RODO w bankowości

Przewodnik

przygotowany przez Katarzynę Szewczuk Gontarz
z kancelarii Kruk i Wspólnicy.

CyberDefence 24

2018

RODO wywołało spore „zamieszanie” w zasadzie w każdej branży. Szczególnie odczuwalne jest jednak w takich dziedzinach jak bankowość czy sprzedaż wysyłkowa, w których dane są niezwykle cenne nie tylko ze względu na konieczność ich ochrony, ale także z uwagi na pozyskiwanie klientów.

W dniu 25 maja 2018 roku weszły w życie nowe przepisy dotyczące ochrony danych osobowych, tj.:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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, powszechnie znane jako „RODO”) oraz

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

Należy mieć na uwadze, że przepisy te należy stosować bezpośrednio, co oznacza, iż nie ma potrzeby przyjmowania tych regulacji w polskiej ustawie.

RODO wywołało spore „zamieszanie” w zasadzie w każdej branży, aczkolwiek wydaje się, że szczególnie odczuwalne jest w dziedzinach takich jak np. bankowość czy sprzedaż wysyłkowa, w których dane osobowe są niezwykle cenne nie tylko ze względu na konieczność ich ochrony, ale także z uwagi na pozyskiwanie klientów czy sprzedaż produktów itp. „Zamieszanie” związane z RODO wynika przede wszystkim z dość ogólnych zapisów i możliwości ich różnej interpretacji. Spore obawy budzą także wysokie kary za złamanie przepisów dotyczących ochrony danych osobowych. Poza tym, naturalnym jest, że nowe prawo, bez utartej ścieżki postępowania, rodzi wiele pytań i obaw.

Cel RODO

Aby zrozumieć, czemu ma służyć RODO, warto przywołać cel jakiemu służyło jego wprowadzenie. Otóż przepisy te wprowadzono **w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych, a w szczególności ich prawa do ochrony danych osobowych**. Wszelkie regulacje zawarte w RODO realizują więc ten cel.

Kto musi stosować RODO?

Przepisy RODO mają zastosowanie do wszystkich przedsiębiorców, bez względu na ich formę działalności (tj. spółka, jednoosobowa działalność gospodarcza) czy też wielkość (mikro-, mały, średni przedsiębiorca), jeżeli:

- ✓ przetwarzają dane osobowe osób fizycznych,
- ✓ prowadzą działalność na terytorium Unii Europejskiej.

Tak więc, przepisy RODO dotyczą szczególnie podmiotów z sektora bankowości, albowiem banki niewątpliwie zajmują się one przetwarzaniem danych osobowych (o czym mowa poniżej).

PODSTAWOWE POJĘCIA NA GRUNCIE RODO

W celu przybliżenia regulacji RODO, konieczne jest wyjaśnienie podstawowych pojęć w nim funkcjonujących:

Dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą")

- Osoba zidentyfikowana to taka, której tożsamość jest znana, np. klient banku, który podał swoje dane osobowe przy zakładaniu rachunku bankowego, pracownik zatrudniony w banku, którego dane osobowe są znane pracodawcy (bankowi), itd.

- Osoba możliwa do zidentyfikowania to taka którą można zidentyfikować w szczególności na podstawie identyfikatora, takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy (np. adres IP, identyfikatory plików cookie) lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

- W przypadku osoby możliwej do zidentyfikowania, identyfikacja nie następuje wprost, lecz z wykorzystaniem różnych danych, którymi dysponujemy, np. imieniem i miejscem zamieszkania. Jeżeli dane te będziemy mogli powiązać z konkretną osobą, to będą one danymi osobowymi

- Warto mieć na uwadze, że poniższe dane, które często są przekazywane przez klientów banków, bądź są w posiadaniu banku stanowią dane osobowe według RODO:

- ✓ imię i nazwisko,
- ✓ numer PESEL/NIP,
- ✓ adres zamieszkania,
- ✓ numer telefonu (dysponując numerem telefonu, możemy w bardzo prosty ustalić tożsamość danej osoby),
- ✓ adres e-mail, o ile na jego podstawie jesteśmy w stanie ustalić tożsamość danej osoby (np. w adresie e-mail użyto imienia i nazwiska),
- ✓ data urodzenia,
- ✓ dane dotyczące transakcji dokonywanej przez klienta banku (tj. wpłaty, wypłaty, przelewy),
- ✓ dane dotyczące stanu cywilnego itd.

Powyższe dane to jedynie część przykładów, które mogą stanowić dane osobowe w rozumieniu RODO.

Przetwarzanie danych osobowych to pojęcie bardzo ogólne, które oznacza wszelkie operacje na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
Przykłady:

- ✓ przechowywanie danych osobowych klientów banków, takich jak: imię i nazwisko, adres zamieszkania, numer PESEL/NIP, numer telefonu, itp.,
- ✓ tworzenie baz danych klientów banku,
- ✓ zbieranie danych osobowych klienta w celu przedstawienia oferty banku,
- ✓ weryfikacja klienta banku,
- ✓ ocena zdolności kredytowej klienta banku,
- ✓ analiza ryzyka kredytowego w związku z udzielanym kredytem
- ✓ odbiór korespondencji,
- ✓ windykacja należności banku

Administrator danych - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Podmiot przetwarzający to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

- ✓ W bankach dane osobowe są w szczególności przetwarzane przez pracowników (to oni wykonują konkretne operacje na danych osobowych),
- ✓ Pracownicy banku, aby móc przetwarzać dane osobowe zgodnie z prawem, powinni dysponować upoważnieniem do przetwarzania danych osobowych.

Odbiorca to osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

- Wyjątek: Organy publiczne, jeżeli otrzymują dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, np. przekazywanie przez banki sądom informacji stanowiących tajemnicę bankową w trybie art. 105 prawa bankowego.
- W bankowości dane osobowe najczęściej są ujawniane są następującym podmiotom, które należy uznać za odbiorców:

  - ✓ podmioty uczestniczące w procesach niezbędnych do wykonywania zawartych z osobą, której dane dotyczą umów, (np. Krajowa Izba Rozliczeniowa S.A., VISA, Mastercard, First Data Polska S.A.),
  - ✓ biura informacji gospodarczej, działające na podstawie przepisów ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, na podstawie przepisów tej ustawy (np. Krajowy Rejestr Długów S.A. z siedzibą we Wrocławiu).

PRZETWARZANIE DANYCH OSOBOWYCH W BANKOWOŚCI – O CZYM WARTO PAMIĘTAĆ?

1. Przetwarzanie danych osobowych – warunki dopuszczalności:

- **zgoda** osoby, której dane dotyczą na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- **brak zgody**, jeżeli:

  - ✓ przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
  - ✓ przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

- ✓ przetwarzanie jest niezbędne do ochrony prawnie uzasadnionych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (np. wytoczenie powództwa przeciwko klientowi, który zalega ze spłatą kredytu).

2. Zgoda na przetwarzanie danych osobowych, podobnie jak w uprzednio obowiązujących przepisach prawa musi się charakteryzować pewnymi cechami, aby została uznana za wyrażoną w sposób prawidłowy. Zgoda ta powinna być:

- ✓ **dobrowolna** – oznacza to, że dana osoba ma rzeczywistą możliwość wyboru, a odmowa wyrażenia zgody nie będzie się dla niej wiązała z negatywnymi konsekwencjami,
- ✓ **jednoznaczna** – czyli fakt wyrażenia zgody nie powinien budzić wątpliwości. Wyrażenie zgody następuje w formie oświadczenia woli lub wyraźnego działania potwierdzającego. Należy mieć na uwadze, że milczenie nie może zostać uznane za wyrażenie zgody.
- ✓ **świadoma** – oznacza świadomość konsekwencji wyrażenia zgody i praw z tym związanych. Przyjmuje się, że aby zgodę uznać za świadomą należy w szczególności przekazać informacje dotyczące administratora danych osobowych, celu i zakresu przetwarzania danych osobowych oraz możliwości wycofania zgody.
- ✓ **konkretna** – oznacza to, że ze zgody musi wynikać cel w jakim dane osobowe będą przetwarzane. Jeżeli dane osobowe będą przetwarzane w kilku celach, zgoda powinna dotyczyć każdego z nich.

Istotne jest, że zgoda musi zostać udzielona przed rozpoczęciem przetwarzania danych osobowych. Należy mieć na uwadze, że zgody uzyskane przez banki w oparciu o przepisy uprzednio obowiązującej ustawy o ochronie danych osobowych, zachowują swoją aktualność, jeżeli cel przetwarzania się nie zmienił, a zgoda odpowiada wymogom RODO. Wówczas nie ma konieczności uzyskiwania nowych zgód. Jeżeli natomiast cel przetwarzania danych uległ zmianie, niezbędne jest uzyskanie nowej zgody dotyczącej zmienionych, nowych celów i spełniającej wymogi RODO.

3. Warunki wyrażenia zgody

Po pierwsze, należy mieć na uwadze, że w przypadku przetwarzania danych osobowych na podstawie zgody, to **administrator danych osobowych musi wykazać fakt udzielenia zgody**. W związku z tym warto zadbać o to, aby zgody były udzielane w formie pisemnej lub innej formie pozwalającej na udokumentowanie faktu jej udzielenia (np. forma elektroniczna; podczas nagrywanej rozmowy telefonicznej, przy czym należy uprzedzić o fakcie nagrywania rozmowy). Wszelkie dokumenty czy też inne nośniki informacji potwierdzające fakt udzielenia zgody należy przechowywać i udostępnić np. na żądanie organu nadzoru. Jeżeli

bowiem administrator danych osobowych nie będzie w stanie wykazać, że zgoda została udzielona, poniesie odpowiedzialność za nielegalne przetwarzanie danych osobowych.

Po drugie, w przypadku wyrażenia zgody w pisemnym oświadczeniu, dotyczących również innych kwestii, zapytanie o zgodę musi wyraźnie odróżniać się od pozostałych kwestii. Ponadto, musi być zrozumiałe, w łatwo dostępnej formie oraz sporządzone jasnym i prostym językiem.

Po trzecie, **zgoda na przetwarzanie danych osobowych może zostać w każdym czasie wycofana**, o czym należy poinformować daną osobę jeszcze przed udzieleniem zgody. Wycofanie zgody nie może wiązać się z żadnymi niedogodnościami i musi być równie łatwe co jej wyrażenie.

Po czwarte, oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

4. Zasady przetwarzania danych osobowych

- **zasada zgodności z prawem, rzetelności i przejrzystości,**
- **zasada ograniczenia celu** – dane mogą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach. Zasada ta jest powiązana z obowiązkiem informacyjnym, która nakazuje informowanie osoby fizycznej m.in. o celu przetwarzania danych. Nie można dalej przetwarzać danych w sposób niezgodny z tymi celami,
- **zasada minimalizacji danych** – zakres przetwarzanych danych powinien być adekwatny, stosowny oraz ograniczony do osiągnięcia celu w jakim są przetwarzane,
- **zasada prawidłowości** – dane osobowe muszą być zgodne z rzeczywistością, co wiąże się z koniecznością ich uaktualnienia w razie potrzeby. Jeżeli dane okażą się nieprawidłowe należy je usunąć lub sprostować,
- **zasada ograniczenia przechowywania** – dane osobowe mogą być przechowywane w formie umożliwiającej identyfikację osoby przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane,
- **zasada integralności i poufności** – zasada ta wiąże się z koniecznością zapewnienia bezpieczeństwa danych osobowych. Przetwarzanie danych osobowych musi więc następować w sposób zapewniający ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Bank jako administrator danych osobowych w rozumieniu RODO, jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie.

5. Niedopuszczalność przetwarzania szczególnych kategorii danych osobowych

Co do zasady zabronione jest przetwarzanie danych osobowych ujawniających: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

JAKIE SĄ PRAWA KLIENTA BANKU W ZWIĄZKU Z PRZETWARZANIEM DANYCH OSOBOWYCH?

Jak wskazano powyżej zasadniczym celem RODO jest wzmocnienie praw osób fizycznych w związku z przetwarzaniem ich danych osobowych. Nie powinno zatem dziwić, że przepisy RODO wprowadzają szereg praw osób fizycznych, których dane są przetwarzane. Część z nich stanowi powtórzenie dotychczas przysługujących praw, a pozostałe stanowią zupełnie nowe rozwiązania. Obowiązek zapewnienia realizacji tych uprawnień spoczywa na podmiocie przetwarzającym dane osobowe, tj. banku.

