Deloitte.

# DORA: Seznamte se s nařízením o digitální provozní odolnosti

## Jakby měly finanční instituce zohlednit nová pravidla ve svých strategiích?

Zákonodárci EU ratifikovali nařízení o digitální provozní odolnosti (známé jako DORA). Nařízení bylo publikováno v Úředním věštníku Evropské unie dne 27. prosince 2022, v platnost vstupuje dne 16. ledna 2023. Od této chvíle se finanční instituce, na které se nařízení vztahuje, musí nejpozději do 24 měsíců začít novými pravidly řídit v praxi. Tento čas by měly využít a připravit se nejen na výzvy, které aktuální znění nařízení přináší, ale i zhodnotit širší strategické důsledky této regulace.

DORA je stěžejní iniciativou EU v oblasti digitální provozní a kybernetické odolnosti v sektoru finančních služeb. Nařízení zavádí jednotný soubor regulatorních a dohledových pravidel pro provozní odolnost informačních a komunikačních technologií ve finančním sektoru. Mimo jiné vyžaduje po finančních institucích významné investice do zlepšení odolnosti vůči digitálním a kybernetickým rizikům.

Nové povinnosti budou vyžadovat především změnu přístupu vedoucích orgánů - ty budou mít za úkol posílit odolnost institucí vůči digitálním hrozbám, které se budou dynamicky vyvíjet, a minimalizovat zranitelnost obchodních modelů. Vedoucí orgány finančních institucí, ICT risk management a další lídři finančních institucí sehrají důležitou roli při vedení interních změn v reakci na požadavky DORA, jejich implementaci a při přijímání strategických investičních rozhodnutí nezbytných pro budování odolnosti.

Detailní technické dohody o obsahu DORA dosáhli vyjednavači EU v létě 2022. Naši analýzu této dohody v rámci tzv. „pěti pilířů" DORA naleznete v našem článku z července 2022, kde se dočtete o pěti strategických bodech, které budou muset finanční instituce vzít v úvahu při implementaci a zavádění DORA do praxe.

# Strategické oblasti pro finanční instituce vyplývající z nařízení DORA

## 1. Koncept „provozní odolnosti" bude pro finanční instituce znamenat změnu přístupu

Nařízení DORA poprvé přináší do regulatorního rámce EU v oblasti FSI perspektivu provozní odolnosti. Nahrazuje tak dosavadní mozaiku pokynů zaměřených na kybernetická a IT rizika novým, holistickým přístupem k budování odolnosti vůči digitálním hrozbám. Jde však o víc než jen o změnu terminologie - provozní odolnost přesahuje tradiční přístupy k řízení rizik používané v oblastech kybernetických rizik, IT rizik a kontinuity podnikání. Nutí totiž finanční instituce k tomu, aby předpokládaly, že závažným narušením se nelze vyhnout (bez ohledu na to, jak silnou má instituce ochranu), a aby do provozního modelu svých nejdůležitějších služeb nebo funkcí integrovaly vyšší úroveň odolnosti vůči takovým narušením. Tento přístup povede k nastavení průběžného dialogu mezi institucemi, regulátory a dohledovými orgány.

Vývoj výše popsaného přístupu znamenal ve Velké Británii (která zavedla svůj regulatorní rámec provozní odolnosti v březnu 2022), že instituce si musely stanovit vysoké referenční hodnoty pro svou budoucí odolnost. A aby těmto cílům dostály, budou se muset připravit na značné investice. Příklad Velké Británie rovněž ukázal, že bude potřeba více posílit (případně vytvořit) mezi-sektorovou spolupráci pro řešení globálních otázek v souvislosti s provozní odolností, které nelze efektivně řešit na úrovni jednotlivých institucí. Bude proto potřeba, aby finanční sektor projevil iniciativu při vývoji metod řešení rizik koncentrace vůči třetím stranám, postupů testování třetích stran a sdílení informací o hrozbách v reálném čase.

