**Návrh zákona o platebním styku - transpozice Revised Payment Services Directive**

Po poslední změně zákona o platebním styku novelou s účinností od 1. března 2017, jež zavedla mimo jiné například základní platební účet a novou pravomoc Úřadu na ochranu hospodářské soutěže, dochází důsledkem transpoziční povinnosti vůči sekundárnímu právu Evropské unie k ukotvení změn v souvislosti se směrnicí o platebních službách na vnitřním trhu, 2015/2366 (“PSD2”), které budou promítnuty do nového zákona o platebním styku (“zákon”), a který byl dne 15. 9. 2017 doručen do Senátu ČR v rámci další fáze legislativního procesu.



Samotné PSD2 je reakcí na rozvoj informačních technologií po přijetí první směrnice o platebních službách na vnitřních trhu (“PSD”) a především důsledkem rozvoje a zvýšení počtu jednotlivých poskytovatelů v rámci služeb platebního styku, pro něž byla dosavadní úprava nedostatečná. Zavedení nové regulace sice zvyšuje tlak na compliance u tradičních poskytovatelů platebních služeb, ale zároveň snižuje bariéry vstupu na trh pro FinTech společnosti. Tradiční poskytovatelé platebních služeb tak získávají na poli platebního styku novou konkurenci.

Prvním nově regulovaným institutem a subjektem trhu platebních služeb je správce informací o platebním účtu (“Account information services provider”, “AISP”). Jedná se o specifickou službu spočívající ve sdělování informace o platebním účtu prostřednictvím internetu poskytovatelem rozdílným od poskytovatele, který vede daný účet. Výkon činnosti je nově podmíněn povolením od České národní banky. Pro spotřebitele to bude především znamenat nové možnosti, jak kontrolovat a řídit své finance skrze AISP, na něhož budou kladeny poměrně vysoké nároky. Tyto nároky se především týkají implementace patřičných vnitřních procesů u AISP za účelem ochrany osobních údajů v souvislosti s Obecným nařízením o ochraně osobních údajů a nastavení řídících a kontrolních systémů nebo řízení rizik v souladu s § 48 zákona.

Další novinkou je služba nepřímého dání platebního příkazu, která spočívá v udělení platebního příkazu k převodu peněžních prostředků z platebního účtu jménem plátce poskytovatelem (“Payment initiation services provider”, “PISP”) rozdílným od poskytovatele, který pro plátce vede daný účet, je-li platební příkaz dán prostřednictvím internetu. Klienti poskytovatele služby nepřímého dání platebního příkazu mají možnost udělit online platební příkaz k bankovnímu účtu bez přímého přístupu k internetovému bankovnictví. Pro účely ochrany spotřebitele, osobních údajů a ochrany zdravého konkurenčního prostředí je kladen vysoký důraz na bezpečnost této služby. S tím souvisejí i zákonné podmínky, které musí subjekty poskytující takto specifické služby splňovat.

Pro účely vyšší ochrany elektronických transakcí je nově zavedena povinnost tzv. silného ověření uživatele. Tyto zvýšené bezpečnostní požadavky mají snížit míru rizik výskytu podvodných plateb a zvýšit šance na jejich odhalování. Každá osoba oprávněná poskytovat platební služby uplatní silné ověření uživatele, pokud plátce přistupuje ke svému platebnímu účtu prostřednictvím internetu, dává platební příkaz k elektronické platební transakci, provádí jiný úkon, který je spojen s rizikem podvodu v oblastech platebního styku, zneužitím platebního prostředku nebo informaci o platebním účtu, nebo požaduje informace o platebním účtu prostřednictvím poskytovatele služby informováním o platebním účtu. Dále dává-li uživatel platební příkaz prostřednictvím internetu, elektronického zařízení anebo nepřímo. Silné ověření plátce využívá identifikaci na základě údajů známých pouze uživateli, zařízení, co má uživatel ve své moci, nebo biometrických údajů uživatele.

Změnou v oblasti reportingu je každoroční povinnost osob poskytující platební služby informovat orgán dohledu, Českou národní banku, o bezpečnostních a provozních rizicích, kterým v souvislosti s poskytováním služeb byla vystavena, a o podvodech, které v oblasti platebního styku zaznamenala.

V souvislosti se zákonem o platebním styku a především PSD2 se na poli evropské legislativy objevily nové nároky na poskytovatele služeb platebního styku s účinností od 13. 1. 2018. První jsou zejména tzv. Závěrečné pokyny pro ohlašování závažných nehod (“Final Guidelines on Major Incident Reporting”), které kompletně upravují kritéria a metodologii, které se musí subjekty poskytující služby platebního styku držet, a to především z hlediska vyhodnocování a posouzení bezpečnostních a provozních rizik. Dále také, co je považováno za závažnou nehodu, a jakým způsobem, a v jaké lhůtě, je subjekt poskytující služby platebního styku orgán dozoru povinen o vzniklé nehodě informovat. Druhou je finální návrh Evropského bankovního úřadu tzv. technických standardů regulace silného ověření uživatele a bezpečné komunikace (“Regulatory Technical Standards on strong customer authentication and secure communication”). Tyto standardy do detailu upravují zabezpečení transakce, risk management, monitoring a nakládání s osobními údaji spotřebitelů poskytovateli služeb platebního styku.

Je zřejmé, že největší výzvou nebude ani tak inkorporace ustanoveních nového zákona o platebním styku do vnitřních mechanismů poskytovatelů služeb platebního styku, ale především compliance k Final Guidelines a RTS, což bude problematické především pro FinTech společnosti s nedostatečným kapitálem a zkušenostmi v oblasti regulace.