1. Prawo dostępu do danych - na żądanie osoby, której dane dotyczą, administrator danych osobowych (bank) zobowiązany jest poinformować ją, czy jej dane są przetwarzane, a jeżeli tak, musi jej zapewnić dostęp do tych danych oraz udzielić następujących informacji: jakie dane, w jakim celu i na jakiej podstawie prawnej są przetwarzane; jakie są kategorie odnośnych danych osobowych; kto jest odbiorcą danych osobowych, jaki jest planowany okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okres, o prawie do żądania od administratora sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby; o prawie wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego.

2. Prawo do sprostowania danych - na żądanie osoby, której dane dotyczą, administrator danych osobowych (bank) zobowiązany jest niezwłocznie sprostować te dane, jeżeli są nieprawidłowe lub je uzupełnić w przypadku ich niekompletności.

3. Prawo do bycia zapomnianym - polega na skierowaniu do administratora danych osobowych (banku) przez osobę, której dane dotyczą żądania usunięcia jej danych osobowych, jeżeli:

- ✓ nie ma podstawy prawnej do przetwarzania danych osobowych (np. cofnięcie zgody, a nie ma innej podstawy do przetwarzania),
- ✓ dane osobowe nie są już potrzebne do celów, w których zostały one zgromadzone;

- ✓ dane osobowe były przetwarzane niezgodnie z prawem,
- ✓ osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania,
- ✓ dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego,
- ✓ dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

Usunięcie danych osobowych powinno nastąpić bez zbędnej zwłoki. Podkreślić należy, że RODO przewiduje również przypadki, w których prawo do bycia zapomnianym nie znajduje zastosowania (np. ustalenie, dochodzenie roszczeń przez bank wobec klientów, którzy nieterminowo spłacają kredyt).

4. Prawo do ograniczenia przetwarzania danych osobowych – przysługuje osobie, której dane dotyczą, jeżeli:

- ✓ zgromadzone dane są nieprawidłowe (na czas pozwalający na sprawdzenie prawidłowości danych),
- ✓ przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- ✓ administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- ✓ został wniesiony sprzeciw wobec przetwarzania danych osobowych.

5. Prawo do przenoszenia danych – czyli prawo do otrzymania przez osobę, której dane dotyczą wszystkich danych, które administrator danych (bank) zgromadził na jej temat. Dane powinny zostać przekazane w sposób umożliwiający ich odczytanie. Po uzyskaniu tych danych, dana osoba może je przekazać inne administratorowi. Prawo do przysługuje, jeżeli:

- ✓ przetwarzanie danych odbywa się na podstawie zgody lub w celu wykonania umowy,
- ✓ przetwarzanie danych odbywa się w sposób zautomatyzowany.

6. Prawo do sprzeciwu oraz do niepodleganiu decyzji opartych na zautomatyzowanym przetwarzaniu

- **prawo do wniesienia sprzeciwu** – każda osoba, której dane dotyczą może w dowolnym czasie wnieść sprzeciw:
  - ✓ podstawa wniesienia sprzeciwu: przyczyny związane ze szczególną sytuacją osoby,
  - ✓ w przypadku wniesienia sprzeciwu, administrator danych osobowych nie może przetwarzać danych osobowych tej osoby, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów,

praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń,

- ✓ w przypadku przetwarzania danych osobowych w celach marketingowych, osoba, której dane dotyczą może w dowolnym czasie wnieść sprzeciw wobec przetwarzania danych w tym celu. **Wniesienie sprzeciwu, oznacza, że administrator danych osobowych nie może przetwarzać danych osobowych w celach marketingowych**.

- **prawo do niepodlegania decyzji opartych na zautomatyzowanym przetwarzaniu, w tym profilowaniu, jeżeli wywołuje wobec osoby której dane dotyczą skutki prawne lub w podobny sposób istotnie na nią wpływa** (np. automatyczna decyzja kredytowa)

  - ✓ **Wyjątki:** 1) jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; 2) jest to dozwolone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; 3) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W wyżej wymienionych przypadkach **prawo do niepodlegania decyzji opartych na zautomatyzowanym przetwarzaniu, w tym profilowaniu nie przysługuje**.

ZBIERANIE DANYCH OSOBOWYCH W BANKOWOŚCI – CO WARTO WIEDZIEĆ?