## 2. Posílení odpovědnosti vedoucích orgánů za provozní odolnost

Nařízení DORA stanovuje, že za provozní odolnost instituce je zodpovědné její představenstvo. Vrcholový management bude tedy muset převzít vedoucí úlohu při implementaci nejdůležitějších složek DORA. V praxi tak budou muset členové představenstva a vrcholového vedení schválit soubor klíčových plánů, jako je strategie digitální provozní odolnosti firmy a její politika týkající se třetích stran v oblasti ICT. Kromě toho budou vedoucí orgány zodpovědné také za přijímání rozhodnutí o provozním modelu, která jsou nezbytná k začlenění požadavků DORA do každodenní činnosti institucí. Konkrétně bude nově v jejich kompetenci stanovovat úrovně tolerance rizik a rozhodovat o tom, jak stanovit priority nápravných opatření s cílem řešit zjištěné provozní nedostatky.

Po zavedení DORA bude pro vedoucí orgány stále důležitější prokázat orgánu dohledu, že jejich instituce jsou odolné vůči hrozbám specifickým pro danou instituce i obecným hrozbám v daném odvětví. Budou muset dobře rozumět připravenosti firmy vyrovnat se s možným narušením ICT a zároveň zachovat kontinuitu služeb. Budou muset prokázat, že: učinili správná manažerská rozhodnutí; řádně přezkoumali plány odolnosti a následně posílili odolnost instituce. Pravidelné informace vedoucím orgánům o hrozbách a zranitelnostech vycházejících z vnějšího prostředí bude třeba dynamicky zohlednit v celkové odolnosti firmy.

## 3. Průběžné povinnosti budou ovlivňovat opatření institucí i po skončení období implementace

Implementační lhůta 24 měsíců bude pro většinu finančních institucí (včetně těch velkých a sofistikovaných) výzvou v mnoha oblastech, mimo jiné v otázkách pokročilého testování, hlášení incidentů, impact assessmentu a dalších. Nařízení DORA nicméně zavádí také průběžný způsob řízení odolnosti založený na průběžném přezkumu. Finanční instituce tak budou mít povinnost provádět průběžné testování odolnosti a vyhodnocování rizik a vhodnosti svých plánů odolnosti. Budou také muset průběžně shromažďovat informace o hrozbách, aby splnily novou povinnost hlášení hrozeb a incidentů, a také vypracovávat vlastní rizikové scénáře. Nařízení DORA vyžaduje, aby instituce určily kritické nebo významné funkce (CIF) jako ústřední bod strategie vyhodnocení, kterou musí projít při budování své odolnosti, zejména pokud jde o identifikaci hrozeb a testování scénářů.

Hlavním záměrem nařízení DORA je skrze nastavení trvalé regulatorní povinnosti přimět firmy, aby dosáhly takové provozní odolnosti, která se bude schopna dostát neustále se měnícím nárokům podle toho, jak se budou formovat hrozby a oblasti zranitelnosti. Díky investicím do strategických schopností, jako je zjišťování hrozeb a testování odolnosti, budou vedoucí orgány lépe vybaveny nejen k tomu, aby pochopily, jak mohou scénáře ovlivnit kritické funkce jejich firmy a vést k dalším následným dopadům, ale také, jaké investice bude třeba vynaložit k dosažení dostatečné úrovně připravenosti. Strategické schopnosti tohoto druhu budou navíc klíčové i pro efektivní reakci na případná nepředvídaná narušení, protože vedoucí orgány budou mít hlubší a podrobnější znalosti o základní struktuře a fungování své instituce.

