

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

Outsourcing ICT služeb dle nařízení DORA

Za jednu z rizikových oblastí v rámci kybernetické bezpečnosti lze považovat využívání třetích osob k poskytování ICT služeb. Tento outsourcing s sebou nese novou vrstvu rizik, a to zvláště v situacích, kdy poskytované služby jsou zásadní pro činnost finančního subjektu a vytváří určitou formu závislosti. V praxi se může jednat např. o poskytovatele softwaru, cloudu či datových služeb.

Nařízení DORA (Digital Operational Resilience Act)[\[1\]](#) oblast outsourcingu specificky upravuje, když vedle vymezení samotného poskytovatele ICT služeb, nastavení odpovědnosti, vedení registru informací atd., stanoví též požadavky na předsmuvní a smluvní fázi vztahu s poskytovatelem ICT služeb.

Vymezení základních pojmů, řízení rizik

Nařízení DORA rozeznává několik skupin poskytovatelů ICT služeb, když vymezuje nejen „standardního“ poskytovatele z řad třetích osob, ale též specifické poskytovatele typu poskytovatele v rámci skupiny, kritického poskytovatele či poskytovatele usazeného ve třetí zemi.[\[2\]](#) Společným je pro tyto poskytovatele poskytování ICT služeb tzv. finančním subjektům, mezi které patří např. banky, pojišťovny, obchodníci s cennými papíry či obhospodařovatelé investičních fondů.[\[3\]](#)

Vymezení ICT služeb v nařízení je poměrně široké a rozumí se jimi digitální a datové služby poskytované prostřednictvím ICT systémů včetně hardware jako služby a hardwarových služeb, které zahrnují poskytování technické podpory prostřednictvím aktualizací s výjimkou tradičních analogových telefonních služeb.[\[4\]](#)

V rámci řízení rizik jsou finanční subjekty (se stanovenými výjimkami) zejména povinny přijmout a přezkoumávat strategii pro riziko související s outsourcingem ICT služeb.[\[5\]](#) Důležitou součástí řízení rizik spojených s outsourcingem ICT služeb je také jeho odpovídající smluvní zajištění. Nařízení v tomto ohledu upravuje nejen některé obsahové náležitosti samotné smlouvy o poskytování ICT služeb, ale též samotný kontraktační proces.

Předsmuvní fáze

Nařízení DORA v rámci předsmuvní fáze požaduje, aby finanční subjekty zejména s náležitou péčí prověřily potenciální třetí strany, posoudily, zda se budoucí smlouva týká využívání ICT služeb podporujících zásadní nebo důležité funkce, identifikovaly relevantní rizika a možnosti střetu zájmů a zvážily riziko koncentrace ICT služeb.

Finanční subjekty by vždy měly uzavřít příslušnou smlouvu pouze s poskytovatelem, který splňuje požadavky na bezpečnost informací. Samotná předsmuvní fáze tak může být poměrně náročným cvičením, a to jak po časové, tak finanční stránce.

Obsah smlouvy

Vedle formálních požadavků na smlouvu[\[6\]](#) stanoví nařízení DORA též požadavky obsahové.[\[7\]](#)

Smlouva o poskytování ICT služeb by tak měla zejména obsahovat:

- a. srozumitelný a úplný popis všech funkcí a ICT služeb včetně popisu úrovně služeb;
- b. místa, kde mají být ICT služby poskytovány a kde mají být zpracovávána data včetně povinnosti poskytovatele ICT služeb oznámit finančnímu subjektu plán na změnu těchto míst;
- c. ustanovení týkající se dostupnosti a důvěrnosti ohledně ochrany údajů včetně osobních údajů;
- d. povinnost poskytovatele ICT služeb poskytnout finančnímu subjektu pomoc, dojde-li k ICT incidentu, a povinnost spolupracovat s příslušnými orgány dohledu;
- e. ustanovení ohledně ukončování smlouvy včetně úpravy minimální výpovědní doby.

Nařízení DORA dále upravuje též specifické a podrobnější nároky na obsah smluv týkajících se zásadních či důležitých funkcí včetně závazku poskytovatele ICT služeb uplatňovat a testovat plány zachování provozu a přijmout taková opatření, která zajistí bezpečnost poskytovaných služeb v souladu s regulačním rámcem finančního subjektu či práva finančního subjektu na neomezený přístup, kontrolu a audit poskytovatele ICT služeb.

