3. 4. 2017

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Silné ověření klienta podle RTS ke směrnici PSD2

Evropský orgán pro bankovnictví (EBA) publikoval dne 23. února 2017 finální návrh regulatorních technických standardů (RTS) k nové směrnici o platebních službách na vnitřním trhu (PSD2)[1]. RTS upravují podmínky a výjimky z povinnosti provádět silné ověření klienta[2] a další povinnosti při provádění platebních transakcí.

Publikaci finálního návrhu RTS[3], které představují důležitou součást nového právního rámce pro provádění platebních transakcí v Evropské unii, předcházely rozsáhlé veřejné konzultace. V rámci poslední veřejné konzultace, která trvala do října roku 2016 EBA obdržel rekordní počet 224 podnětů od zástupců platebních institucí, bank, obchodníků či IT společností. V návaznosti na tyto podněty EBA identifikoval jako stěžejní témata (i) zajištění technologické neutrality v RTS[4], (ii) výjimky z povinnosti provádět silné ověření klienta a (iii) podmínky pro přístup k informacím o platebních účtech třetími stranami. RTS se tak vyznačují rozsáhlým katalogem povinností a představují kompromis mezi požadavky směrnice PSD2 a podněty z veřejných konzultací. Níže naleznete základní přehled povinností, které RTS přináší.

Kontrolní mechanismy

RTS ve svých obecných ustanoveních požadují, aby poskytovatel platebních služeb (PSP)[5] zavedl bezpečnostní opatření a kontrolní mechanismy, které mají zamezit neautorizovaným a neoprávněným platebním transakcím, a to i v případě, kdy využije výjimky z povinnosti provádět silné ověření klienta (viz níže). V rámci kontrolních mechanismů bude potřebné zohlednit rizikové faktory jako je (i) seznam zpronevěřených nebo zcizených ověřovacích prvků, (ii) výši každé platební transakce, (iii) známé podvodné scénáře a (iv) znaky malware[6] útoků v každé fázi ověřovacího procesu.

V případě, že PSP využije výjimku pro vynětí z povinnosti provádět silné ověření klienta na základě tzv. TRA[7] (podrobnosti níže), bude nad rámec výše uvedených rizikových faktorů povinen zohlednit i další rizikové faktory jako jsou platební zvyklosti klienta, platební historie klienta, abnormální chování klienta s ohledem na jeho platební historii či polohu plátce a příjemce plateb při provádění platebních transakcí.

Způsob implementace bezpečnostních opatření musí být pravidelně dokumentován, periodicky testován a auditován. V případě, že PSP využije výjimku z povinnosti provádět silné ověření klienta na základě TRA, bude povinen zajistit audit minimálně jednou ročně. Auditní zpráva musí být na požádání poskytnuta dozorovým orgánům.

Bezpečnostní požadavky na silné ověření klienta

Silné ověření klienta je podle směrnice PSD2 nutné provést na základě dvou nebo více ověřovacích prvků. Směrnice PSD2 zařazuje ověřovací prvky do kategorií (i) znalostí - tj. prvek co zná pouze klient jako je např. heslo, (ii) držení - tj. prvek co má v dispozici pouze klient jako je např. bezpečnostní token a (iii) inherence - tj. to čím klient je jako je např. digitální otisk prstu nebo sken oční duhovky. Silné ověření klienta na základě těchto prvků vyústí ve vygenerování ověřovacího kódu. Takto vygenerovaný ověřovací kód klient použije pro účely realizace platební transakce. Ověřovací kód musí být nenapodobitelný, přičemž znalost předchozího vygenerovaného ověřovacího kódu nesmí umožnit vygenerování nového kódu. Z ověřovacího kódu nesmí být zjistitelný žádný ověřovací prvek.

PSP bude povinen zajistit vzájemnou nezávislost ověřovacích prvků včetně toho, že v případě prolomení jednoho z ověřovacích prvků, nedojde k ohrožení integrity dalšího ověřovacího prvku. Zvláštní pozornost by v této souvislosti měla být věnována multifukčním zařízením, jako jsou smartphony či tablety, které jsou pro účely ověřování klientů používány ve stále větší míře. Bližší informace k požadavkům týkajících se jednotlivých ověřovacích prvků jsou uvedeny níže:

Ověřovací prvky z kategorie znalostí

PSP bude povinen zajistit, aby ověřovací prvky z kategorie znalostí nebyly zveřejněny nebo zpřístupněny neoprávněným osobám. Pro tyto účely bude PSP povinen přijmout taková technická opatření, která zajistí, že tyto ověřovací prvky nebudou zjistitelné.

Ověřovací prvky z kategorie držení

PSP bude povinen zajistit, že ověřovací prvky z kategorie držení nebudou použity neoprávněnými osobami. V této souvislosti bude potřebné, aby PSP zavedl opatření, která znemožní replikaci těchto ověřovacích prvků.

