się dostosować swoje działania oraz stosować regulacje zawarte w kodeksie, podlegając konsekwencjom ich ewentualnego naruszenia[21]. W tym też kontekście należy pamiętać, iż przepisy RODO przewidują stosowanie mechanizmów kontroli przestrzegania postanowień kodeksów postępowań[22].

Zgodnie z art. 40 ust. 2 RODO zrzeszenia oraz inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres w celu doprecyzowania zastosowania RODO. Na gruncie przywołanego przepisu wskazuje się więc, iż RODO w sposób wyraźny określa dwie kategorie podmiotów mogących wystąpić z inicjatywą dotyczącą kodeksu postępowania, implikując tym samym brak uprawnienia do tworzenia kodeksu postępowania przez indywidualnego administratora[23]. Jednocześnie na gruncie RODO możliwe jest sporządzanie kodeksów postępowania przez organy oraz podmioty publiczne[24]. Podnosi się przy tym również, że przepisy RODO nie definiują pojęcia „zrzeszenia", przez co może być ono rozumiane w różny sposób – na gruncie polskiego prawa przyjmuje się, iż przykładem zrzeszenia, o którym mowa w art. 40 RODO, jest izba gospodarcza[25] (a więc np. Związek Banków Polskich). W tym też względzie na gruncie RODO katalog zrzeszeń mogących wystąpić z inicjatywą dotyczącą kodeksu postępowania jest szeroki i zależny od ustawodawstwa poszczególnych państw członkowskich UE[26].

W art. 40 ust. 2 RODO określono również zakres przedmiotowy kodeksów postępowania, przy czym wyliczenie zawarte w art. 40 ust. 2 lit. a)–k) RODO ma wyłącznie przykładowy charakter, skutkując możliwością uregulowania w kodeksach postępowania również innych kwestii dotyczących stosowania RODO[27]. Zgodnie z przywołanym

[12] *P. Litwiński* (red.), Rozporządzenie…, s. 596–597.
[13] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 821–822.
[14] *P. Litwiński* (red.), Rozporządzenie…, s. 597.
[15] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 819.
[16] *Ibidem.*
[17] *Ibidem.*
[18] *Ibidem.*
[19] *Ibidem.*
[20] *Ibidem.*
[21] *Ibidem.*
[22] *P. Litwiński* (red.), Rozporządzenie…, s. 599; *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 827.
[23] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 824.
[24] *P. Litwiński* (red.), Rozporządzenie…, s. 598.
[25] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 824.
[26] *Ibidem.*
[27] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 825; *P. Litwiński* (red.), Rozporządzenie…, s. 598.

przepisem kodeksy postępowania mogą doprecyzować zastosowanie RODO m.in. w odniesieniu do: rzetelnego i przejrzystego przetwarzania (art. 40 ust. 2 lit. a); prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach (art. 40 ust. 2 lit. b); zbierania danych osobowych (art. 40 ust. 2 lit. c); pseudonimizacji danych osobowych (art. 40 ust. 2 lit. d); informowania opinii publicznej i osób, których dane dotyczą (art. 40 ust. 2 lit. e); wykonywania przez osoby, których dane dotyczą, przysługujących im praw (art. 40 ust. 2 lit. f); informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem (art. 40 ust. 2 lit. g); środków i procedur, o których mowa w art. 24 i 25 RODO, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32 RODO (art. 40 ust. 2 lit. h); zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą (art. 40 ust. 2 lit. i); przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych (art. 40 ust. 2 lit. j); postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą, na mocy art. 77 i 79 RODO (art. 40 ust. 2 lit. k).

W kontekście zakresu przedmiotowego kodeksu postępowania podnosi się, iż jego regulacje powinny obejmować w pierwszej kolejności zagadnienia dotyczące specyfiki określonego sektora oraz jej wpływu na ogólne zasady ochrony danych[28]. Co istotne, postanowienia kodeksu postępowania muszą być zgodne z obowiązującymi przepisami i nie mogą prowadzić do obniżenia poziomu ochrony danych przewidzianego przez RODO[29].