## 4. Předpokládaný dopad na strategie firem v oblasti outsourcingu

Řešení zranitelnosti třetích stran je hlavní výzvou při posilování provozní odolnosti i pro britské firmy, které jsou na cestě k provozní odolnosti dále. Nařízení DORA zavádí rámec dohledu nad kritickými třetími stranami (CTP) jako první na světě, rozšiřuje rozsah regulatorních perimetru finanční regulace a uděluje evropským orgánům dohledu (ESA) nové pravomoci k dohledu nad CTP a řešení rizik pro odolnost finančního sektoru EU. Regulatorní orgány EU nicméně jasně uvedly, že to nijak nesnižuje individuální odpovědnost finančních institucí, pokud jde o outsourcing. Nařízení DORA skutečně ukládá finančním institucím několik nových požadavků na řízení rizik třetích stran, které budou ještě přísnější, pokud třetí strany podporují poskytování kritické funkce či služby. To se může stát obzvláště důležité pro poskytovatele z řad FinTech či digitálních společností, jejichž závislost na určitých digitálních platformách je může vystavit větším ICT rizikům třetích stran a vyvolat podrobnější dohled nad tímto rizikem.

Finanční instituce by také měly věnovat zvláštní pozornost požadovanému posouzení rizika koncentrace. Oblasti zranitelnosti, které mohou být z těchto vyhodnocení identifikovány (nadměrná závislost na jediném externím poskytovateli, kritičnost obsluhovaných funkcí atd.), mohou pro finanční instituce znamenat zvýšenou intenzitu kontrol ze strany orgánů dohledu. Tato situace může následně vyvinout tlak na vedoucí orgány, aby přezkoumaly svá strategická rozhodnutí týkající se jejich ochoty podstupovat riziko při navazování vztahů s třetími stranami. Lídři firem by se měli zaměřit také na role interních oddělení a zaměstnanců, kteří mají na starosti řízení rizik a zadávání zakázek s ohledem na jejich ochotu podstupovat riziko v provozních modelech instituce. Vedoucí orgány mohou také zvážit řešení identifikovaných rizik koncentrace tím, že přistoupí k nápravným opatřením, jako je přijetí strategie pro více dodavatelů.

## 5. Oblast provozní odolnosti jako klíčový faktor investičních rozhodnutí na úrovni vedoucích orgánů instituce

Budování provozní odolnosti v instituci vyžaduje, aby byla tato oblast zakotvena jako klíčový faktor při rozhodování o byznysové strategii a navrhování změn obchodního modelu. Přesněji řečeno, finanční instituce budou mít za úkol stanovit požadovanou úroveň odolnosti v rámci vývoje strategie digitální provozní odolnosti vyžadované DORA, což přiměje vedoucí orgány více se zapojit do rozhodování o rizicích a odolnosti. Vedoucí orgány a ředitelé obchodních oddělení budou muset jednak pochopit obchodní důvody pro investice do schopnosti provozní odolnosti, jednak budou muset umět vyjádřit, jak jsou počáteční náklady vyváženy tím, že nastaví provozní model, který v průběhu času obstojí při rostoucí regulatorní kontrole. Aby toto bylo v praxi proveditelné, měly by vedoucí orgány upřednostnit oblasti, které budou v průběhu implementace DORA v popředí zájmu orgánů dohledu. Jde například o požadavky, které vyžadují pravidelné výstupy (např. výběr CIF, impact assessment, postupy testování odolnosti, výstupy z rámce pro hlášení incidentů atd.).

Vedoucí orgány by měly mít na paměti, jak by orgány dohledu mohly interpretovat zásadu proporcionality obsaženou v DORA. Je pravděpodobnější, že větší podniky budou mít v určitých oblastech pokročilejší schopnosti (např. testování odolnosti), ale budou také podléhat mnohem širší úrovni kontroly vzhledem k potenciálnímu systémovému významu jejich klíčových služeb. Menší podniky mohou naopak těžit z méně přísných požadavků (např. nemusí provádět pokročilé testování TLPT, využívat zjednodušený rámec řízení rizik v oblasti ICT atd.), ale přesto mohou čelit značným investičním nárokům na vybudování kapacit potřebných k dosažení souladu s těmi částmi nařízení, které jsou aplikovány na celý sektor jednotně (jako je například požadavek na hlášení incidentů v oblasti ICT a ustanovení o řízení rizik třetích stran).

# Sečteno a podtrženo

Nařízení DORA není pouhým „jednorázovým compliance cvičením na dodržování předpisů“. Jeho cílem je naopak pomoci finančním institucím, aby zůstaly dlouhodobě odolné vůči stále se měnícím hrozbám ve stále složitějším technologickém prostředí.

Přestože evropské orgány dohledu musí ve dvouletém implementačním období ještě zapracovat značnou část sekundárních předpisů DORA a vyjasnit očekávání týkající se odolnosti, je již nyní jasné, že se od vedoucích orgánů firem očekává, že se ujmou klíčové role při vytváření odolnosti a že převezmou větší díl odpovědnosti za zásadní rozhodnutí. Bude důležité nastavit silný „tone from the top“ – signál, který jasně definuje důležitost provozní odolnosti a který regulatorní orgány, investoři a další zúčastněné strany vezmou na vědomí, protože provozní hrozby v sektoru finančních služeb jsou na vzestupu.

# Jak vám můžeme pomoci?

**Odborníci ze společnosti Deloitte jsou připraveni podpořit finanční instituce při vytváření pevných pilířů provozní odolnosti, jak je navrhováno a požadováno nařízením DORA. Nabízíme komplexní služby zahrnující kompletní proces od readiness analýzy až po její implementaci, a to vše přesně na míru vašim potřebám.**

- Rámec řízení rizik. Aby instituce splnily požadavky DORA, budou muset mít zavedeny spolehlivé procesy řízení rizik. Deloitte vám pomůže sladit obchodní strategie a (nejen) kybernetická rizika vaší organizace a udržovat komplexní a účinný rámec jejich řízení.
- Hlášení incidentů. Cílem nařízení DORA je harmonizovat procesy klasifikace a hlášení incidentů. Zásadní význam má včasné odhalení incidentů a rychlá reakce. Našim klientům proto pomáháme přizpůsobit se novým pravidlům EU v oblasti podávání zpráv a sladit v tomto směru interní procesy s cílem optimalizovat přidělování zdrojů.
- Testování odolnosti. Nařízení DORA vyžaduje, aby finanční instituce testovaly své systémy na základě souvisejících rizik. To zahrnuje screening zranitelností a penetrační testy, stejně jako robustní testování kontinuity podnikání.
- Penetrační testování na základě hrozeb (TLPT) pro kritické hráče. Kybernetická praxe společnosti Deloitte ve střední Evropě poskytuje nejkvalitnější služby penetračního testování svého druhu, a to díky našim vysoce kvalifikovaným odborníkům a technologickému zázemí.
- Sdílení analýzy hrozeb. Aktivity v oblasti kybernetických hrozeb se často vztahují na více organizací ve finančním sektoru současně. Nařízení DORA, které se zaměřuje na sdílení informací o hrozbách, pomůže celému sektoru stát se zodpovědnějším a aktivnějším v obraně proti rostoucímu počtu kybernetických útoků. Našim klientům proto pomáháme s vývojem a integrací procesu sdílení informací o těchto hrozbách.
- Řízení rizik třetích stran (TPRM) a monitorování. Instituce by měly posoudit, zda jejich strategie a plány reakce a obnovy rovněž relevantním způsobem reagují na rozšířená pravidla vztahující se na řízení rizik v oblasti IKT. TPRM rámec společnosti Deloitte je založen na špičkových postupech a vychází z globálních regulatorních požadavků. Poskytujeme tak našim klientům komplexní řešení při řízení procesů, postupů a aktivit v rámci ekosystémů třetích stran. Díky implementaci TPRM platformy budou naši klienti využívat všech výhod komplexní technologické platformy, která kombinuje mobilní sběr dat, nástroje pro zlepšení výkonu na podnikové a jednotkové úrovni a analytický reporting.

Více informací o našich službách najdete na našich webových stránkách

# Kontaky

**Martin Kubačka**
**Partner**
mkubacka@deloittece.com
+420 776 306 694

**Jakub Höll**
**Director**
jholl@deloittece.com
+420 734 353 815

**Martin Antoš**
**Manager**
mantos@deloittece.com
+420 734 783 919

**Štěpán Pekárek**
**Manager**
spekarek@deloittece.com
+420 778 764 214