1. 8. 2024

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Blížící se termín pro uplatnění nařízení o digitální provozní odolnosti (DORA): Úvod

Nařízení DORA[1] je spolu se směrnicí NIS2 zásadním evropským právním předpisem, jehož cílem je posílit kybernetickou bezpečnost napříč celou EU. Na rozdíl od směrnice NIS2 se nařízení DORA zaměřuje konkrétně na zvýšení provozní odolnosti finančního sektoru a zároveň zavádí komplexní rámec, který má zajistit, aby všechny finanční subjekty regulované nařízením DORA byly schopny odolávat narušením a hrozbám souvisejícím s informačními a komunikačními technologiemi (IKT), reagovat na ně a zotavit se z nich.

Dalším důležitým evropským právním předpisem v oblasti kybernetické bezpečnosti je druhá směrnice o bezpečnosti sítí a informací (NIS2), která na rozdíl od nařízení DORA zavádí harmonizovaný rámec pro dohled a dozor nad řízením rizik v oblasti informačních a komunikačních technologií v dalších různých kritických odvětvích, od energetiky až po výrobu a distribuci potravin.

DORA, která doplňuje další regulační rámce uplatňované ze strany EU, zavádí jednotný soubor standardů pro digitální provozní odolnost, které musí regulované finanční subjekty začlenit do svých strategií řízení rizik po 17. lednu 2025.

Tento článek slouží jako úvod pro nadcházející sérii článků týkajících se regulace kybernetické bezpečnosti v rámci finančního sektoru, jejímž cílem bude v prvé řadě seznámit čtenáře se základními parametry nařízení DORA a z něj vycházejících povinností.

Na koho se nařízení vztahuje?

V zájmu zajištění vysoké úrovně kybernetické bezpečnosti ve finančním systému EU se evropští zákonodárci rozhodli zahrnout pod nařízení DORA velký počet různých finančních institucí, které budou muset – ve větší či menší míře – uplatňovat pravidla a normy zavedené tímto nařízením. Seznam povinných subjektů podle nařízení DORA zahrnuje, mimo jiné:

- úvěrové instituce;
- investiční podniky (obchodníky s cennými papíry);
- pojišťovny a zajišťovny;
- platební instituce a instituce elektronických peněz;
- správce alternativních investičních fondů;
- správcovské společnosti (SKIPCP);
- poskytovatele služeb souvisejících s kryptoaktivy;
- poskytovatele crowdfundingových služeb; či

- poskytovatele služeb IKT z řad třetích stran.

Subjekty podléhající nařízení DORA jsou považovány za zásadní pro infrastrukturu a bezpečnost finančního systému EU, a proto se od nich očekává, že budou udržovat vysokou úroveň digitální provozní odolnosti za účelem ochrany finančních trhů i jejich účastníků.

Povinnosti podle nařízení DORA

Subjekty, na které se vztahuje nařízení DORA, budou muset splňovat řadu požadavků, které nařízení ukládá, zahrnujících různá technická, organizační a právní opatření. Mezi základní povinnosti, které mají příslušné subjekty plnit, patří:

1. **řízení rizik v oblasti IKT**;
2. **hlášení kybernetických bezpečnostních incidentů příslušným orgánům, včetně zřízení komunikačních kanálů**;
3. **pravidelné testování digitální provozní odolnosti**;
4. **pravidelné školení zaměstnanců a vedoucích pracovníků**; a
5. **řízení rizik spojených s poskytovateli služeb z řad třetích stran (včetně nastavení klíčových smluvních ustanovení s těmito poskytovateli)**.

Kromě výše uvedených základních povinností se mohou finanční instituce také (za určitých podmínek) účastnit **ujednání o sdílení operativních a jiných informací o kybernetických hrozbách**, což by mělo dále posílit povědomí o bezpečnosti a kybernetických hrozbách v rámci celé EU prostřednictvím sdílení zkušeností s různými kybernetickými útoky a jejich praktickými řešeními.

Co bude dál?

Jelikož se datum použitelnosti nařízení DORA pomalu blíží, měly by všechny (potenciálně) dotčené instituce posoudit, zda a do jaké míry se jich nová pravidla budou týkat. Vzhledem k tomu, že nařízení pro regulované subjekty představuje řadu nových povinností a dosažení souladu s ním si vyžádá vynaložení značného množství času a různých zdrojů, doporučujeme včas alokovat dostatečné množství těchto zdrojů a adekvátní podporu jak technického, tak právního charakteru.

Sebastian Špeta

Martin Svoboda

Schönherr Rechtsanwälte GmbH, organizační složka
Jindřišská 937/16
110 00 Praha 1

Tel.: +420 225 996 500
Fax: +420 225 996 555
e-mail: se.speta@schoenherr.eu
e-mail: ma.svoboda@schoenherr.eu

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o provozní digitální odolnosti finančního sektoru.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Novelizace nařízení EU o odlesňování (EUDR)
- Zneužití práva na přístup podle GDPR
- Doručování soudních písemností ze zahraničí do ČR
- Novinky z české a evropské regulace finančních institucí za měsíc únor 2026
- Digital Fairness Act a influencer marketing – cesta ke konci roztříštěnosti regulace?
- Novinky z české a evropské regulace finančních institucí za měsíc leden 2026
- IATA Travel & Cargo akreditace v letectví – v čem spočívají její výhody?
- Digital Omnibus o AI: návrh nařízení o zjednodušení pravidel pro umělou inteligenci
- Rozhodčí nálezy vydané ruskými rozhodčími soudy a jejich uznání a výkon na území EU
- Environmentální tvrzení společností v hledáčku EU: Jak se vyhnout greenwashingu a obstát v nové regulaci?
- AIFMD II v České republice: Schvalovací proces a co čeká investiční společnosti