Zbieranie danych osobowych to jedna z form przetwarzania danych osobowych. Proces ten jest nieodłączny w bankowości, gdzie pracownicy w zasadzie każdego dnia pozyskują dane osobowe od osób fizycznych (np. przy zawarciu umowy o prowadzenie rachunku bankowego, złożenie wniosku o przyznanie kredytu). Już na etapie zbierania danych osobowych, administrator danych osobowych musi pamiętać o spełnieniu obowiązków nałożonych na niego przez RODO.

Podstawowym obowiązkiem związanym ze zbieraniem danych osobowych jest **obowiązek informacyjny**. W ramach tego obowiązku, należy przekazać następujące informacje:

- ✓ tożsamość i dane kontaktowe administratora,
- ✓ dane kontaktowe inspektora ochrony danych, gdy ma to zastosowanie (jak wskazano poniżej, powołanie inspektora ochrony danych w banku jest konieczne),
- ✓ cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
- ✓ prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią, jeżeli przetwarzanie danych osobowych następuje w tym celu,
- ✓ informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,

- ✓ okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- ✓ informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- ✓ jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- ✓ informacje o prawie wniesienia skargi do organu nadzorczego;
- ✓ informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- ✓ informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Pamiętać należy, że obowiązek informacyjny będzie spoczywał na banku niezależnie od sposobu zbierania informacji, tj. osobiście od klienta, telefonicznie, itp. Należy go również spełnić w sytuacji, gdy informacje zostały uzyskane w inny sposób niż od osoby, której dotyczą (np. z Internetu, CEIDG).

Informacje wskazane powyżej jak również dalsza komunikacja z osobą, której dane dotyczą musi następować w zwięzłej, zrozumiałej formie oraz jasnym i prostym językiem. Ma to służyć wyeliminowaniu jakichkolwiek niejasności w zakresie przetwarzania danych osobowych.

Zbierając dane osobowe, należy również mieć na uwadze zasady przetwarzania danych osobowych. Oznacza to w szczególności, że:

- ✓ dopuszczalne jest zbieranie tylko tych danych, które są niezbędne do osiągnięcia celu przetwarzania
- ✓ należy mieć podstawę prawną do przetwarzania danych osobowych (przypomnieć należy, że zbieranie danych osobowych to jedna z operacji dokonywanych w ramach przetwarzania danych osobowych), np. zgoda.

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W BANKU

Przepisy RODO to nie tylko zasady przetwarzania danych osobowych czy też prawa osób, których dane dotyczą, ale także bezpieczeństwo danych osobowych. Zapewnienie bezpieczeństwa danych osobowych zgodnie z RODO to niemałe wyzwanie dla sporej ilości przedsiębiorców. Wydaje się jednak, że banki czeka szczególnie trudne zadanie, albowiem znaczna część ich klientów korzysta z bankowości elektronicznej czy też aplikacji mobilnych. Ponadto, dane osobowe klientów banków, do których mają dostęp jego pracownicy są w znacznej części zapisywane na serwerach komputerowych czy też komputerach. W związku z tym banki są szczególnie mocno narażone na cyberataki, zwłaszcza że dane przez nie gromadzone są niezwykle cenne dla przestępców. Bank zaś jako administrator danych osobowych, musi podjąć wszelkie środki, aby takim atakom zapobiegać. Podkreślić jednak należy, że bezpieczeństwo danych osobowych nie odnosi się tylko do danych gromadzonych w systemach informatycznych, ale także do danych gromadzonych w formie papierowej.

Zapewnienie należytego bezpieczeństwa danych osobowych stosownie do przepisów RODO jest o tyle trudne, że RODO nie nakazuje stosowania przez administratora danych osobowych żadnych konkretnych środków zabezpieczenia danych osobowych. Określa jedynie **przykładowe środki bezpieczeństwa**, tj.:

- ✓ pseudonimizacja (*czyli przetwarzanie danych osobowych w taki sposób, aby nie było możliwe zidentyfikowanie, do kogo one należą*) i szyfrowanie danych osobowych;
- ✓ zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- ✓ zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- ✓ regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Wybór odpowiednich środków bezpieczeństwa został pozostawiony administratorowi, który przy wyborze ma się kierować stanem wiedzy technicznej, kosztem wdrażania oraz charakterem, zakresem, kontekstem i celami przetwarzania oraz ryzykiem naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Istotne jest, w przypadku naruszenia bezpieczeństwa danych osobowych, pomimo zastosowanych środków bezpieczeństwa, administrator danych osobowych będzie musiał wykazać, że zrobił wszystko, aby do takiej sytuacji nie doszło.

