17. 2. 2023

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

Nařízení DORA, na co se připravit?

Dne 14. prosince 2022 bylo přijato nařízení o digitální provozní odolnosti finančního sektoru[1]. Účelem nařízení DORA, které vstoupí v celém svém rozsahu v použitelnost dne 17. ledna 2025, je zajistit provozní odolnost finančních subjektů v oblasti informačních a komunikačních technologií[2].

Spolu s nařízením DORA byly přijaty také směrnice NIS2[3] a směrnice CER[4] upravující taktéž oblast IT a kybernetické bezpečnosti. Směrnice NIS2 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii reguluje cca 60 služeb v 18 různých odvětvích (např. oblast dopravy či chemický průmysl)[5]. DORA je pak k této směrnici ve vztahu speciality, když pokrývá problematiku kybernetické bezpečnosti především finančních subjektů. Poslední norma, směrnice CER, se zaměřuje na odolnost tzv. kritických subjektů, jakými jsou např. dodavatelé a distributoři pitné vody, banky nebo potravinářské podniky[6].

Předmět a oblast působnosti

Generálně můžeme říci, že cílem[7] je zvýšení úrovně IT bezpečnosti v oblasti bankovnictví a kapitálového trhu. Nařízení ukládá povinnosti finančním subjektům jako takovým, ale i na poskytovatelům služeb v oblasti ICT, a stanovuje minimální požadavky na smlouvy uzavírané mezi těmito osobami.

Co si však pod předcházením kybernetickým hrozbám představit a jak toho má být dosaženo? Hlavními oblastmi jsou ICT risk management, ohlašování významných incidentů[8] a hrozeb spojených s ICT, sdílení informací o kybernetických hrozbách či preventivní testování odolnosti informačních systémů.

Veškeré subjekty, na něž regulace dopadá, jsou definovány jako finanční subjekty, a jsou jimi např. banky, pojišťovny, obchodníci s cennými papíry, správci a obhospodařovatelé investičních fondů[9], ratingové agentury či poskytovatelé služeb souvisejících s kryptoaktivy podle nařízení MiCA[10].

DORA se tak vztahuje téměř na celý finanční trh. Z tohoto důvodu je třeba řídit se při aplikaci předpisu zásadou proporcionality a přihlédnout k velikosti, rizikovému profilu či složitosti služeb poskytovaných finančním subjektem[11]. Zároveň je v určitých částech nařízení stanoven odlišný režim pro skupinu mikropodniků[12].

Vnitřní implementace

V rámci vnitřní implementace nařízení musí být na prvním místě vypracovány vnitřní předpisy upravující řešení ICT incidentů (včetně komunikace s regulátorem[13]) a jejich klasifikaci. Stanovují se postupy pravidelných kontrol, je třeba jmenovat osoby odpovědné za ICT risk management a zajistit průběžné školení zaměstnanců v této oblasti. Svou strategii digitální odolnosti musí finanční subjekt také pravidelně vyhodnocovat.

Odpovědným za risk management, za schvalování celkové strategie digitální odolnosti i za rozdělení konkrétních povinností a úkolů souvisejících s ICT je vedoucí orgán finančního subjektu. Vedoucím orgánem[14] zde přitom nemusí být pouze statutární orgán, ale také všechny osoby ve vedoucím postavení v rámci vnitřní struktury finančního subjektu (např. vedoucí oddělení risk managementu

nebo vedoucí oddělení compliance).

Prevence – jak hrozbám předcházet?

Finanční subjekty nemají povinnost pravidelného reportingu a s regulátorem v zásadě komunikují pouze v případě hrozícího či již proběhlého incidentu/kybernetické hrozby, případně na základě výslovné žádosti regulátora o poskytnutí určitých dat či informací[15].

K předejití či ubránění se kybernetickým hrozbám má přispět povinné testování odolnosti finančních subjektů. Standardní testování systémů a aplikací by mělo probíhat alespoň jednou ročně[16]. Penetrační testování na základě hrozeb[17], tedy jakési simulování kybernetické hrozby, pak musí probíhat alespoň jedenkrát za tři roky[18]. Penetrační testování může probíhat také hromadně a může být zajišťováno třetí stranou pro více finančních subjektů najednou (např. testování prováděné poskytovatelem cloudových služeb).