Zgodnie z art. 40 ust. 5 RODO zrzeszenia oraz inne podmioty chcące opracować kodeks postępowania lub zmienić lub rozszerzyć zakres kodeksu już obowiązującego są zobowiązane przedłożyć projekt kodeksu, zmiany lub rozszerzenia organowi nadzorczemu właściwemu na podstawie art. 55 RODO. Organ nadzorczy przeprowadza ocenę, a następnie wydaje opinię o zgodności ww. projektu z RODO i – jeżeli uzna, że stanowi on odpowiednie zabezpieczenia – zatwierdza taki projekt kodeksu, zmiany lub rozszerzenia. Na gruncie art. 40 ust. 6 RODO zatwierdzony projekt kodeksu, zmiany lub rozszerzenia jest następnie rejestrowany oraz publikowany przez organ nadzorczy – jeśli nie dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich UE. Jeżeli bowiem projekt kodeksu postępowania dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, zastosowanie znajduje procedura określona w art. 40 ust. 7–11 RODO, przewidująca uwzględnienie mechanizmu spójności, o którym mowa w art. 63 RODO[30].

„Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe" jako kodeks postępowania (*code of conduct*) dla polskiego sektora bankowego

Mając na względzie wyżej zarysowaną charakterystykę oraz zalety instytucji kodeksów postępowania na gruncie RODO, jak również wychodząc z założenia, iż opracowanie oraz przyjęcie kodeksu postępowania pozwala na lepsze przygotowanie danego sektora do wykazania zgodności procesów przetwarzania danych z przepisami RODO[31], wraz z wejściem RODO w życie w maju 2016 r. Związek Banków Polskich rozpoczął intensywne prace nad projektem stosownego dokumentu, który miałby stanowić kodeks postępowania dla polskiego sektora bankowego. Jednym z najważniejszych założeń przyjętych przez Związek Banków Polskich było przy tym, aby opracowywanie Kodeksu przedstawiało interdyscyplinarny charakter umożliwiający wszechstronne spojrzenie na procesy przetwarzania danych dokonywane przez banki oraz rejestry kredytowe. W tym też względzie Związek Banków Polskich dołożył znacznych starań, aby przedstawiciele banków oraz rejestrów kredytowych biorący udział w bezpośrednim projektowaniu oraz konsultacji Kodeksu reprezentowali wszystkie obszary kluczowe z punktu widzenia omawianego zagadnienia.

Co istotne, mając nieustannie na uwadze, iż kodeks postępowania ma służyć nie tylko administratorom oraz podmiotom przetwarzającym, lecz również – w takim samym stopniu – osobom, których dane dotyczą[32], Związek Banków Polskich projektując Kodeks, przywiązywał szczególną wagę do sposobu formułowania jego treści. Jeżeli bowiem stosowanie kodeksów postępowania ma na celu m.in. podnoszenie poziomu świadomości ochrony danych oraz budowanie zaufania do jakości procesów przetwarzania danych[33], Związek Banków Polskich uznał za niezbędne, aby projektowany Kodeks był przejrzysty oraz zrozumiały dla jak najszerszego grona odbiorców. W tym też względzie przyjęto, iż choć język Kodeksu ma odzwierciedlać terminologię RODO, postanowienia Kodeksu powinny być formułowane w sposób zrozumiały nie tylko dla osób profesjonalnie zajmujących się problematyką prawa ochrony danych osobowych, lecz także dla osób, które w bankach zajmują się obsługą Klientów oraz samych Klientów banku lub rejestru kredytowego.

[28] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 825–826.
[29] *Ibidem.*
[30] *P. Litwiński* (red.), Rozporządzenie…, s. 601.
[31] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 821.
[32] *Ibidem.*
[33] *Ibidem.*

Dla Związku Banków Polskich równie istotne było także położenie nacisku na aspekt praktyczny Kodeksu. Stąd też Kodeks tylko w niezbędny sposób odnosi się wprost do postanowień RODO, starając się przełożyć dyspozycje RODO na praktyczne opisy stosowania określonych instytucji RODO w praktyce bankowej (np. prawo do bycia zapomnianym, prawo do przenoszenia danych, obowiązek informacyjny).

