JAN PROCHÁZKA, ADVOKÁT
DELOITTE LEGAL

PSD2 a GDPR: Harmonie, či disonance?

PRÁVO A FINANCE

V první polovině roku 2018 se stanou účinnými dvě významné regulace, nová směrnice o platebních službách na vnitřním trhu a obecné nařízení o ochraně osobních údajů.

Na první pohled se může zdát, že jsou směrnice o platebních službách na vnitřním trhu („*PSD2*“) a obecné nařízení o ochraně osobních údajů („*GDPR*“) na sobě nezávislé, jakmile se však posuneme od obecných principů ke konkrétní implementaci, brzy narazíme na výzvy dané potřebou sladit detaily obou regulací v praxi. Pokud nebude rozdílnostem přístupů obou předpisů věnována patřičná pozornost, může být v konečném důsledku ohrožena i úspěšná implementace PSD2.

Jak GDPR,[1] tak PSD2 staví na obecném principu, že výlučným majitelem osobních údajů je jednotlivec a ten má mít možnost rozhodnout, jakým způsobem budou jeho data zpracovávána, uchovávána a s kým budou sdílena. V okamžiku, kdy se začneme zabývat konkrétní implementací, jsme však konfrontováni s nemalými výzvami sladit požadavky obou předpisů v reálné praxi.

Souhlas klienta

V rámci PSD2 budou moci třetí strany mající povolení od regulátora (tzv. TPP) přistupovat napřímo k informacím o klientově platebním účtu. Tento přístup bude podmíněn výslovným souhlasem klienta, na jehož základě budou TPP moci využít infrastrukturu banky za účelem poskytnutí dvou nových platebních služeb, a to služby nepřímého dání platebního příkazu (PIS) či služby informování o platebním účtu (AIS).[2]

Také nový zákon o platebním styku ve svém návrhu stanoví, že

1) GDPR zavádí nový standard souhlasů vyžadovaných pro zpracování osobních údajů. Ačkoliv PSD2 nenabízí vlastní definici (klientského) souhlasu, společnosti implementující PSD2 by neměly automaticky vycházet z předpokladu, že interpretaci GDPR bude nutno aplikovat ve všech případech, neboť ne všechny údaje o platbách jsou nutně současně osobními údaji.
2) Toto označení pro uvedené služby užívá současný návrh nového zákona o platebním styku, sněmovní tisk č. 1059, jenž implementuje ustanovení PSD2 do českého právního řádu.

výslovný souhlas udělí uživatel platební služby právě TPP.

Jinou věcí pak bude otázka, kdo udělení takového souhlasu v podmínkách poskytnutí služby zajistí, případně ověří. Ze strany bank jako zpřístupňujících stran totiž může existovat oprávněný zájem ujistit se o tom, že informace o platebním účtu předávané TPP jsou skutečně předávány na základě výslovného souhlasu klienta. Na druhé straně jsou právě TPP poskytovateli služby, kteří integrují poskytnutí souhlasu do procesu jejího nastavení optimálním způsobem z hlediska hladkého průběhu procesu a atraktivnosti služby jako takové. Navíc se bude jednat o subjekty disponující povolením od regulátora podrobené jeho dohledu a banky budou disponovat i určitými oprávněními v některých situacích požadované informace TPP neposkytnout.

Po pečlivém zvážení těchto souběžných požadavků jsme názoru, že ačkoliv budou TPP iniciátory zajištění si souhlasu klienta za účelem využití dat souvisejících s poskytnutím konkrétní platební služby, případně souhlasu s dalším využitím těchto dat nad rámec platebních služeb dle PSD2, ponesou banky v konečném důsledku odpovědnost za ověření předmětného souhlasu svého klienta. Tento proces bude pravděpodobně zahrnovat potvrzení údajů, jako je identita TPP, s nimiž si klient přeje sdílet své osobní údaje, rozsah osobních údajů, které budou sdíleny, včetně četnosti a délky udělení takového souhlasu. Dvoustupňový proces, kdy bude souhlas od klienta získán a až následně potvrzen, má potenciál zajistit lepší ochranu jak samotným bankám, tak jejich klientům a v neposlední řadě zároveň jednotlivým TPP.

Ze zahraničích příkladů je tento postup v souladu například s návrhem API standardu nedávno publikovaným britskou vládní iniciativou UK Open Banking. Zatímco britský Open Banking API standard, který nabude účinnosti v lednu 2018, bude povinný pouze pro devět největších britských bank[3] a bude se vztahovat na užší spektrum produktů, než definuje PSD2. Britský regulátor (*Financial Conduct Authority* – FCA) a ministerstvo financí (HM Treasury – HMT) se snaží motivovat všechny banky a třetí strany – TPP, aby přijaly tyto standardy jako společný základ pro bezpečné a efektivní sdílení bankovních dat.

S novou výší finančních sankcí za nedodržení požadavků GDPR hrozí při trvající absenci takového sjednocujícího předpisu, že některé banky upřednostní soulad s GDPR nad PSD2.

Lze předpokládat, že banky a TPP napříč EU budou tyto standardy sledovat se zájmem a budou se jimi inspirovat nebo se k nim dobrovolně připojí.

Citlivé údaje o platbách

Aktuální návrh regulatorních technických standardů (RTS) pro silné ověření klienta (SCA) a bezpečnou komunikaci (SC) v rámci PSD2 stanoví, že banky jsou povinny poskytnout poskytovatelům služby AIS stejné informace, jaké jsou dostupné klientovi při přímém on-line přístupu k jeho informacím o účtu, nesmí se však při tom jednat o „citlivé údaje o platbách“. Z hlediska návrhu zákona o platebním styku pak TPP nebudu oprávněny tyto citlivé údaje o platbách od klientů požadovat (AISP), případně je uchovávat (PISP).