Nařízení dále stanoví minimální požadavky na smlouvy uzavírané mezi finančním subjektem a poskytovatelem služeb ICT[19]. Ve smlouvě musí být např. ujednán přesný a srozumitelný popis všech dodávaných služeb, podmínky ukončení smlouvy nebo povinnost poskytovatele poskytnout pomoc finančnímu subjektu, dojde-li k incidentu v oblasti ICT.

Jak postupovat v případě incidentu?

V případě incidentu (kybernetického útoku, ohrožení řádného fungování informačních systémů) je kladen důraz především na zachování provozu (*business continuity*) při současném odstranění vzniklého rizika. Postupuje se podle předem připravených krizových plánů, komunikováno je s klienty, obchodními partnery i regulátorem. Proběhlé incidenty jsou hlášeny orgánu dohledu, který o nich sepíše zprávu, a ta by pak měla sloužit ostatním finančním subjektům jako inspirace k vylepšení vlastní strategie odolnosti.

Závěrem

Nařízení bylo schváleno před třemi měsíci a přímo použitelným se stane až na začátku roku 2025. Přesto by finanční subjekty (zejména ty menší) již dnes měly zpozornět a začít se na dodržování nových pravidel připravovat. Ke správnému aplikování nové regulace, věřme, přispějí také unijní prováděcí předpisy (na které zatím čekáme), jelikož samo nařízení je psáno, i na poměry evropské legislativy, velmi obecným jazykem. Stejně tak je možné očekávat stanoviska a vyjádření orgánů dohledu (ESMA a v České republice ČNB, příp. NÚKIB).

Mgr. Ondřej Kučera,
právník

Filip Jindra

KLB LEGAL

KLB Legal, s.r.o., advokátní kancelář

Letenská 121/8
118 00 Praha 1

Tel.: +420 739 040 363
e-mail: info@klblegal.cz

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 („nařízení DORA“ nebo „nařízení“).

[2] Z anglického Information and Communication Technologies („ICT“)

[3] Směrnice Evropského parlamentu a Rady (EU) 2022/2055.

[4] Směrnice Evropského parlamentu a Rady (EU) 2022/2557.

[5] Směrnice by měla být provedena zejména novelou zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

[6] Směrnice by měla být provedena zejména novelou zákona č. 240/2000 Sb., krizový zákon.

[7] Čl. 1 a 2 nařízení DORA.

[8] Pojem incident související s ICT je definován v čl. 3 bodu 8 nařízení DORA.

[9] Povinnosti podle DORA by se neměly vztahovat na alternativní fondy podle § 15 zákona č. 240/2013 Sb., o investičních společnostech a investičních fondech.

[10] Nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937.

[11] Čl. 4 nařízení DORA.

[12] Podle čl. 3 bodu 60 nařízení jsou jimi některé druhy finančních subjektů, které zaměstnávají méně než deset osob a jejichž roční obrat nebo celková roční bilanční suma nepřekračuje 2 miliony EUR.

[13] Národním orgánem dohledu bude zřejmě ČNB nebo NÚKIB, případně oba tyto orgány dohromady.

[14] Vedoucí orgán je definován v čl. 3 bodě 30 nařízení DORA.

[15] Zpráva o ICT risk managementu se vyhotovuje jednou ročně, ale orgánu dohledu se předkládá pouze na žádost.

[16] Čl. 24 odst. 6 nařízení DORA.

[17] Definováno v čl. 3 bodě 17 nařízení DORA.

[18] Čl. 26 odst. 1 nařízení DORA.

[19] Čl. 30 nařízení DORA.

Další články:

- Žaloba na fair exit vůči společníkům s. r. o. jednajícím ve shodě
- Reklamace vad stavby
- Hodnotící dotazníky jako obchodní sdělení v kontrolním plánu ÚOOÚ pro rok 2026
- Konec „severních ateliérů“? Nový stavební zákon otevírá dveře k rekolaudaci ubytovacích jednotek na plnohodnotné byty
- Byznys a paragrafy, díl 33.: Prevence střetu zájmů (jednatel × společnost)
- Jak se vyhnout zákazu a postihu dohod o určování cen pro další prodej?
- Střet zájmů členů volených orgánů obchodních korporací: pravidla, proces a následky
- Nová „tlačítková” povinnost pro e-shopy
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie