25. 4. 2024

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

Nařízení DORA, aneb bezpečnost finančních subjektů v oblasti IKT

17. ledna 2025 vstoupí v účinnost, v plném rozsahu, nařízení Evropského parlamentu a Rady (EU) 2022/2554 o digitální provozní odolnosti finančního sektoru (dále jen „DORA“). Cílem tohoto nařízení je zajistit bezpečnost finančních subjektů v oblasti informačních a komunikačních technologií (dále jen „IKT“).

DORA je reakcí především na rostoucí digitalizaci a vzájemnou propojenost finančního sektoru, což vede k vyššímu riziku v oblasti IKT a zvyšuje zranitelnost vůči kybernetickým hrozbám, zdůrazňuje význam adaptace a připravenosti finančního sektoru na digitální věk, zajišťuje lepší ochranu proti kybernetickým hrozbám a usiluje o zajištění stabilního a bezpečného finančního prostředí v Evropské unii.

Společně s nařízením DORA, byly přijaty i dvě směrnice NIS 2 a CER, jež se také vztahují na oblast IKT a kyberprostoru, první jmenovaná, NIS 2, se zabývá opatřeními, které mají vést k zajištění vysoké společné úrovně kybernetické bezpečnosti v rámci Unie u středních a velkých podniků, provozujících služby uvedené v přílohách směrnice. Směrnici NIS 2 a co od ní očekávat shrnul ve svém článku kolega Mgr. Petr Hanzel tady NIS 2. Druhá jmenovaná, směrnice CER, se zase zaměřuje na kybernetickou bezpečnost tzv. kritických subjektů, jakými jsou například dodavatelé a distributoři strategických komodit, či třeba banky.

Cíl nařízení DORA a na koho se vztahuje

Prvně k vyjasnění toho, kdo jsou těmi finančními subjekty, na něž regulace dopadá? Finančními subjekty, které podléhají nařízení, jsou banky, pojišťovny, obchodníci s cennými papíry, správci a obhospodařovatelé investičních fondů, ratingové agentury, či poskytovatelé služeb spojených s krypto aktivy. Jakož i „třetí strany“, tedy poskytovatelé služeb, které souvisejí s IKT, jako jsou například cloudové platformy, či služby analýzy dat a další.

Cílem nařízení DORA je posílit digitální provozní odolnost finančního sektoru prostřednictvím zavedení rámce pro řízení rizik spojených s IKT. Nařízení má za cíl zajistit, aby finanční instituce byly lépe připraveny identifikovat, chránit se a efektivně reagovat na kybernetické hrozby a jiné incidenty IKT. Toho hodlá dosáhnout sjednocením regulačního rámce v celé EU, posílením odolnosti proti rizikům z třetích stran a podporou sdílení informací o hrozbách, což povede ke zlepšení bezpečnosti a stabilitě celého finančního sektoru.

Povinnosti, které DORA zakládá

Finanční subjekty jsou povinny zavést a udržovat komplexní rámec pro řízení rizik v oblasti IKT, který zahrnuje postupy a kontrolní mechanismy pro identifikaci, hodnocení, monitorování a minimalizaci rizik. Rámec by měl být integrován do celkové struktury finančního subjektu, s tím, že odpovědným je za tento risk management vedoucí orgán. Vedoucím orgánem však v kontextu digitálního risk managementu nemusí být pouze statutární orgán, ale také všechny osoby ve vedoucím postavení v rámci vnitřní struktury finančního subjektu. Tím se rozumí například vedoucí oddělení risk managementu nebo jakákoliv jiná vedoucí osoba k tomu určená.

Finančním subjektům vznikne nařízením povinnost pravidelně provádět testování odolnosti IKT, a to minimálně jednou ročně. Zároveň i povinnost data z testování vzniklá shromažďovat, aby byla identifikovaná zranitelnost systémů a procesů. To však nezakládá finančním subjektům povinnost pravidelného oznamování kontrolnímu orgánu, s kontrolním orgánem finanční subjekty komunikují pouze v případě hrozícího, či již proběhlého incidentu, či na základě výslovné žádosti kontrolního orgánu poskytnutí určitých dat nebo informací.

Tímto kontrolním orgánem v rámci České republiky bude ČNB a NÚKIB, kteří v rámci memoranda o vzájemné spolupráci ze dne 31. května 2022 spojují síly pro věci kybernetické bezpečnosti a odolnosti.

Důležitou pasáží nařízení je i stanovení minimálních požadavků na smlouvy uzavírané mezi finančním subjektem a poskytovatelem služeb IKT. DORA cílí především na ujednání přesného a srozumitelného popisu všech dodávaných služeb, ale i na podmínky ukončení smlouvy a zároveň i na povinnost poskytovatele služeb IKT poskytnout finančnímu subjektu pomoc, nastane-li incident v oblasti IKT.

Jak se rizika v oblasti IKT stávají stále složitějšími a sofistikovanějšími, závisí správná opatření pro detekci a prevenci rizika ve značné míře na sdílení informací o kybernetických hrozbách a zranitelnosti mezi finančními subjekty navzájem. Tím se posiluje kolektivní schopnost sektoru identifikovat a předcházet potenciálním hrozbám. Toho chce nařízení DORA docílit apelem na finanční subjekty, aby mezi sebou vybudovali, či posílili komunikační kanály.

Shrnutí klíčových dopadů nařízení DORA

1. **Zavedení komplexního rámce pro řízení rizik IKT:** Finanční subjekty jsou povinny implementovat, do celkové struktury subjektu, postupy a kontrolní mechanismy pro identifikaci, hodnocení, monitorování a minimalizaci IKT rizik.
2. **Povinnost pravidelného testování odolnosti:** Finanční subjekty musí alespoň jednou ročně provádět testování odolnosti IKT, shromažďovat data z těchto testů a identifikovat zranitelnost svých systémů a procesů, v rámci zlepšování bezpečnosti.
3. **Zpřísnění požadavků na smlouvy s poskytovateli služeb IKT:** Nařízení stanoví minimální požadavky na smlouvy s poskytovateli služeb IKT. Těmi jsou například: jasný popis služeb, přesné podmínky ukončení smlouvy a povinnost poskytovatele služeb IKT pomoci finančnímu subjektu při incidentu.
4. **Podpora sdílení informací o hrozbách:** DORA zdůrazňuje význam vzájemného sdílení informací o kybernetických hrozbách a zranitelnostech mezi finančními subjekty, aby se posílila kolektivní schopnost sektoru identifikovat a předcházet potenciálním hrozbám.

Postup v případě incidentu

Jako součást rámce pro řízení rizika v oblasti IKT jsou finanční subjekty povinny zavést krizové komunikační plány, které mají umožnit odpovědné a efektivní informování klientů, obchodních partnerů, veřejnosti a samozřejmě regulátora alespoň o závažných incidentech souvisejících s IKT. Dále **nařízení klade důraz na politiku zachování provozu finančního subjektu, při současném odstranění rizika. Proběhlé incidenty jsou pak hlášeny orgánu dohledu**, který o nich sepíše zprávu, která by měla sloužit ostatním finančním subjektům k reakci na proběhlou situaci a vylepšení vlastní strategie.

Sankce

DORA také opravňuje kontrolní orgán **uložit sankci poskytovateli IKT služeb**. Kdy? Za

předpokladu, že poskytovatel:

1. **neposkytne informace a dokumentaci**
2. **neumožní šetření a kontrolu**
3. **neodevzdá zprávu o nápravě na základě doporučení orgánu dohledu**

Sankce, kterou může kontrolní orgán uložit, **se ukládá na denním základě 1 % průměrného denního celosvětového obratu** poskytovatele služeb IKT z řad třetích stran za předchozí účetní období, avšak n**ejdéle po dobu 6 měsíců**. Sankce se tak může **po 6 měsících vyšplhat až na maximálně 0,5 % celosvětového ročního obratu poskytovatele za předešlý rok.**

Závěr

Nařízení DORA přináší významné změny pro finanční sektor EU s cílem zvýšit digitální provozní odolnost a ochranu proti kybernetickým hrozbám. Implementace těchto opatření vyžaduje pečlivou přípravu a adaptaci finančních subjektů, aby byly schopny splnit nové požadavky a zároveň zajistit bezpečnost a stabilitu finančního prostředí.

Pokud byste si s implementací povinností, plynoucích z nařízení, nebo čímkoliv v této oblasti nevěděli rady či potřebovali právní poradenství, neváhejte se na nás obrátit, rádi Vám pomůžeme.

JUDr. Jakub Dohnal, Ph.D., LL.M.,
advokát, partner

Matěj Menšík,
paralegal

ARROWS advokátní kancelář, s.r.o.

Plzeňská 3350/18
150 00 Praha 5 – Smíchov

Tel.: +420 245 007 740
e-mail: office@arws.cz

Další články:

- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti
- Detekce podezřelého obchodu v kontextu hazardních her
- AI omnibus