Efektem powyższych starań było sfinalizowanie na forum Związku Banków Polskich – po blisko półtora roku prac – projektu Kodeksu z końcem grudnia 2017 r. Ogólne założenia projektu Kodeksu zostały następnie zaprezentowane publicznie podczas zorganizowanych przez Generalnego Inspektora Ochrony Danych Osobowych 11.1.2018 r. warsztatów „Kodeksy postępowania w świetle RODO"[34].

Główne założenia „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe"

Główne założenia Kodeksu zostały w bezpośredni sposób sformułowane we wprowadzeniu do Kodeksu (dalej jako: Wprowadzenie), które zawiera postanowienia opisujące zakres podmiotowy oraz przedmiotowy Kodeksu, jak również wskazuje ogólne cele, które mają zostać osiągnięte przez przyjęcie oraz stosowanie Kodeksu.

Zgodnie z przyjętymi założeniami Kodeks stanowi zbiór zasad postępowania w zakresie ochrony danych osobowych w polskim sektorze bankowym (ust. 1 Wprowadzenia), będąc doprecyzowaniem zasad przetwarzania i ochrony danych osobowych określonych w RODO z uwzględnieniem specyfiki sektora bankowego (ust. 2 Wprowadzenia). W tym też miejscu warto zwrócić uwagę, że twórcy Kodeksu w sposób bezpośredni zawarli odniesienie do pojęcia „specyfiki sektora bankowego", co stanowi wyraźne nawiązanie do wskazanej na gruncie motywu 98 RODO i art. 40 ust. 1 RODO charakterystyki kodeksów postępowania jako uregulowań sektorowych[35], dostosowujących wymogi RODO do specyfiki konkretnych sektorów[36]. Ponadto, w celu uniknięcia jakichkolwiek wątpliwości odnośnie do charakteru Kodeksu, zawiera on wyraźne postanowienie stwierdzające wprost, że jest to kodeks postępowania w rozumieniu art. 40 RODO (ust. 3 Wprowadzenia).

W odniesieniu do podmiotowego zakresu zastosowania Kodeksu zostało przyjęte, iż ma on zastosowanie do banków krajowych oraz rejestrów kredytowych działających na terytorium Rzeczpospolitej Polskiej, będących członkami Związku Banków Polskich (ust. 4 Wprowadzenia). Kodeks zawiera przy tym postanowienie wskazujące, że banki i rejestry kredytowe przetwarzają dane osobowe w związku z prowadzeniem swojej działalności zgodnie z przepisami ustawy z 29.8.1997 r. – Prawo bankowe[37] oraz innych właściwych ustaw oraz w zakresie działalności wynikającej ze swoich statutów z uwzględnieniem wytycznych i rekomendacji Komisji Nadzoru Finansowego oraz innych właściwych regulatorów (ust. 5 Wprowadzenia).

Co istotne, do stosowania Kodeksu mogą przystąpić również inne niż wyżej wskazane podmioty – dotyczy to w szczególności podmiotów świadczących na rzecz banków i rejestrów kredytowych usługi wymagające przetwarzania danych osobowych, jednakże wyłącznie w zakresie świadczenia takich usług na rzecz banków i rejestrów kredytowych (ust. 6 Wprowadzenia). Przystępując do stosowania Kodeksu, tak określone podmioty zobowiązują się do stosowania wszystkich wyrażonych w nim zasad – w celu przystąpienia do stosowania Kodeksu, właściwy podmiot składa bowiem do Związku Banków Polskich pisemne oświadczenie zawierające zobowiązanie do przestrzegania zasad Kodeksu (ust. 9 Wprowadzenia).

W odniesieniu do zakresu przedmiotowego Kodeksu zostało przyjęte, iż będzie mieć on zastosowanie do przetwarzania danych osobowych Klientów[38], w tym osób, których dane są przetwarzane przez rejestry kredytowe w związku z realizacją przez te rejestry obowiązków i uprawnień wskazanych we właściwych przepisach prawa oraz w aktach wewnętrznych (ust. 7 Wprowadzenia). Jednocześnie Kodeks przewiduje wyraźne wyłączenie – nie ma on mianowicie zastosowania do przetwarzania danych osobowych pracowników, współpracowników oraz kandydatów do pracy w bankach i rejestrach kredytowych (ust. 8 Wprowadzenia).

