Deloitte.

PSD2: Praktické pokyny ke konečnému znění regulatorních technických standardů pro silné ověření klienta (RTS on SCA)

11. prosince 2017

Evropská komise vydala na konci listopadu konečné znění regulatorních technických standardů (RTS) upravujících silné ověření zákazníka. Tím bylo ukončeno období nejistoty, během nějž banky i nezávislí poskytovatelé platebních služeb (TPP) připravovali své systémy, aniž by v podstatě věděli, jak bude finální úprava vypadat.

Konečné znění regulatorních technických standardů přináší oproti předchozím návrhům několik významných změn, přičemž však některé klíčové otázky zůstávají i nadále nedořešené.

Konečné stanovisko k problematice tzv. „screen scrapingu"

Podle finálního znění RTS nejsou dedikovaná rozhraní pro programování aplikací (API) jediným možným způsobem komunikace mezi bankami a nezávislými poskytovateli platebních služeb. Poskytovatel, který vede platební účet (banka) má možnost určit, komu bude povolen přístup k účtům prostřednictvím stejných rozhraní, která používá pro své zákazníky. Tato rozhraní však musí nezávislým poskytovatelům platebních služeb umožnit, aby se bance identifikovali. Tradiční „screen scraping" (aniž by byl nezávislý poskytovatel platebních služeb identifikován) bude zakázán ve chvíli, kdy RTS vstoupí v platnost.

Hlavní změny:

- Konečný návrh obsahuje detailnější podmínky pro dedikovaná rozhraní (API), jako např. transparentní klíčové ukazatele výkonnosti (KPI) a cílové úrovně služeb (SLA). Rovněž vyžaduje, aby banky nechaly u všech komunikačních rozhraní provést zátěžové testy, které budou vykonány ostatními subjekty na trhu platebních služeb a orgánem dohledu. Nejpozději šest měsíců před datem účinnosti RTS budou muset banky zveřejnit technické specifikace svých rozhraní a zpřístupnit testovací zařízení všem poskytovatelům platebních služeb, kteří požádali o příslušné oprávnění.
- Je zaveden nový záložní mechanismus – pokud dedikované rozhraní nefunguje podle standardů, nezávislí poskytovatelé platebních služeb budou mít právo na přístup k účtům prostřednictvím zákaznického rozhraní. To v podstatě znamená, že kromě rozhraní pro programování aplikací budou banky muset připravit taková zákaznická rozhraní, která budou v souladu s RTS a směrnicí PSD2, aby nezávislým poskytovatelům platebních služeb umožnily se prostřednictvím takového rozhraní identifikovat.

Hlavní nedořešené otázky:

- Stále visí otazník nad tím, zda banky mají právo sdílet prémiová data či právo zpracovávat údaje o platbách pro jiné účely, než jsou služby informování o účtu, přičemž v obou případech je třeba získat souhlas uživatele. Přestože nařízení o ochraně osobních údajů (GDPR) obecně uvádí, že údaje lze zpracovat se souhlasem uživatele, jak směrnice PSD2, tak regulatorní technické standardy stanoví, že banky by měly sdílet pouze ty údaje, které jsou nezbytné pro poskytování služeb informování o účtu, a že nezávislí poskytovatelé platebních služeb by neměli zpracovávat údaje o platbách pro jiné účely. Věříme však, že převáží první uvedený výklad, tj. že se souhlasem uživatele bude možné zpracovávat údaje i pro jiné účely. Přestože nezávislí poskytovatelé platebních služeb a banky jsou pod dohledem vnitrostátních orgánů dohledu, banky a nezávislí poskytovatelé platebních služeb by měli být schopni příslušným orgánům dohledu prokázat, že jejich obchodní plán je v souladu s právními požadavky.
- Koncept „explicitního souhlasu" ve smyslu směrnice PSD2 je i nadále nejasný (např. měl by se souhlas vztahovat na konkrétní platební účty nebo je postačující, aby se vztahoval obecně na všechny platební účty, které jsou u dané banky vedeny?). Kromě požadavků RTS by se měl získat souhlas v souladu s požadavky nařízení GDPR (jasné souhlasné jednání, souhlas získaný pro každý účel, souhlas je informovaný a jednoznačný).
- Regulatorních technické standardy obnovu uživatelského souhlasu stále neupravují. Přestože je diskutabilní, zda obnovení silného ověření klienta (SCA) lze při nedostatku informací poskytnutých

Deloitte.

uživateli považovat za obnovení souhlasu, požadavky na ochranu osobních údajů týkající se obnovení souhlasu by měly být důkladně přezkoumány během navrhování komunikační platformy pro nezávislé poskytovatele platebních služeb.

- RTS neobjasňují, zda se na banky vztahuje povinnost ověřit existenci souhlasu, jakož i podmínky, za nichž byl souhlas uživatele vyjádřen. Vnitrostátní orgány se mohou v této souvislosti chopit iniciativy a poskytnout pokyny, avšak nekonzistentní přístup napříč Evropskou unií může vést k fragmentaci trhu. V každém případě, přestože převod osobních údajů nezávislým poskytovatelům platebních služeb se chápe jako zpracování údajů podle nařízení GDPR a rovněž vyjadřuje právo na přenositelnost údajů, banky budou muset zajistit, aby byl takový převod v souladu s požadavky na ochranu dat, a rovněž by měly zavést ochranná opatření k zajištění toho, aby jednaly výhradně jménem uživatele. S ohledem na vysoké pokuty, které nařízení GDPR zavádí, se důrazně doporučuje, aby národní úřady pro ochranu osobních údajů vydaly patřičné pokyny.

Přechodné období:

Evropská komise se rovněž vyjádřila k přechodnému období (mezi 13. lednem 2018 a datem účinnosti RTS). Vyjádření Komise naznačují, že tradiční „screen scraping" bude v přechodném období povolen. Avšak explicitní stanovisko k této problematice Komise neposkytla. Interpretace národních orgánů dohledu se proto může lišit, což se projeví v nadcházejících měsících.

Česká národní banka (spolu s Ministerstvem Financí ČR) již stanovisko k některým otázkám přechodného období vydala[1)]. V tomto stanovisku se dozorové orgány jednoznačně vyjádřily k otázce, zda postačí v přechodném období umožnit jeden ze způsobů zpřístupnění účtu. Dle ČNB a MFČR je na volbě banky, aby si zvolila jeden ze způsobů (buď API, nebo screen scraping); druhý ze způsobů pak umožnit nemusí.

Konečný návrh RTS bude nyní důkladně přezkoumán orgány EU a poté bude zahájena lhůta 18 měsíců, po kterých vstoupí RTS v účinnost. Datum účinnosti regulatorních technických standardů se tedy očekává přibližně v září 2019.

Radek Musílek
Senior Managing Associate
Ambruz & Dark Deloitte Legal s.r.o., advokátní kancelář
rmusilek@deloittece.com

[1)] SDĚLENÍ MINISTERSTVA FINANCÍ A ČESKÉ NÁRODNÍ BANKY ze dne 1. prosince 2017 k přechodnému období podle zákona č. 370/2017 Sb., o platebním styku, dostupné na http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/platebni_styk/pravni_predpisy/download/sdeleni_mfcr_a_cnb_k_zakonu_370_2017.pdf

---