UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

1 lipca 2019 r.

Komunikat Urzędu Komisji Nadzoru Finansowego w sprawie zwolnienia z tzw. opcji fallback

Rozporządzenie Delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (RTS) przewiduje m.in. posiadanie przez dostawcę usług płatniczych prowadzącego rachunek (*Account Servicing Payment Service Provider* – ASPSP), który oferuje płatnikowi rachunek płatniczy dostępny za pośrednictwem Internetu, specjalnego interfejsu dostępowego (*Applicaton Programming Interface* – API) oraz reguluje zasady działania tego interfejsu i wymagania z nim związane. API ma umożliwiać świadczenie usług płatniczych przez tzw. TPP (*Third Party Providers*), tj. dostawców świadczących usługę inicjowania płatności (*Payment Initiation Service Providers* – PISP), usługę dostępu do informacji o rachunku (*Account Information Service Providers* – AISP) oraz wydawców instrumentów płatniczych opartych na karcie świadczących usługę potwierdzania dostępności środków na rachunku (*Card-Based Payment Instrument Issuers* – CBPII).

Zgodnie z art. 33 ust. 4 RTS, w ramach mechanizmów awaryjnych mających zastosowanie w sytuacji, gdy API nie działa zgodnie z wymogami RTS, bądź w przypadku nieplanowanej niedostępności interfejsu lub awarii systemów, ASPSP ma obowiązek umożliwić TPP – do momentu przywrócenia poziomu dostępności i efektywności API – korzystanie z interfejsów udostępnionych użytkownikom usług płatniczych na potrzeby uwierzytelnienia i komunikacji z ASPSP. Jest to tzw. „opcja fallback".

W myśl art. 33 ust. 6 RTS Komisja Nadzoru Finansowego (KNF) może zwolnić ASPSP z obowiązku posiadania opcji fallback, jeżeli spełnione zostały wszystkie następujące warunki:

1) stosowane API spełnia wszystkie określone w art. 32 RTS obowiązki dotyczące specjalnych interfejsów;
2) API został opracowany i przetestowany, zgodnie z art. 30 ust. 5 RTS, w sposób zadowalający TPP;
3) od co najmniej trzech miesięcy API jest powszechnie stosowany w celu świadczenia usług płatniczych przez TPP;
4) wszelkie problemy związane z API rozwiązano bez zbędnej zwłoki.

Szczegółowe zasady stosowania art. 33 ust. 6 RTS zarówno przez właściwe organy nadzoru, jak i dostawców usług płatniczych zostały określone w wydanych 4 grudnia 2018 r. przez Europejski Urząd Nadzoru Bankowego *Wytycznych w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389* (link: EBA/GL/2018/07).

Zwolnienie przez KNF z opcji fallback następować będzie w drodze decyzji administracyjnej wydanej indywidualnie dla każdego podmiotu po przeprowadzeniu postępowania administracyjnego, na wniosek zainteresowanego ASPSP spełniającego wymagania, o których mowa w art. 33 ust. 6 RTS. W tym kontekście należy zwrócić uwagę na dyspozycję art. 38 ust. 2 i 3 RTS, zgodnie z którym RTS (za wyjątkiem art. 30 ust. 3 i 5, które mają zastosowanie od 14 marca 2019 r.) stosuje się od 14 września 2019 r. W świetle przepisów prawa administracyjnego oznacza to, że wniosek o wszczęcie postępowania administracyjnego w sprawie wydania decyzji zwalniającej z obowiązku posiadania opcji fallback, może być skutecznie złożony dopiero po 13 września 2019 r. Z tych względów, decyzja może być wydana przez KNF dopiero po tym terminie.

Uwzględniając cel regulacji art. 33 ust. 6 RTS, jakim jest przede wszystkim zwolnienie ASPSP, którego API spełnia określone w tym przepisie warunki, z obowiązku tworzenia, wdrażania i utrzymywania opcji fallback, KNF informuje, że sprawdzenie spełniania tych warunków będzie mogło być dokonane w toku bieżącego nadzoru, jeszcze przed złożeniem wniosku o zwolnienie z opcji fallback i wydaniem przez KNF decyzji w tym zakresie. Sprawdzenie to powinno umożliwić ASPSP zainteresowanemu zwolnieniem z opcji fallback dokonanie oceny zasadności posiadania tych rozwiązań na dzień rozpoczęcia stosowania RTS i podjęcia decyzji co do ich przygotowania i wdrożenia. Oceniając w tym kontekście zgodność działalności ASPSP z przepisami RTS, niezależnie od ostatecznego rozstrzygnięcia w przedmiocie zwolnienia z opcji fallback, KNF będzie brać pod uwagę ustalenia poczynione w toku bieżącego nadzoru. Podkreślić należy, że nawet w przypadku ostatecznego zwolnienia zainteresowanego ASPSP z opcji fallback, ryzyko związane z nawet przejściowym niewypełnieniem obowiązku jej posiadania po 13 września 2019 r. i w związku z tym uniemożliwieniem TPP świadczenia jego usług obciążać będzie obowiązany ASPSP.

ASPSP, którzy nie będą zainteresowani zwolnieniem z opcji fallback lub nie będą w stanie spełnić wymogów dla takiego zwolnienia, powinni utworzyć, wdrożyć i utrzymywać mechanizm awaryjny. Jak wskazano wyżej, RTS wymaga, by w ramach opcji fallback ASPSP umożliwiał TPP korzystanie z interfejsów udostępnionych użytkownikom usług płatniczych na potrzeby uwierzytelnienia i komunikacji z ASPSP. Takie sformułowanie normy rozporządzenia wskazuje, że w przypadku zastosowania opcji fallback, TPP może uzyskać dostęp do danych identyfikujących i uwierzytelniających użytkownika (login, hasło) na potrzeby komunikacji elektronicznej z ASPSP. Stosowanie opcji fallback powinno w związku z tym uwzględniać w szczególności następujące zasady:

- Zapewnienie, aby TPP korzystający z opcji fallback był należycie zidentyfikowany i uwierzytelniony stosownym certyfikatem elektronicznym.
- Dostęp TPP do danych użytkownika i informacji o jego produktach przy zastosowaniu opcji fallback powinien być taki sam jak w przypadku normalnej komunikacji poprzez API.
- Jeżeli w wyniku zastosowania opcji fallback doszło do ujawnienia jakimkolwiek podmiotom trzecim, w tym TPP, danych uwierzytelniających użytkownika (wielorazowego hasła dostępowego), dane te należy traktować jako skompromitowane – stosownie

do odpowiednich procedur ASPSP dotyczących bezpieczeństwa. Następstwem tego powinno być w szczególności wymuszenie zmiany tych danych przy próbie następnego logowania przez użytkownika oraz przekazanie użytkownikowi niezbędnych informacji i wyjaśnień.

- ASPSP powinien oceniać i monitorować ryzyko ujawniania danych uwierzytelniających użytkownika podmiotom trzecim. Jeżeli w szczególności na podstawie liczby zapytań kierowanych przez TPP do API, analizy awaryjności API lub częstotliwości stosowania opcji fallback, ryzyko to jest oceniane jako wysokie, ASPSP powinien dążyć do jego ograniczenia, w szczególności poprzez wdrażanie rozwiązań w zakresie mechanizmów awaryjnych, wyłączających możliwość ujawniania danych uwierzytelniających użytkownika.