Główne cele, które mają zostać osiągnięte przez wprowadzenie Kodeksu, zostały określone jako (ust. 10 Wprowadzenia):

– wsparcie banków i rejestrów kredytowych we właściwym stosowaniu RODO z uwzględnieniem cech przetwarzania danych osobowych w sektorze bankowym i szczególnych potrzeb banków i rejestrów kredytowych;

[34] Zob. informację o przedmiotowych warsztatach: https://www.giodo.gov.pl/pl/1520310/10311 (dostęp z 27.4.2018 r.).

[35] *P. Litwiński* (red.), Rozporządzenie…, s. 597.

[36] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 819.

[37] T.j. Dz.U. z 2018 r. poz. 2187 ze zm.

[38] Na gruncie Kodeksu zostało przyjęte, że klient oznacza potencjalnego, aktualnego lub byłego: a) klienta banku oraz jego przedstawicieli, osobę korzystającą z usług świadczonych przez banki niebędącą klientem banku lub osobę, której dane osobowe bank przetwarza w związku z prowadzeniem przez bank działalności obejmujących czynności bankowe oraz w związku z realizacją przez bank obowiązków i uprawnień wskazanych we właściwych przepisach prawa, mających zastosowanie do banków oraz w aktach wewnętrznych banków, takich w szczególności jak statuty (klient banku); b) klienta rejestru kredytowego oraz jego przedstawicieli, osobę korzystającą z usług świadczonych przez rejestr kredytowy niebędącą klientem rejestru kredytowego lub osobę, której dane osobowe rejestr kredytowy przetwarza w związku z prowadzeniem przez rejestr kredytowy działalności oraz w związku z realizacją przez rejestr kredytowy obowiązków i uprawnień wskazanych we właściwych przepisach prawa, mających zastosowanie do rejestrów kredytowych (klient rejestru kredytowego).

– dopasowanie obowiązków banków i rejestrów kredytowych oraz podmiotów przetwarzających do wymogów odnoszących się do ryzyka naruszenia praw i wolności osób fizycznych, które może nieść przetwarzanie ich danych osobowych;
– ograniczanie ryzyka naruszenia praw i wolności osób fizycznych, które może nieść przetwarzanie danych osobowych, poprzez wskazanie obowiązków dla banków i rejestrów kredytowych oraz podmiotów przetwarzających dane osobowe w tym zakresie;
– ułatwienie klientom dokonania oceny, czy dany bank lub rejestr kredytowy stosuje odpowiednie zasady ochrony przetwarzanych danych osobowych;
– zwiększenie zaufania klientów do banków oraz rejestrów kredytowych, że ich dane osobowe są chronione na odpowiednim poziomie.

Należy przy tym zauważyć, iż wyżej zarysowane cele wprowadzenia Kodeksu stanowią kolejne bezpośrednie nawiązanie do charakterystyki instytucji kodeksu postępowania określonej na gruncie motywu 98 RODO i art. 40 ust. 1 RODO, w szczególności w obszarze wyjaśniania oraz dostosowania wymogów RODO do konkretnego sektora i związanej z nim specyfiki[39].

Główne elementy „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe"

Oprócz wprowadzenia, które zostało opisane już wcześniej, na Kodeks składa się osiem głównych części tematycznych podzielonych na szczegółowe rozdziały.

Pierwsza część Kodeksu (Część A) stanowi zbiór definicji i skrótów używanych na jego gruncie. Oprócz skrótów dotyczących aktów prawnych, na które powołuje się Kodeks, tak określony słowniczek obejmuje definicje: administratora, danych osobowych, profilowania, pseudonimizacji, zgody, organu nadzorczego, rejestru kredytowego, klienta oraz grupy. Z wyjątkiem trzech ostatnich wszystkie ww. definicje stanowią powtórzenie definicji zawartych w art. 4 RODO. Co istotne, w celu uniknięcia jakichkolwiek wątpliwości zawarte zostało wyraźne zastrzeżenie, iż inne pojęcia użyte w Kodeksie bez nadania im odrębnej definicji mają znaczenie, które zostało im nadane w przepisach RODO.

Kolejna część Kodeksu (Część B) odnosi się do trzech kluczowych zagadnień omawianych w odrębnych, dedykowanych im rozdziałach, tj.: (I) zasad dotyczących przetwarzania danych osobowych; (II) podstaw prawnych przetwarzania danych osobowych; (III) warunków pozyskiwania zgody na przetwarzanie danych osobowych. W ramach pierwszego z ww. rozdziałów Kodeks wymienia oraz opisuje podstawowe zasady dotyczące przetwarzania danych osobowych, tj.: zasadę zgodności z prawem, rzetelności i przejrzystości; zasadę ograniczenia celu przetwarzania; zasadę minimalizacji danych; zasadę prawidłowości; zasadę ograniczenia przechowywania; zasadę integralności i poufności, jak również zasadę rozliczalności. W drugim rozdziale zostają omówione podstawy prawne przetwarzania danych osobowych. W tym też względzie Kodeks wskazuje warunki, przy których spełnieniu bank lub rejestr kredytowy przetwarza dane osobowe. Podstawy prawne przetwarzania danych osobowych zawarte w Kodeksie są przy tym analogiczne do podstaw przetwarzania danych osobowych przewidzianych na gruncie art. 6 ust. 1 RODO. Trzeci rozdział omawia zaś warunki pozyskiwania zgody na przetwarzanie danych osobowych. Jak już zostało wcześniej nadmienione, na gruncie Kodeksu – tak jak w przypadku art. 4 pkt 11 RODO – przez zgodę osoby, której dane dotyczą, należy rozumieć dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. W tym też względzie Kodeks zawiera szczegółowe postanowienia określające m.in.: moment wyrażenia zgody; formę oraz sposoby sformułowania zapytań o zgodę; formę oraz sposoby sformułowania zgody; katalog przykładowych działań klienta, które można uznać za wyraźne działania wskazujące na wyrażenie przez niego zgody; przykłady sytuacji, w których jedna zgoda klienta może obejmować wiele podobnych celów; przykłady sytuacji, których nie należy uznawać za wyrażenie zgody przez klienta; szczegółowe przypadki, w których zgody klienta nie uważa się za wyrażoną świadomie lub dobrowolnie; postanowienia dotyczące przykładowych sposobów wycofania uprzednio wyrażonej zgody; powinności banku lub rejestru kredytowego związane ze zbieraniem zgody lub oświadczenia o wycofaniu zgody.

Następna część Kodeksu (Część C) poświęcona jest niezwykle istotnemu zagadnieniu praw osoby, której dane dotyczą. W tym też względzie Kodeks w szczegółowy, wszechstronny sposób określa zasady oraz sposób realizacji przez banki i rejestry kredytowe praw osób, których dane dotyczą, przy czym każde z omawianych praw zostało opisane w odrębnym, dedykowanym mu rozdziale. Co istotne, Kodeks określa zarówno zasady ogólne – wspólne dla wszystkich omawianych praw, jak i szczegółowe postanowienia dotyczące realizacji poszczególnych praw, uwzględniające ich specyfikę. W powyższym zakresie regulacje Kodeksu obejmują: obowiązek informacyjny; prawo dostępu do danych osoby, której dane dotyczą; prawo do sprostowania danych; prawo do usunięcia danych (prawo do bycia zapomnianym);

[39] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 819.

prawo do ograniczenia przetwarzania danych osobowych; obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania; prawo do przenoszenia danych (w tym: prawo do otrzymywania danych oraz prawo do żądania do przesłania danych innemu administratorowi); prawo sprzeciwu.

Kodeks zawiera również szczegółowe regulacje dotyczące przechowywania i usuwania danych osobowych (Część D), wychodząc z ogólnej zasady, iż dane osobowe klientów lub potencjalnych klientów nie mogą być przechowywane w formie umożliwiającej ich identyfikację przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. W tym też względzie Kodeks podkreśla m.in., iż po osiągnięciu zamierzonych (pierwotnych) celów przetwarzania, o których mowa wyżej, dane osobowe osób, których dane dotyczą, powinny zostać usunięte, chyba że ich dalsze przechowywanie znajduje podstawę prawną. Jako przykłady tak określonej podstawy prawnej Kodeks podaje ustawę z 29.9.1994 r. o rachunkowości, ustawę z 29.8.1997 r. – Ordynacja podatkowa[40], ustawę z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[41] czy też ustawę z 24.11.2017 r. o zmianie niektórych ustaw w celu przeciwdziałania wykorzystywaniu sektora finansowego do wyłudzeń skarbowych[42].

