



V Praze 1. března 2024
Čj. 84/24+85/89

Stanovisko

k návrhu zákona o implementaci předpisů Evropské unie v oblasti digitálních financí

I. Úvod

Návrh zákona obsahuje implementaci dvou evropských nařízeních, a to nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (tzv. nařízení DORA) a nařízení Evropského parlamentu a Rady (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937 (tzv. nařízení MiCA). Obě tato nařízení jsou součástí Balíčku pro oblast digitálních financí, který byl Evropskou komisí zveřejněn v září roku 2020.

Požadavky na odolnost informačních systémů finančních institucí jsou aktuálně roztržštěny v jednotlivých evropských sektorových předpisech, a to směrnicích i nařízeních. Nařízení DORA je tedy novým jednotným předpisem, který tuto roztržštěnou právní úpravu sjednocuje. Nařízení DORA představuje standard, který musí každá finanční instituce, na niž se nařízení DORA vztahuje, dodržovat.

V rámci České republiky již existuje obecná právní úprava týkající se kybernetické bezpečnosti, a to především zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů. Stávající zákon o kybernetické bezpečnosti se vztahuje pouze na část subjektů působících na finančním trhu. Nová směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) **obsahuje obecnou úpravu kybernetické bezpečnosti, proto nařízení DORA ve vztahu k ní představuje lex specialis, což stanoví i samotné nařízení DORA.**

Hlavní principy nařízení DORA:

- dopadá na většinu regulovaných finančních subjektů, které budou muset dodržovat nařízení DORA, má tak představovat jednotný rámec pro finanční trh;
- doplnění nových požadavků na zavádění bezpečnostních opatření;
- doplnění nových požadavků na proces hlášení kybernetických bezpečnostních incidentů;
- jednotná pravidla pro testování kybernetické bezpečnosti;
- důraz na sdílení informací;
- prohloubení spolupráce mezi příslušnými orgány a regulovanými osobami, ale i mezi příslušnými orgány a dalšími orgány veřejné moci (např. návaznost na směrnici NIS2);

- nové požadavky třetí strany, tj. poskytovatele služeb informačních a komunikačních technologií.

Hlavní principy nařízení MiCA:

- ochrana klientů – především větší informovanost, právo na odstoupení od smlouvy v případě zbytkové kategorie kryptoaktiv;
- poskytování služeb souvisejících s kryptoaktivy licencovanými subjekty pod dohledem orgánu dohledu;
- nabízení kryptoaktiv veřejnosti pouze za dodržení stanovených podmínek;
- větší kontrola tzv. významných vydavatelů ARTs a EMTs;
- možnost orgánů dohledu zasáhnout v případě obav o ochranu investorů nebo o řádné fungování a integritu trhů.

II. Připomínky a návrhy změn:

Závěrečná zpráva z hodnocení dopadů regulace je, ač stručně, poměrně kvalitně zpracovaná. Obsahuje téměř všechny požadované i potřebné informace a prezentuje je relativně srozumitelnou formou, byť s jistými limity, které uvádím v textu. **Definice a popis problému včetně popisu existujícího právního stavu v dané oblasti** jsou v RIA popsány dostatečně. To, co se zprávě RIA dá vytknout, jsou prakticky naprosto nulové ekonomické a statistické informace.

V rámci popisu cílového stavu popisuje pouze obecné teze o efektivním fungování postupů daných nařízením DORA, efektivní výkon dohledu nad poskytovateli služeb souvisejících s kryptoaktivy a dalšími subjekty podle nařízení MiCA; Řádné plnění požadavků nařízení DORA i MiCA.

Vyhodnocení rizik obsahuje základní argumentaci o adaptaci českého právní řádu na dvě přímo účinná evropská nařízení. Poněvadž se právě jedná o evropská nařízení, měla by tato část obsahovat informace o tom, co by se stalo a jaká jsou rizika spojena s nepřijetím návrhu zákona o implementaci předpisů Evropské unie v oblasti digitálních financí.