Przepisy RODO dzielą **środki bezpieczeństwa** na:

- **techniczne**, np.:
  - ✓ szyfrowanie danych osobowych,
  - ✓ szyfrowanie połączeń,
  - ✓ kody zabezpieczające do logowania,
  - ✓ stosowanie programów chroniących przed wirusami,
  - ✓ mechanizmy wymuszające zmianę haseł do komputerów, programów komputerowych,
  - ✓ dostęp do komputerów, w których gromadzone są dane po uprzednim zalogowaniu z wykorzystaniem identyfikatora i hasła,
  - ✓ wykorzystywanie systemu firewall,
  - ✓ przechowywanie danych osobowych w formie papierowej w zamkniętych pomieszczeniach zabezpieczonych przed skutkami pożaru, itd.
- **organizacyjne**, np.:
  - ✓ przeszkolenie pracowników z zakresu ochrony danych osobowych,
  - ✓ udzielenie pracownikom upoważnień do przetwarzania danych osobowych (tylko pracownicy dysponujący takim upoważnieniem mogą przetwarzać dane osobowe),
  - ✓ prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych
  - ✓ powołanie inspektora ochrony danych osobowych (konieczne w banku, albowiem po pierwsze przetwarzanie danych osobowych jest związane z główną działalnością banku, a po drugie przetwarzanie danych osobowych odbywa się dużą skalę),
  - ✓ opracowanie polityki bezpieczeństwa, itd.

Podkreślić należy, że wskazany powyżej katalog środków bezpieczeństwa ma **charakter przykładowy**, a wybór odpowiednich należy do administratora. Nie można bowiem stworzyć zamkniętego katalogu środków bezpieczeństwa adekwatnego dla każdego przedsiębiorcy, każdego banku. Aby środki bezpieczeństwa były skuteczne muszą być indywidualnie dopasowane do potrzeb przedsiębiorcy, skali jego działalności, zakresu przetwarzania danych osobowych, itd. Aby zastosować właściwe środki bezpieczeństwa należy przeprowadzić analizę ryzyka, czyli określić jakie są zagrożenia dla danych osobowych oraz prawdopodobieństwo ich wystąpienia.

Niezależnie od podejmowania środków bezpieczeństwa, za ważne aspekty bezpieczeństwa danych osobowych należy uznać:

- **prowadzenie rejestru czynności przetwarzania** – do prowadzenia rejestru zobowiązany jest bank jako administrator danych osobowych. Rejestr powinien być prowadzony w formie pisemnej. Rejestr powinien zawierać następujące informacje:
  - ✓ imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
  - ✓ cele przetwarzania;
  - ✓ opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
  - ✓ kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
  - ✓ jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
  - ✓ jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
- **zgłaszanie naruszeń ochrony danych osobowych Prezesa Urzędu Ochrony Danych Osobowych** – zgłoszenia dokonuje bank jako administrator danych osobowych, jeżeli dojdzie do naruszenia ochrony danych osobowych chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenia należy dokonać bez zbędnej zwłoki, w miarę możliwości nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia. Jeżeli zgłoszenie nastąpi po upływie tego terminu, należy podać przyczyny opóźnienia. Zgłoszenie musi zawierać co najmniej:

  - ✓ charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
  - ✓ imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - ✓ możliwe konsekwencje naruszenia ochrony danych osobowych;
  - ✓ środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
  - **zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych** – zawiadomienie powinno być dokonane jasnym i prostym językiem, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W zawiadomieniu należy opisać charakter naruszenia; imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; możliwe konsekwencje naruszenia ochrony danych osobowych; środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych. **Nie ma obowiązku zawiadomienia,** jeżeli:
    - ✓ w stosunku do danych, których dotyczy naruszenie, bank wdrożył odpowiednie środki ochrony, a w szczególności szyfrowanie uniemożliwiające odczyt danych,

- ✓ bank zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- ✓ wiązałoby się to z niewspółmiernym wysiłkiem (wówczas wystarczający jest np. publiczny komunikat, w którym powiadamia się o naruszeniu).