Jednym z najistotniejszych obszarów tematycznych regulowanych przez Kodeks jest instytucja profilowania oraz zautomatyzowanego przetwarzania danych osobowych osób fizycznych (Część E). W tym też względzie Kodeks zawiera zbiór zasad dotyczących procesu profilowania oraz zautomatyzowanego przetwarzania danych osobowych, wskazując, że profilowanie jest metodą przetwarzania danych osobowych, które może być oparte na różnych modelach oraz algorytmach. W szczególności Kodeks podkreśla, że profilowanie opiera się na odpowiednich matematycznych lub statystycznych procedurach profilowania, z zachowaniem środków technicznych i organizacyjnych zapewniających zmniejszenie ryzyka błędów w procedurach profilowania. Kodeks wyraża ponadto zasadę, iż do profilowania banki i rejestry kredytowe wykorzystują dane osobowe osoby, której dane dotyczą, i dane o jej zobowiązaniach (w tym historię kredytową klienta) w takim zakresie, w jakim przetwarzanie tych danych jest niezbędne i adekwatne do celu przetwarzania. Należy przy tym wskazać, że Kodeks zawiera niezwykle szeroki katalog przykładowych celów profilowania klientów przez banki oraz rejestry kredytowe – stanowi to również odzwierciedlenie informacyjnej funkcji Kodeksu, w ramach której klient będzie mógł poprzez treść Kodeksu zapoznać się z przykładami sytuacji, w których banki oraz rejestry kredytowe dokonują profilowania. W podobnym kontekście należy również odczytywać przewidziany w Kodeksie katalog przykładowych działań dotyczących procesu oceny zdolności i wiarygodności kredytowej klienta, w związku z którymi wykorzystywana jest ocena punktowa klienta lub inny profil udostępniony przez rejestr kredytowy czy też będący wynikiem profilowania przez bank zgodnie z modelami własnymi banku. W bezpośrednim nawiązaniu do wyżej zarysowanych zagadnień Kodeks zawiera również – w formie załączników – opis modelu oceny punktowej (scoringowego) wykorzystywanego w procesie zarządzania ryzykiem kredytowym (Załącznik Nr 3) oraz przykłady zautomatyzowanego przetwarzania danych (Załącznik Nr 6).

Kodeks odnosi się również do zagadnienia powierzenia przetwarzania danych osobowych w kontekście klauzul umów z dostawcami (Część F). Na gruncie Kodeksu przewidziane jest bowiem, iż banki jako administratorzy mogą stosować do umów zawieranych z podmiotami przetwarzającymi przykładowe zapisy wymienione w Załączniku Nr 5 do Kodeksu – z zastrzeżeniem, że w przypadku wydania przez Komisję Europejską lub organ nadzoru standardowych klauzul umownych mają one pierwszeństwo przed postanowieniami Kodeksu. Kodeks podkreśla przy tym, iż przewidziane w nim standardowe klauzule umowne mają charakter przykładowy i nie wyłączają prawa banku do zastosowania we własnych umowach z podmiotami przetwarzającymi dane odmiennych klauzul.

Kodeks określa również zasady dotyczące powiadomienia o naruszeniu ochrony danych osobowych (Część G). W tym względzie Kodeks zawiera postanowienia dotyczące zarówno sytuacji naruszenia ochrony danych osobowych podlegającego obowiązkowi zgłoszenia organowi nadzorczemu, jak i naruszenia ochrony danych osobowych podlegającego obowiązkowi zgłoszenia osobie, której dane dotyczą. Na gruncie Kodeksu przyjęto, że naruszenie ochrony danych osobowych w bankach i rejestrach kredytowych rozpatrywane jest jako zdarzenie występujące w ramach ryzyka operacyjnego, które należy rozumieć jako możliwość wystąpienia straty wynikającej z niedostosowania lub zawodności procesów wewnętrznych, ludzi i systemów lub ze zdarzeń zewnętrznych. Kodeks doprecyzowuje przy tym, iż naruszeniem ochrony danych osobowych jest naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w ramach prowadzonej przez administratora danych działalności. Co istotne, Kodeks zawiera m.in. przykłady sytuacji, które mogą prowadzić do naruszenia ochrony danych osobowych, jak również przykłady przypadków stanowiących naruszenie ochrony danych osobowych podlegające obowiązkowi zgłoszenia organowi nadzorczemu oraz przykłady przypadków stanowiących naruszenie ochrony danych osobowych podlegające obowiązkowi zgłoszenia osobie, której dane dotyczą. W powyższym kontekście warto również podkreślić, iż jednymi z załączników do Ko-