Návrh variant řešení je zpracován v několika variantách pro 5 vybraných klíčových okruhů navržené právní úpravy. Co se týče zvolených okruhů, tak je lze považovat za dostatečné. Předkladatel pojal popis variant poměrně jednoduchým způsobem.

U návrhu varianty 2.1 - Nařízení DORA – hlášení závažných incidentů by bylo dobré popsat, jakým způsobem bude fungovat hlášení pro subjekty, které budou regulovány jak nařízením DORA, tak budou spadat pod nový zákon o kybernetické bezpečnosti (implementace NIS2).

Vyhodnocení variant

V této části RIA předkladatel rekapituluje a vyhodnocuje náklady u jednotlivých zpracovaných variant řešení. V tomto případě by vedle právních argumentů měly být doplněny částečně také ekonomické a statistické údaje. Zde rozhodně doporučujeme část dopracovat.

Stanovení nákladů a přínosů je pro jednotlivé okruhy a u nich navržené varianty zpracováno velmi stručně. Zde by bylo určitě dobré udělat aspoň elementární odhad nákladů, které mohou být s nařízením DORA spojeny. Jak sice překladatel uvádí „*Celkové náklady bohužel není možné jednoznačně stanovit, neboť změny u dotčených subjektů budou zcela individuální.*“, tak právě proto, že se DORA inspiruje např. ISO/IEC 27000, bylo by dobré tam tyto potenciální náklady v určitém rozpětí uvést. Zcela chybí stanovení nákladů regulátora.

Výběr nejvhodnějšího řešení je proveden v samostatné kapitole a je založen na předchozím vyhodnocení nákladů a přínosů jednotlivých variant.

Přezkum účinnosti budoucí regulace

Předkladatel uvádí, že subjekty spadající do působnosti nařízení DORA i MiCA mají vykazovací povinnost vůči České národní bance. Z tohoto důvodu bude přezkum účinnosti a vhodnosti nové právní úpravy prováděn Českou národní bankou, která vykonává funkci dohledového orgánu nad finančním trhem. Dále pak informuje o přezkumech regulace, které jsou součástí jak nařízení DORA (Čl. 58) tak nařízení MiCa (Čl. 140,141,142). Vzhledem k tomu, že součástí diskrece je stanovení výše některých sankcí, bylo by vhodné, aby toto bylo reflektováno i v přezkumu účinnosti regulace.

Konzultující organizace

Předkladatel uvádí, že řešené otázky byly konzultovány s Českou národní bankou a Národním úřadem pro kybernetickou a informační bezpečnost, dále pak, že návrh zákona byl předmětem veřejné konzultace a k nařízení DORA byl dne 31. 1. 2023 Ministerstvem financí konán seminář, kde byly taktéž diskutovány některé otázky. Konzultace se zdají být dostatečné.

III. Shrnutí připomínek ke zprávě z hodnocení dopadů regulace (zpráva RIA)

Obecně lze konstatovat, že RIA je zpracována na základní úrovni. Předkladatel v tomto případě zvolil cestu „nejmenšího odporu“ a v RIA pracuje se základními známými údaji a fakty. Věnuje se zejména právnímu posouzení a právním dopadům, v RIA chybí odpovídající ekonomické a statistické údaje.

Jako konkrétní připomínky lze k RIA uvést následující:

Pracovní komise Legislativní rady vlády pro hodnocení dopadů regulace shrnuje konkrétní připomínky, které uplatňuje vůči závěrečné zprávě RIA:

1. Zpracovat do RIA statistické údaje, především náklady spojené s implementací u stávajících a nově regulovaných subjektů
2. Zpracovat základní informace o návrhů regulačních technických norem (čl. 15,16 DORA) (RTS, ITS)

IV. Závěr

Pracovní komise Legislativní rady vlády pro hodnocení dopadů regulace **doporučuje** Legislativní radě vlády, **aby byl Návrh zákona o implementaci předpisů Evropské unie v oblasti digitálních financí doporučen vládě ke schválení** za předpokladu zohlednění výše **uvedených připomínek**.

Vypracoval:

Marek Ondroušek

Mgr. et Mgr. Marek Havrda, MA, MPA, Ph.D.

předseda komise