



DORA Vytváří regulační rámec pro digitální provozní odolnost, na jehož základě všechny podniky musí zajistit, aby byly schopny přestát všechny druhy narušení a hrozeb souvisejících s informačními a komunikačními technologiemi, reagovat na ně a zotavit se z nich.

– Rada EU

Nařízení o digitální provozní odolnosti (DORA)

Přehled pro finanční subjekty a třetí strany v oblasti IKT

Proč je DORA důležitá pro mou organizaci?

DORA se bude vztahovat na více než 22 000 finančních subjektů a poskytovatelů služeb IKT. Nařízení zavede **nové požadavky pro všechny účastníky finančního trhu**.

DORA vnímáme jako významnou změnu pro subjekty v rámci dohledu ESMA či EIOPA, ale také pro banky, které již musí být v souladu se stávajícími směrnici EBA o bankovním dohledu.

Nařízení je jedinečné tím, že zavádí **Union Oversight Framework**, což je celounijní rámec pro dohled nad **kritickými poskytovateli IKT** dle evropských orgánů dohledu (ESA).

DORA se zaměří na pět klíčových témat



Řízení rizik IKT

- Komplexní přehled služeb a IT mgmt založený na scénářích.
- Provozní a technické možnosti kybernetické bezpečnosti
- Odolnost podnikové architektury a BCM



Hlášení incidentů

- Hlášení incidentů souvisejících s IKT
- Root-cause analýza následující po IKT incidentech
- Identifikace a hlášení zlepšení



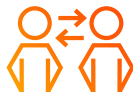
Testování odolnosti

- Každoroční testování všech kritických systémů IKT
- Pokročilé penetrační testování na základě hrozeb každé 3 roky
- Spolupráce s poskytovateli služeb



Řízení rizik poskytovatelů IKT

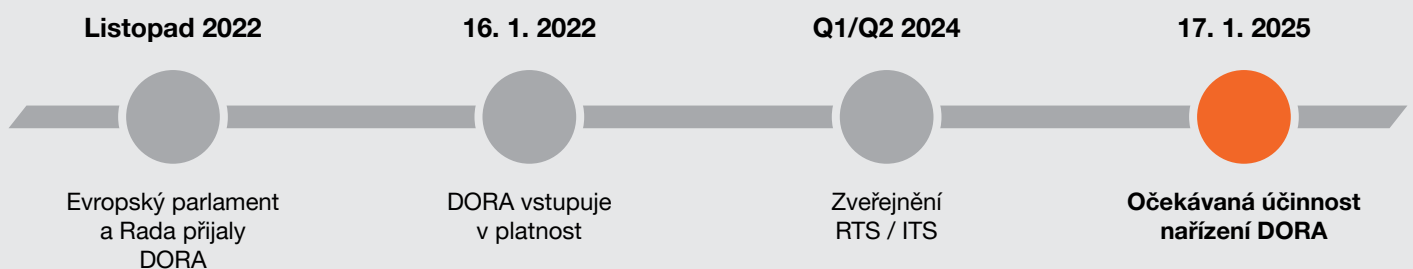
- Hlášení kompletního outsourcingového registru a změn
- Zajištění kompletního monitoringu služeb třetích stran
- Hodnocení rizika koncentrace a sub-outsourcingu



Sdílení informací

- Opatření pro výměnu informací o hrozbách
- Spolupráce mezi důvěryhodnými komunitami finančních subjektů
- Procesy kontroly sdílených informací

Časový harmonogram



Doporučujeme následující kroky, abyste byli připravení a odolní vůči DORA

1

Pochopení DORA

1–2
týdny

Proč: DORA je komplexní nařízení a může se překrývat s jinými již platnými předpisy. Jasné pochopení požadavků je zásadním prvním krokem.

Jak Vám může PwC pomoci:

- Poskytování zaměřených workshopů, upskilling a školení pro lepší porozumění DORA
- Scoping Vašeho programu DORA a provedení počáteční analýzy dopadu
- Sdílení aktuálních poznatků z širší perspektivy trhu



**Pravidelný, úzký
kontakt s regulačními
orgány**

2

Hodnocení vyspělosti vůči DORA

Q1/Q2
2023

Proč: Pochopení klíčových mezer ve vyspělosti je stěžejní pro zajištění efektivního a strategického plánování odolnosti.

Jak Vám může PwC pomoci:

- Definování rozsahu projektu s přihlédnutím k souladu se stávajícími předpisy

1. „Bottom-up“ hodnocení vyspělosti na základě řízených rozhovorů a analýz



2. „Top-down“ strategické plánování odolnosti a cesty k ní



**Spojování
regulačních bodů**

3

DORA plán

Q1/Q2
2023

Proč: Vytvoření plánu s cílem dosáhnout vhodné pozice pro plnění požadavků DORA.

Jak Vám může PwC pomoci:

- Stanovení priorit pro mezery a doporučení na základě zkušeností ze spolupráce s regulačními orgány.
- Vývoj vhodného rámce pro DORA
- Hledání potenciálu pro optimalizaci a zefektivnění procesů



**Odborná
strategie**

4

Implementace DORA

2023
–
2025

Proč: Během dvouletého období příprav bude potřeba zvážit, implementovat a demonstrovat mnoho věcí.

Jak Vám může PwC pomoci:

- Od strategické a operativní koncepce až po technickou realizaci



**Vlastní nástroje
a technická řešení**



Náš pohled na DORA pro české subjekty: Evoluce spíše než revoluce

- DORA se zabývá mnoha tématy, která jsou již v České republice zohledněna **stávajícími předpisy**.
- **Některá témata**, jako je například threat intelligence či threat-led penetrační testování, mají nový charakter, a **vyžadují proto zvýšenou pozornost**.
- Další výzvou, kterou vidíme, je **schopnost vytvořit kompletní viditelnost a pochopit všechny klíčové závislosti** mezi Vaším subjektem a Vašimi kritickými poskytovateli IKT služeb.

Doporučujeme, aby nařízení DORA bylo spouštěčem pro zlepšení Vaší digitální provozní odolnosti bez ohledu na to, kde se z hlediska vyspělosti právě nacházíte.

Již jsme podpořili řadu klientů v jejich úsilí o kybernetickou bezpečnost a odolnost. Subjekty, které dodržují současné regulační požadavky v souladu se současnými auditorskými postupy, mohou mít lepší pozici k implementaci většiny požadavků DORA. Přesto říkáme: **efektivita je klíčová** – jak pro **dosažení požadované odolnosti**, tak pro **zajištění souladu s požadavky DORA**.

Kontaktujte nás



Petr Špiřík
Partner
+420 774 191 101
petr.s.pirik@pwc.com



Ondřej Linhart
Manager – DORA expert
+420 732 633 983
ondrej.linhart@pwc.com



Petr Simsa
Manager – DORA expert
+420 735 701 568
petr.simsa@pwc.com