Ověřovací prvky z kategorie inherence

PSP bude povinen zajistit, aby tyto ověřovací prvky nemohly zjistit neoprávněné třetí osoby. Pro tyto účely bude PSP povinen zajistit, že při používání technických prostředků využívaných pro účely „načtení“ těchto ověřovacích prvků nedojde k identifikaci neoprávněné osoby jako plátce.

Výjimky z povinnosti provádět silné ověření klienta

V případě splnění podmínek pro výjimky podle RTS není potřebné provádět silné ověření klienta. Výjimky z povinnosti provádět silné ověření klienta byly jednou z nejvíce diskutovaných oblastí RTS. Základní informace o těchto výjimkách naleznete níže.

Přístup k informacím o platebním účtu

Výjimka z povinnosti silného ověření klienta se bude za stanovených podmínek aplikovat za předpokladu, že klient přistupuje online k informacím o zůstatku na platebním účtu či k informacím o platebních transakcích provedených v posledních 90 dnech. Tato výjimka se neuplatní, pokud klient k těmto informacím přistupuje poprvé nebo v případě, kdy klient přistupuje k informacím o platebních transakcích provedených v posledních 90 dnech, pokud silné ověření klienta bylo provedeno před více než 90 dny.

Bezkontaktní elektronické platební transakce, bezobslužné platební terminály

Výjimka z povinnosti provádět silné ověření klienta se bude aplikovat v případě bezkontaktních elektronických platebních transakcí za předpokladu, že výše transakce nepřesáhne 50 EUR a za předpokladu, že celková výše předchozích bezkontaktních elektronických platebních transakcí od posledního silného ověření klienta nepřesáhla 150 EUR nebo nedošlo k více než 5 po sobě jdoucím transakcím. Tato výjimka by se měla vztahovat na bezkontaktní platební karty, které se v České republice těší stále větší oblibě. Silné ověření klienta nebude podle RTS potřebné provádět i v případě provádění plateb za parkování či za jízdné prostřednictvím bezobslužných platebních terminálů. Tato výjimka byla do RTS zařazena v návaznosti na požadavky vzešlé z veřejných konzultací.

Specifické platební transakce

Výjimky by se měly aplikovat i na další platby jako jsou za stanovených podmínek platby mezi známými osobami (trusted beneficiaries) či pokud plátce provádí platební transakce o stejné výši se stejným příjemcem nebo pokud plátce a příjemce jsou tatáž osoba. Další z výjimek je za stanovených podmínek aplikovatelná v případě provádění platebních transakcí na dálku[8], jejichž výše nepřesahuje 30 EUR, pokud celková výše transakcí od posledního silného ověření klienta nepřesáhla 100 EUR nebo nedošlo k více než 5 po sobě jdoucím transakcím. Původní limit v případě těchto transakcí byl stanoven na 10 EUR, EBA se v návaznosti na veřejné konzultace rozhodl tento limit navýšit na 30 EUR.

Analýza transakční rizikovosti (TRA)

Silné ověření klienta nebude potřebné v případě, kdy PSP provede tzv. analýzu transakční rizikovosti (TRA) a dospěje k závěru, že platební transakce na dálku představuje nízké riziko. PSP bude oprávněn využít výjimku na základě TRA v případě transakcí dosahujících maximální výše 500 EUR. RTS stanovují podrobná pravidla pro provádění TRA včetně metodiky určování nízkorizikových transakcí, kontrolních mechanismů a případů, kdy je potřebná součinnost PSP s dozorovými orgány. Lze předpokládat, že výjimka z povinnosti silného ověření klienta na základě TRA, kterou se EBA rozhodl zařadit do RTS, bude pro řadu PSP atraktivní.

Zabezpečení osobních bezpečnostních údajů klientů

Velká pozornost je v RTS věnována i zabezpečení osobních bezpečnostních údajů klientů. PSP budou povinni zabezpečit, aby osobní bezpečnostní údaje klientů byly nezjistitelné v průběhu celého ověřovacího procesu (tj. v průběhu zobrazení, přenosu a ukládání bezpečnostních údajů). Zabezpečení má být mj. zajištěno tím, že osobní bezpečnostní údaje budou v průběhu ověřovacího procesu skryty a nebudou spolu s kryptografickými materiály ukládány ve formě Plaintext. Zvláštní bezpečnostní opatření se mají aplikovat i na doručování osobních bezpečnostních údajů klientovi, obnovování osobních bezpečnostních údajů a na jejich zneplatnění.

