

Minimální smluvní ustanovení a úskalí implementace nařízení DORA do praxe finančních institucí

14.10.2025
Praha

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.

PORTOS
Strategic Legal Advisory

1

Obsah

- **01** Základní požadavky a povinnosti subjektů NZKB
- **02** Zkušenosti z implementace DORA
- **03** Minimální a hlavní smluvní ustanovení
- **04** Plnění požadavků na smlouvy s dodavatele v praxi - hlavní úskalí
- **05** Diskuse

2

Základní požadavky regulace dle DORA

☐ Nastavení interního systému řízení rizik vyplývajících z outsourcingu a 3. stran

☐ Promítnutí regulatorních požadavků do smluvních ujednání s externími poskytovateli



3

Zkušenosti s implementací DORA

- Dohled a komunikace – spolupráce s ČNB, NÚKIB
- Interní audit připravenosti – ověřování souladu a účinnosti opatření
- Revize směrnic a politik – detailní aktualizace
- Krizová připravenost – jasné postupy a role při incidentu
- Interní audit připravenosti – ověřování souladu a účinnosti opatření
- Koordinační meetingy

4

Minimální požadavky na smlouvy



- ☐ Nařízení DORA rovněž uvádí výčet minimálních smluvních ustanovení, která mají být součástí outsourcingových smluv
- ☐ Požadavky jsou přísnější, pokud se jedná o outsourcing významných služeb IKT
- ☐ Regulatorní požadavky na případné ukončení smluvního vztahu s externím poskytovatelem
- ☐ Některá ustanovení budou upřesněna prováděcími předpisy, který by měl být zveřejněn v první polovině roku 2024
- ☐ Nové povinnosti se budou vztahovat rovněž na kritické externí poskytovatele služeb informačních a komunikačních technologií, jejichž činnost má systémový dopad na finanční sektor v Evropské unii - dohled nad těmito poskytovateli ze strany evropských orgánů dohledu

5

Hlavní požadavky na smlouvy



- ☐ Srozumitelný a úplný popis všech funkcí a služeb IKT dodávaných poskytovatelem služeb IKT s uvedením, zda je povoleno zajišťování služeb IKT podporujících zásadní nebo důležité funkce nebo jejich podstatných součástí subdodavatelem, a v kladném případě podmínky, kterými se toto využití subdodavatele řídí;
- ☐ Místa, konkrétně regiony nebo země, kde mají být nasmlouvané nebo subdodavatelem zajišťované funkce a služby IKT poskytovány a kde mají být zpracovávána data, včetně místa jejich uchovávání, a povinnost poskytovatele služeb IKT oznámit finančnímu subjektu předem, plánuje-li změnu těchto míst;
- ☐ Ustanovení týkající se dostupnosti, hodnověrnosti, integrity a důvěrnosti, pokud jde o ochranu údajů, včetně osobních údajů;
- ☐ Ustanovení o zajištění přístupu, obnovy a vrácení ve snadno přístupném formátu osobních a jiných než osobních údajů zpracovávaných finančním subjektem v případě platební neschopnosti, řešení krize nebo přerušování činností poskytovatele služeb IKT nebo v případě ukončení smluvních ujednání;

6

Hlavní požadavky na smlouvy II



- ☐ Popis úrovně služeb, včetně aktualizací a revizí;
- ☐ Povinnost poskytovatele služeb IKT poskytnout finančnímu subjektu pomoc bez dodatečných nákladů nebo za náklady, které jsou stanoveny ex ante, dojde-li k incidentu v oblasti IKT, který souvisí se službou IKT poskytovanou finančnímu subjektu;
- ☐ Povinnost poskytovatele služeb IKT plně spolupracovat s příslušnými orgány a s orgány příslušnými k řešení krize finančního subjektu, včetně osob jimi jmenovaných;
- ☐ Práva na ukončení smlouvy a související minimální výpovědní lhůty pro ukončení smluvních ujednání v souladu s očekáváními příslušných orgánů a orgánů příslušných k řešení krize;
- ☐ Podmínky pro účast poskytovatele služeb IKT na programech zvyšování povědomí o bezpečnosti v oblasti IKT a školeních o digitální provozní odolnosti

7

Interní systém řízení rizik

- Nutnost vyhotovení funkčního interního systému pro řízení rizik vyplývajících z outsourcingu služeb IKT – odpovědnost vedoucího orgánu
- Systém musí být proporcionální velikosti a obchodní činnosti finančního subjektu, zohledňuje povahu outsourcovaných služeb
- Nutné posouzení, zda je outsourcovaná IKT zásadní nebo důležitou (významná služba IKT) pro činnost finančního subjektu, neboť od toho se odvíjí rozsah požadavků na řízení souvisejících rizik
- Povinnosti v rámci interního systému řízení rizik:
 - ☐ provádět audity externích poskytovatelů
 - ☐ vést registr informací
 - ☐ hlásit nové outsourcingové smlouvy orgánům dohledu

8

Obecné požadavky na řízení rizik



- ☐ Finanční subjekty jsou vždy samy plně odpovědné
- ☐ Řízení rizika s ohledem na: princip proporcionality, povahu, rozsah, složitost atd., rizika vyplývající ze smluvních ujednání s třetími stranami
- ☐ Registr informací s ohledem na všechna smluvní ujednání o využívání služeb IKT
- ☐ Strategie pro riziko IKT třetími stranami se přijímá a pravidelně přezkoumává
- ☐ Před uzavřením smlouvy se hodnotí rizika a poskytovatelé IKT
- ☐ Auditní standardy se používají při kontrolách a auditu třetích stran – předem finanční subjekty stanoví četnost auditů a kontrol
- ☐ Strategie ukončení smlouvy se zavádějí pro zásadní funkce IKT

9

Povinnosti v rámci systému řízení rizik u významných služeb IKT

- Předběžně notifikovat orgány dohledu o plánovaném uzavření outsourcingové smlouvy
- Prověřovat plnění bezpečnostních norem u externích poskytovatelů
- Zavést strategii ukončení smluvního vztahu – nesmí být ohrožena činnost finančního subjektu a plnění regulatorních požadavků nebo nedojde ke zhoršení kvality služeb poskytovaných klientů, musí existovat plán přechodu k alternativnímu externímu poskytovateli či zajištění vlastního poskytování příslušných služeb
- Předběžně posuzovat přínosy a rizika nově outsourcovaných významných služeb IKT, a to z hledisek potenciální nahraditelnosti externího poskytovatele a koncentrace vícero významných služeb IKT u externího poskytovatele nebo úzce propojených poskytovatelů
- Sledovat, zda případné subdavatelské řetězce u externích poskytovatelů významných služeb IKT nevedou do zemí mimo EU, zda svou délkou či složitostí nepředstavují riziko z hlediska poskytování sjednaných služeb, nebo zda nenarušují efektivní dohled nad tímto poskytováním



? Otázka – bude prokázána dostatečná digitální odolnost, pokud budou všechny služby IKT, nebo jejich většina, outsourcovány jednomu externímu poskytovateli?

10

Poskytovatelé IKT z řad 3. stran



- ☐ DORA se vztahuje na širokou škálu poskytovatelů služeb IKT z řad třetích stran
- ☐ Poskytovatelé cloudových služeb, softwaru, služeb analýzy dat a poskytovatelů služeb datových center
- ☐ Podniky, které jsou součástí finanční skupiny a poskytují služby IKT převážně svému mateřskému podniku nebo dceřiným podnikům či pobočkám
- ☐ Subjekty, kteří poskytují činnosti zpracování plateb nebo provozují platební infrastruktury, s výjimkou centrálních bank při provozování platebních systémů nebo systémů vypořádání obchodů s cennými papíry a veřejných orgánů při poskytování služeb souvisejících s IKT

11

Smlouvy o poskytování služeb se 3. stranami

- Evidují se v aktualizovaném registru, který se zpřístupní dohledovým orgánům na žádost – minimálně 1x ročně se hlásí počet nových smluv a související informace
- Je možné ukončit v konkrétních situacích stanovených DORA, což musí finanční subjekty zajistit, a to včetně zamezení negativních důsledků takového ukončení
- Mandatorně obsahují specifická smluvní ujednání stanovená v článku 30, přičemž odpovědnost za plnění povinností plynoucích z DORA nese finanční subjekt
- Další specifika (např. vzory pro registr informací o smlouvách) budou stanoveny v RTS
- Povinný subjekt vytvoří funkci či pověří vedoucího pracovníka pro sledování ujednání o využívání IKT služeb od třetích stran

12

Sjednání smlouvy o outsourcingu 3. stran

- Předsmuvní fáze
 - Jedná se o outsourcing služeb IKT?
 - Je služba zásadní nebo důležitá pro činnost subjektu?
- Příprava smlouvy – nutné dodržet minimální požadavky na smlouvy
- Plnění smlouvy – monitoring plnění smlouvy, reakce na případné problémy
- Ukončení smlouvy – exit strategie, nedodržení SLA, výpadek poskytovatele – nutno mít jasný plán jednotlivých kroků pro jednotlivé případy

13

Testování exit strategií

- Nutné zajistit, aby ukončení smlouvy nevedlo k
 - Narušení činností
 - Narušení dodržování regulatorních požadavků
 - Zhoršení kontinuity a kvality poskytovaných služeb
- Plány ukončení smluvního vztahu
 - Komplexní
 - Zdokumentované
 - Dostatečně otestované
 - Pravidelný přezkum

14

Zásadní nebo důležitá funkce

"funkce, jejíž narušení by významně narušilo finanční výkonnost finančního subjektu nebo řádný průběh nebo kontinuitu jeho služeb a činností nebo jejíž přerušení či chybný nebo neúspěšný průběh by významně narušily dodržování podmínek a povinností finančního subjektu vyplývajících z jeho povolení nebo jeho dalších povinností na základě platného práva v oblasti finančních služeb"



15

DISKUZE

16



Kontakt

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.
info@portos.cz

T \ 00 420 224 827 884
W \ portos.cz

Hvězdova 1716/2b
140 00 Prague 4
Czech Republic

PORTOS
Strategic Legal Advisory