

Regulatorní architektura plateb: PSD3/PSR v AI-driven compliance

Anna Stárková

Advokátka, Head of Legal Engineering Myriad AI

Regulatorní trendy na EU finančních trzích

1. **Ochrana slabší strany** – posilování práv + přenášení odpovědnosti
2. **Deregulace** – fenomén omnibusů, centralizace dozoru
3. **Technologie** – efektivnější zpracování dat, více informací oběma stranám

= Jak reagovat na nové výzvy?

Ochrana slabší strany I - Budou banky dotovat podvodníky?

❖ Nová platební regulace - PSD3/PSR

- Čl. 59: *Jestliže byl uživatel platebních služeb, který je spotřebitelem, zmanipulován třetí osobou, která se vydávala za zaměstnance poskytovatele platebních služeb tohoto spotřebitele, přičemž neoprávněně použila jméno nebo e-mailovou adresu nebo telefonní číslo tohoto poskytovatele platebních služeb, a tato manipulace vedla k následným podvodným autorizovaným platebním transakcím, vrátí poskytovatel platebních služeb spotřebiteli celou částku podvodné autorizované platební transakce ...*

Ochrana slabší strany II - PSR data

❖ Jak to funguje jinde? UK – PSR data v prvním roce (od 7. října 2024 do 30. září 2025):

- Spotřebitelé nahlásili přibližně **269 000 nároků**; z toho 188 000 spadalo do režimu náhrady (a rostoucí trend)
- **88 % (173 mil. GBP)** finančních prostředků ztracených v důsledku APP podvodů bylo obětím nahrazeno
- 82 % nároků bylo vyřízeno do pěti pracovních dnů a 98 % do 35 pracovních dnů
- Jen **3 % žádostí zamítnuta** kvůli hrubé nedbalosti klienta

Ochrana slabší strany III - Opravdu chráníme spotřebitele?

- ❖ Spotřebitel neuvede úplné informace v žádosti o úvěr: Odpovědnost poskytovatele úvěru (neplatnost smlouvy...)
- ❖ Spotřebitel se nechá oklamat podvodníkem: Odpovědnost poskytovatele platebních služeb
- ❖ Před čím chráníme spotřebitele?

Deregulace - Omnibus a centralizace

- ❖ Omnibus = přidání na komplexitě místo zjednodušení
 - ESG omnibus – CSRD, CSDD
 - Data - Digitální omnibus, Omnibus k AI Aktu
- ❖ Centralizace dozoru = sjednocení praxe za cenu odlivu know-how
 - Nové agentury na EU úrovni: AMLA, AI Office
 - Posilování centralizovaného dozoru: ESMA a kryptofirmy

Technologie - Dožene právo technologický rozvoj?

- ❖ Horizontální regulace
 - GDPR, CER, AI Akt, Data Akt
- ❖ Sektorová regulace
 - DORA, CCD II, PSD3/PSR
- ❖ Kumulace povinností
 - ICT incident spojený s AI nástrojem způsobí nedostupnost klientských dat a výpadek karet
 - Reporting na: ČNB, ÚOOÚ, ČTÚ, MVČR... možná NÚKIB

NEBO dožene technologický rozvoj právo?

1. **Ochrana slabší strany** = instituty s důrazem na ochranu spotřebitele a vyřizování jejich práv
2. **Deregulace** = sjednocení reportingových povinností a spolupráce
3. **Technologie** = instituty s důrazem na odpovědnost, transparentnost a přezkum

Jak reagovat na nové výzvy?

- ❖ Sledovat nové regulace, horizontální i sektorové, a jejich výklad
- ❖ Identifikovat tzv. pain points – workproduct / workflow s největším potenciálem k automatizaci
- ❖ Identifikovat překryvy a efektivně je řešit (nebo využít)
 - Automatizované rozhodování
 - Dokumentace
 - Vendor management
 - Řízení rizik
- ❖ Využívat technologie bezpečně:
 - Rizika pro dotčené osoby
 - Rizika pro instituci

Jak reagovat na nové výzvy PSD3/PSR? I

- ❖ **Řízení rizik a podvodů**
 - Kontext PSD3/PSR: Posílená odpovědnost poskytovatelů platebních služeb za autorizované podvodné transakce včetně APP scams, důraz na prevenci, refund mechanismy a systematický monitoring podvodů
 - Příležitost: Real-time behaviorální scoring, detekce social engineering scénářů před autorizací, dynamické risk-based limity a automatizovaný decision engine pro refund workflow
- ❖ **Autentizace zákazníka a rozdělení odpovědnosti**
 - Kontext PSD3/PSR: Zpřesnění pravidel silné autentizace a jasnější rozdělení odpovědnosti mezi poskytovateli, větší důraz na posuzování hrubé nedbalosti klienta
 - Příležitost: Kontextová autentizace založená na chování uživatele, behaviorální biometrie, auditovatelná AI podpora při rozhodování o odpovědnosti a zamítnutí refundace

Jak reagovat na nové výzvy PSD3/PSR? II

❖ Otevřené bankovníctví a řízení přístupu třetích stran

- Kontext PSD3/PSR: Posílení rámce pro přístup třetích stran, povinnost robustních a výkonných API rozhraní, monitoring dostupnosti a incident reporting
- Příležitost: Anomaly detection v API provozu, detekce zneužití oprávnění, predikce porušení SLA a automatizace regulatorního reportingu

❖ Operační odolnost a řízení IKT rizik

- Kontext PSD3/PSR: Vyšší nároky na řízení operačních rizik, kontinuitu platebních služeb a hlášení incidentů, úzká vazba na požadavky DORA
- Příležitost: Prediktivní modely selhání infrastruktury, korelace bezpečnostních událostí, automatizovaná klasifikace incidentů a podpora regulatorního reportingu

Jak reagovat na nové výzvy PSD3/PSR? III

❖ Ochrana spotřebitele a řízení práv

- Kontext PSD3/PSR: Přísnější pravidla pro transparentnost vůči klientům, pevné lhůty pro vyřízení nároků a vyšší dohled nad komunikací
- Příležitost: NLP analýza reklamací, automatizované třídění nároků, predikce regulatorních rizik v komunikaci a explainable AI pro auditní stopu

❖ Prevence finanční kriminality a AML synergie

- Kontext PSD3/PSR: Nepřímé dopady na AML rámec skrze zvýšené požadavky na monitoring platebních toků a ochranu uživatelů
- Příležitost: Redukce false positives, síťová analýza transakčních vztahů, pokročilé modelování rizikových transakcí a prioritizace alertů

Na závěr

- ❖ Vše se mění: trh, klienti, technologie, hrozby, rizika
- ❖ Právo se na to snaží reagovat - často pozdě, někdy příliš robustně
- ❖ Největší výzva je najít rovnováhu mezi:
 - Globálním vývojem trhu
 - Očekáváním a chováním klientů
 - Technologickým rozvojem
 - Snahou vše řešit pomocí detailní a komplexní regulace
 - Nutností zajistit základní práva a svobody

Děkuji!

