10. 7. 2023

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

Nařízení DORA – Revoluce pravidel pro kybernetickou bezpečnost ve finančním sektoru

S nárůstem digitalizace a technologického pokroku čelí podniky novým výzvám v oblasti bezpečnosti. Výjimku nepředstavuje ani finanční sektor, kde je s ohledem na potenciální škody a rizika kybernetických útoků klíčové zajistit vysokou úroveň ochrany dat a informací. Na tyto výzvy reagovala Evropská unie přijetím nařízení Digital Operational Resilience Act (DORA)[1]. Toto nařízení představuje nejvýznamnější část snah EU o posílení digitální odolnosti celého finančního systému a zahrnuje řadu nových pravidel a povinností pro finanční subjekty.

Co je nařízení DORA?

Nařízení DORA, přijaté v prosinci 2022, je právní nástroj EU, který má za cíl **zvýšit odolnost finančního sektoru vůči kybernetickým hrozbám**. DORA vytváří harmonizovaný rámec pro digitalizaci ve finančním sektoru, stanovuje předpisy pro správu rizik spojených s digitálními službami a povinnosti ohledně bezpečnostních incidentů. Cílem nařízení je nejen stanovit pravidla pro řešení kybernetických útoků v evropském finančním odvětví a zmírňování jejich dopadů, ale i pro jejich předcházení.

Nařízení DORA bylo přijato jako speciální regulace finančního sektoru ve vztahu ke směrnici **Network and Information Security 2** (**NIS2**)[2], která upravuje pravidla kybernetické bezpečnosti obecně napříč různými sektory, například v oblasti digitálních služeb, dopravy či výrobního průmyslu. Vedle těchto předpisů byla přijata i směrnice **o odolnosti kritických subjektů (CER)**[3], která stanovuje pravidla pro posílení odolnosti kritických subjektů, mezi které řadí subjekty, jejichž kybernetické odolnost je významná pro bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Na koho se DORA vztahuje?

Nařízení DORA se vztahuje na většinu finančních institucí, mezi které lze zařadit:

- Banky
- Platební instituce
- Instituce elektronických peněz
- Obchodníky s cennými papíry
- Poskytovatele služeb souvisejících s kryptoaktivy dle MiCA či ICOs (vydavatelé tokenů vázaných na aktiva)
- Crowdfundingové platformy (poskytovatelé služeb skupinového financování)
- Investiční společnosti
- Pojišťovny a zajišťovny
- Externí dodavatele ICT služeb (např. dodavatelé cloudových služeb, software a datových center)

Je nezbytné zdůraznit, že z platnosti nařízení DORA nejsou obecně vyloučeny ani mikro či malé podniky, velikost podniku je však relevantní pro určení konkrétního rámce povinností.

Pro účely zjištění toho, zda se na Vás nařízení DORA vztahuje, připravila naše advokátní kancelář jednoduchý dotazník.

Jaké jsou nové povinnosti stanovené nařízením DORA?

DORA stanovuje širokou škálu povinností, které musí finanční instituce splnit. Jak je uvedeno výše, tato pravidla se mohou lišit podle velikosti a typu subjektu, nicméně obecně budou instituce povinny zajistit například:

- **Rámec pro řízení rizik spojených s provozem ICT**
- **Školení vedoucích pracovníků**
- **Zvládání a hlášení bezpečnostních incidentů**
- **Pravidelné testování bezpečnostní odolnosti systémů a služeb**
- **Monitorování rizik spojených s poskytovateli služeb ICT**

Při nesplnění některé ze stanovených povinností bude příslušné finanční instituci hrozit uložení nápravného opatření nebo sankce, které musí být dle znění nařízení **účinné, přiměřené a odrazující**.

Od kdy je nutné povinnosti splnit?

Nařízení DORA vstoupilo v platnost v lednu 2023, od té doby mají povinné subjekty 24 měsíců na implementaci nových pravidel. Lhůta povinným subjektům tak vyprší **17. ledna 2025**.

Přestože stanovená lhůta může působit jako poměrně dlouhý časový horizont, pro zajištění efektivního a bezproblémového průběhu celé implementace povinností z nařízení DORA **doporučujeme, aby finanční instituce zahájily přípravu bez odkladu**.

Evropské dohledové orgány (**EBA, EIOPA a** ESMA)[4] v současné době zahájily veřejnou konzultaci o podobě návrhů regulačních technických standardů (RTS) a prováděcích technických standardů (ITS) k nařízení DORA. Cílem těchto standardů je zajistit jednotný rámec dokumentace v oblasti kybernetické bezpečnosti a hlášení incidentů, kdy obsahují například kritéria pro klasifikaci incidentů či šablony pro registr informací.

Veřejná konzultace k návrhům RTS a ITS bude probíhat do 11. září 2023. Do této doby je možné zasílat dohledovým orgánům připomínky k této konzultaci na jejich webové stránce.

Nikola Prachařová
Advokátní koncipient / Associate

STUCHLIKOVA & PARTNERS

Stuchlíkova & Partners, advokátní kancelář, s.r.o.

Spálená 97/29
110 00 Praha 1 – Nové Město

Tel.: +420 222 767 393
e-mail: info@stuchlikova.com

---

[1] 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

[2] 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

[3] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES

[4] Evropský orgán pro bankovnictví, Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění a Evropský orgán pro cenné papíry a trhy

Další články:

- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Návrh nového zákona o digitální ekonomice
- Byznys a paragrafy, díl 30.: Jednání za s.r.o. – zápis jednatelského oprávnění do obchodního rejstříku
- Prověřování zahraničních investic a kybernetická regulace: řízená služba jako nová transakční proměnná
- Předběžné opatření a další instituty k ochraně věřitelů při přeměnách
- Silná koruna: jaké dopady má posilující koruna na české firmy
- Problematické aspekty změn v úpravě odpovědnosti za škodu způsobenou vadou výrobku
- Byznys a paragrafy, díl 29.: Jednání za s.r.o. – jednatelé
- K (ne)způsobilosti notářského zápisu jako exekučního titulu pro nařízení exekuce prodejem zástavy
- Když korporátní neshody nestačí: soudní zásah do účasti společníka jako krajní řešení
- Do 5 milionů EUR bez prospektu cenných papírů - novela ZPKT!