[40] T.j. Dz.U. z 2018 r. poz. 800 ze zm.
[41] Dz.U. poz. 723.
[42] Dz.U. poz. 2491 ze zm.

deksu są: wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie organu nadzorczego (Załącznik Nr 1), jak również wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie osoby, której dane dotyczą (Załącznik Nr 2).

Ostatnim obszarem regulowanym przez Kodeks jest zaś zagadnienie oceny skutków przetwarzania danych (Część H), w ramach którego Kodeks m.in. wskazuje przykłady sytuacji, kiedy banki i rejestry kredytowe powinny rozważyć przeprowadzenie oceny skutków dla ochrony danych osobowych.

Integralną częścią Kodeksu jest również sześć załączników, z których część została już opisana wcześniej. W tym też względzie należy wskazać, że Kodeks zawiera następujące Załączniki:

– Wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie organu nadzorczego (Załącznik Nr 1);
– Wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie osoby, której dane dotyczą (Załącznik Nr 2);
– Opis przykładowego modelu oceny punktowej (scoringowego) wykorzystywanego w procesie zarządzania ryzykiem kredytowym (Załącznik Nr 3);
– Zakresy informacji przekazywanych Klientowi (Załącznik Nr 4);
– Przykładowe postanowienia umów zawieranych z podmiotami przetwarzającymi (Załącznik Nr 5);
– Przykłady zautomatyzowanego przetwarzania danych (Załącznik Nr 6).

Podsumowanie

Kodeksy postępowania stanowią jedną z najważniejszych instytucji przewidzianych na gruncie przepisów RODO. Charakteryzowane jako instrument samoregulacyjny wspomagający oraz usprawniający proces wdrożenia przepisów RODO poprzez dostosowanie wymogów wskazanego rozporządzenia do specyfiki konkretnych sektorów gospodarki[43], kodeksy postępowania mogą stanowić istotne udogodnienie dla wielu kategorii administratorów oraz podmiotów przetwarzających. W tym też kontekście członkowie Związku Banków Polskich – świadomi wyzwań związanych ze skutecznym oraz prawidłowym wdrożeniem RODO – wraz z wejściem RODO rozpoczęli intensywne prace nad projektem kodeksu postępowania dla polskiego sektora bankowego. Efektem tychże prac przeprowadzanych na forum Związku Banków Polskich jest obecny projekt „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe", który – po przejściu procedury opiniowania oraz zatwierdzania określonej w art. 40 RODO – ma szansę stać się kluczowym instrumentem skutecznie oraz spójnie dostosowującym polski sektor bankowy do wymogów stawianych przez RODO.

[43] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 819.

Słowa kluczowe: RODO, kodeks postępowania, banki, ochrona danych osobowych.

Implementing GDPR in banks based on "The code of good practices in the scope of processing of personal data by banks and credit register"

The aim of the present study is to present the project "The code of good practices in the scope of processing of personal data by banks and credit register" (further referred to as: Code), developed by the Polish Bank Association, as an example of activities implementing regulation of the European Parliament and of the Council 2016/679 of 27.4.2016, in the matter of protection of natural persons in regard to processing of personal data and in the matter of free movement of such data and repealing the directive 95/46/EC (general data protection regulation) in Polish bank sector and its entities. In order to provide direct reference of the abovementioned issue to legislative context in the form of GDPR, discussing contents of the project Code will be preceded by a general characteristics of the institution of the code of conduct based on provisions of the regulation.

Keywords: GDPR, code of conduct, banks, personal data protection.