Shora uvedená podmínka může být problematická, neboť právní úprava konkrétně nestanoví, co ony „*citlivé údaje o platbách*“ jsou. Podle návrhu zákona o platebním styku je citlivým údajem o platbách „*údaj, který může být zneužit k podvodu v oblasti platebních služeb, s výjimkou jedinečného identifikátoru a jména majitele platebního účtu v případě poskytovatele služby informování o platebním účtu nebo služby nepřímého dání platebního příkazu*“.

GDPR pracuje s pojmem osobního údaje jakožto s informací o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je ta fyzická osoba, kterou lze přímo či nepřímo odlišit zejména odkazem na určitý identifikátor, například jméno, rodné číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků, včetně ekonomické identity této fyzické osoby.

GDPR však zároveň umožňuje členským zemím EU stanovit si svá vlastní pravidla „pro zpracování zvláštních kategorií osobních údajů (‚citlivých údajů‘)“, definovaných jako osobní údaje o rasovém či etnickém původu, politických názorech, náboženském či filozofickém přesvědčení nebo odborovém členství, a zpracování genetických a biometrických dat.

Absence jasného vymezení, co vlastně jsou „*citlivé údaje o platbách*“, představuje výzvu v rámci interpretace i implementace a zároveň zvyšuje riziko regulatorního nesouladu. Bez dalšího upřesnění by se mohlo stát, že některé banky zaujmou spíše konzervativní přístup a prohlásí za citlivé údaje všechny, které bude možné do této kategorie zařadit, aby se vyhnuly možnému nesplnění regulatorních požadavků jak podle PSD2, tak GDPR.

Přechodné období

Další komplikaci z pohledu přenosu dat představuje fakt, že RTS pro silné ověření klienta a bezpečnou komunikaci (upřesňující pravidla přístupu k platebním účtům klientů a související sdílení dat) zatím nebyly definitivně dokončeny, a tudíž se neočekává, že by vstoupily v účinnost dříve než v druhém čtvrtletí roku 2019.[4]

Jednou z oblastí, kde zatím nebylo v RTS dosaženo shody, je umožnění tzv. „*screen scrapingu*“.[5] Oba unijní orgány, jak Evropský orgán pro bankovnictví (EBA), tak Evropská komise uvádějí, že praxe „*screen scrapingu*“ by měla být ukončena nejpozději uplynutím přechodného období, tedy ke dni nabytí účinnosti RTS.[6] V případě použití screen scrapingu je však pro ▸

3) Devět největších britských bank dle regulátora CMA, na které se již nyní vztahuje Open Banking standard jsou: Bank of Ireland, Barclays, Danske Bank, HSBC, Lloyds Banking Group, Nationwide, RBS Group a Santander – pozn. autora.
4) RTS pro silnou autentizaci klienta a bezpečnou komunikaci vstoupí v účinnost 18 měsíců od data jejich vydání ve věstníku European Union Official Journal.
5) Metoda využívající počítačový program ke kopírování dat z webové stránky navržené pro zobrazení informací pro běžné uživatele, na rozdíl od využití standardní komunikace přes API. Obvykle se screen scraping software vůči poskytovateli identifikuje jako lidský uživatel, ne jako robot.

banky velmi obtížné omezit přístup pouze na osobní údaje a ostatní data v rozsahu klientem uděleného souhlasu a být tak v souladu s dalšími požadavky na ochranu osobních údajů. Při aplikaci tohoto modelu bude pro banky mimořádně ztížena možnost ověřit si, zda a jaký charakter souhlasu byl klientem poskytnut.

Pro úplnost dodáváme, že v průběhu legislativního procesu se objevil pozměňovací návrh k novému zákonu o platebním styku, který počítal i s variantou, kdy budou pravidla přístupu TPP k platebnímu účtu řešena uzavřením dohody mezi bankou a TPP. Taková dohoda měla objektivně vymezovat pravidla poskytnutí konkrétní služby (AIS nebo PIS) a také stanovit metodiku silného ověření. Návrh rovněž počítal s alternativou dohody, kterou měla být situace, kdy by TPP doložilo bance splnění podmínek „uznávaného standardu“ přístupu k platebnímu účtu a silného ověření. Pozměňovací návrh nakonec nebyl ve třetím čtení v Poslanecké sněmovně přijat, otázka postupu v onom přechodném období tak bude muset být řešena výkladem, kdy k žádoucímu sjednocení praxe mohou přispět buď národní regulátoři, či evropské orgány vydáním svých výkladových stanovisek.

◆◆◆

Ze strany EU a národních regulátorů jsou podle našeho názoru nezbytné další jednotné „pokyny“, které umožní bankám i třetím stranám se adekvátně připravit a interpretovat požadavky PSD2 a GDPR, jak nyní v rámci přechodného období, tak i po něm.

S novou výší finančních sankcí za nedodržení požadavků GDPR (až do výše čtyř procent z globálního ročního obratu společnosti) hrozí při trvající absenci takového sjednocujícího předpisu, že některé banky upřednostní soulad s GDPR před souladem s PSD2.

Takové řešení by pravděpodobně vedlo k zásadnímu omezení přístupu TPP k datům a velmi striktní interpretaci rozsahu souhlasu klienta ze strany jednotlivých bank. V konečném efektu by byla negativně ovlivněna využitelnost služeb třetích stran a upozaděna přidaná hodnota nově zaváděných platebních služeb pro koncové uživatele.◆

6) Screen scraping umožňuje TPP přistupovat k jakýmkoliv informacím, které jsou k dispozici klientům na platformě internetového bankovnictví, stejně jako kdyby se přihlásili uživatelé sami.