Standardy komunikace podle RTS

RTS stanovují přísné požadavky na bezpečnostní standardy používané při komunikaci mezi plátci a příjemci platebních transakcí. PSP by v této souvislosti měl věnovat zvýšenou pozornost využívání mobilních aplikací a měl by zajistit, že při komunikaci mezi plátci a příjemci plateb nedojde k přesměrování komunikace k neoprávněným osobám. PSP musí zajistit, že všechny platební transakce a interakce mezi PSP, klienty, jinými poskytovateli a jinými osobami, jako jsou např. obchodníci, budou zpětně dohledatelné.

RTS dále stanovují podrobné požadavky na komunikační interface ASPSP[9] (komunikační rozhraní

využívané pro účely komunikace mezi ASPSP a klientem). Každý ASPSP bude povinen zřídit alespoň jeden interface v případě, kdy poskytuje klientovi platební účet, který je přístupný online. K tomuto interface bude mít přístup poskytovatel služby iniciování platby a poskytovatel služby informování o účtu podle směrnice PSD2.[10]

ASPSP budou povinni poskytovatelům služby iniciování platby dodat informace potřebné pro účely provedení platební transakce. Z pohledu bank jako poskytovatelů platebních účtů je podstatné, že poskytovatel služby informování o účtu bude oprávněn přistupovat ke stanoveným informacím o vedeném platebním účtu kdykoliv, pokud by tento přístup (informace) aktivně požadoval klient a v případě, kdyby klient tento přístup (informace) aktivně nepožadoval, v maximálním rozsahu 4 přístupů během 24 hodin. Vyšší frekvence přístupů bude možná na základě dohody mezi ASPSP a poskytovatelem služby informování o účtu za předpokladu souhlasu klienta.

Legislativní proces

Dalším legislativním krokem je předložení RTS k adopci Evropské komisi a k projednání v Evropském parlamentu a v Radě EU. Následně se předpokládá publikace RTS v Úředním věstníku Evropské unie. RTS mají být účinné za 18 měsíců ode dne, kdy vstoupí v platnost (platnost RTS nastává 20 dnem po jejich vyhlášení v Úředním věstníku Evropské unie). RTS tak mohou vstoupit v účinnost v listopadu 2018.

Vláda schválila dne 13. března 2017 nový zákon o platebním styku, který transponuje směrnici PSD2 do českého právního řádu. Účinnost nového zákona o platebním styku je s ohledem na transpoziční požadavek směrnice PSD2 stanovena na 13. ledna 2018. Z důvodu, že nový zákon o platebním styku v ustanoveních upravujících silné ověření klienta (uživatele) odkazuje na tyto RTS, je vhodné této prováděcí právní normě věnovat zvýšenou pozornost.

Filip Michalec,
advokát

Dentons Europe CS LLP, organizační složka

Platnéřská 4
110 00 Praha 1

Tel.: +420 236 082 111
Fax: +420 236 082 999
e-mail: prague@dentons.com

_____

[1] Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES.
[2] Resp. silné ověření uživatele podle návrhu nového zákona o platebním styku.
[3] RTS jsou dostupné na www, k dispozici >>> zde.
[4] Technologická neutralita - není upřednostňována konkrétní technologie pro účely splnění povinností podle RTS.
[5] Poskytovatel platebních služeb - payment service provider podle směrnice PSD2.
[6] Škodlivý software, který je určený ke vniknutí nebo poškození počítačového systému.
[7] Analýza transakční rizikovosti - Transaction Risk Analysis.
[8] Platební transakcí na dálku se podle směrnice PSD2 rozumí platební transakce iniciovaná po internetu nebo prostřednictvím zařízení, které lze použít k dálkové komunikaci.
[9] Poskytovatel platebních služeb, který vede účet - account servicing payment service provider podle směrnice PSD2, tj. např. banka, která vede platební účet svého klienta.
[10] Poskytovatel služby iniciování platby a poskytovatel služby informování o účtu jsou noví poskytovatelé platebních služeb podle směrnice PSD2.

Další články:

- Novinky z české a evropské regulace finančních institucí za měsíc duben 2026
- Zaměstnanecké benefity dle ustanovení § 6 odst. 9 písm. d) zákona o daních z příjmů v roce 2026
- Flotilová novela: Kdo a kdy musí nově získat licenci k distribuci pojištění?
- Novinky z české a evropské regulace finančních institucí za měsíc březen 2026
- Převodní ceny v judikatuře a sporech se správcem daně
- Nový daňový režim ESOP v České republice od roku 2026. Posun k ekonomické realitě a mezinárodním standardům?
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- SCHEJBAL& PARTNERS stáli u získání jedné z prvních licencí dle MiCA v ČR
- Mezinárodní dožádání a lhůta pro stanovení daně: kritéria účelnosti, věcnosti a včasnosti v judikatuře
- Prověřování zahraničních investic a kybernetická regulace: řízená služba jako nová transakční proměnná
- Nová úprava kvalifikovaných zaměstnaneckých opcí