Z požadovaných ustanovení smluv o poskytování ICT služeb se podrobněji zaměříme na již zmíněné povinné ustanovení ohledně ukončování těchto smluv. Vedle samotné preambule^[8] upravuje nařízení DORA ukončování smluv v samostatných ustanoveních, která poměrně podrobně upravují celou problematiku s cílem limitovat rizika na straně finančního subjektu, a to zejména riziko přerušení jím poskytovaných služeb. V ustanoveních týkajících se ukončení smlouvy o poskytování ICT tak je třeba mimo jiné upravit možnost ukončit smlouvu, pokud:

- a. poskytovatel ICT služby poruší právní předpisy či smlouvu zásadním způsobem;
- b. v rámci řízení rizika jsou zjištěna slabá místa s ohledem na dostupnost, integritu a důvěrnost údajů;
- c. orgán dohledu není schopen efektivně dohlížet na finanční subjekt v důsledku sjednaných podmínek smlouvy.

V případě ICT služeb zajišťujících zásadní či důležité funkce jsou finanční subjekty povinny zavést tzv. strategie ukončení smluvního vztahu, v rámci kterých zohlední např. riziko selhání či snížení kvality poskytovaných služeb. Finanční subjekty musí být schopny ukončit smlouvu takovým způsobem, aby nedošlo k narušení jejich činnosti, narušení regulatorních požadavků či zhoršení kontinuity a kvality služeb poskytovaných klientům. Vzhledem k tomu, že zásadní rizika mohou vznikat při změně poskytovatele ICT služeb, jsou finanční subjekty povinny vypracovat tzv. plány přechodu, které umožní bezpečný a integrovaný přenos dat k novému poskytovateli či jejich začlenění v rámci finančního subjektu samotného.

Vedení registru informací

Nařízení DORA požadované vedení registru informací lze považovat za další příspěvek do již tak rozsáhlého katalogu formalit, jejichž praktický význam je snad s výjimkou případu tzv. kritických poskytovatelů ICT služeb minimálně pochybný.

Vedení registru informací týkajícího se všech smluvních ujednání o využívání ICT služeb poskytovaných třetími osobami považuje nařízení za součást rámce pro řízení rizika.

Nařízení požaduje, aby smlouvy byly řádně zdokumentovány a bylo rozlišeno mezi ICT službami, které podporují zásadní či důležité funkce a ostatními službami.[9] K žádosti jsou finanční subjekty povinny registr informací či jeho část poskytnout regulátorovi. Finanční subjekty jsou dále povinny zajistit, aby informace uvedené v registru byly zejména přesné, úplné a konzistentní.[10]

Závěrem ohledně odpovědnosti a proporcionality

Pokud v důsledku outsourcované ICT služby dojde k porušení povinností finančního subjektu stanovených nařízením, nese plnou odpovědnost za toto porušení finanční subjekt. Případná smluvní odpovědnost poskytovatele ICT služby vůči finančnímu subjektu tím samozřejmě není dotčena. Z tohoto důvodu lze ve smlouvě doporučit maximálně podrobnou úpravu odpovědnostních ustanovení, včetně např. sjednání motivačních smluvních pokut.

Též v případě outsourcingu se uplatní nařízením DORA zdůrazňovaná zásada proporcionality. Při sledování rizik souvisejících s poskytováním ICT služeb tak je třeba vždy vzít do úvahy zejména důležitost poskytovaných služeb a posoudit potenciální dopad na kontinuitu a dostupnost finančních služeb.[11] Vzhledem k rozsahu nově stanovených povinností nezbývá než doufat, že regulátoři budou zásadu proporcionality opravdu aplikovat a vyvarují se extenzivního výkladu nařízení.



JUDr. Jiří Kokeš, Ph.D.,
vedoucí advokát

AegisLaw

[Aegis Law, advokátní kancelář, s.r.o.](#)

Jungmannova 26/15
110 00 Praha 1

Tel: +420 777 577 562
e-mail: office@aegislaw.cz

[1] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. 12. 2022, o digitální provozní odolnosti finančního sektoru (dále jen „nařízení DORA“ či „nařízení“). Z prováděcích nařízení viz zejména nařízení Komise 2024/1773 ze dne 13. 3. 2024, které upravuje obsah politiky ohledně smluvních ujednání o využívání ICT služeb podporujících zásadní a důležité funkce a nařízení Komise 2024/2956 ze dne 29. 11. 2024, které upravuje standardní vzory pro registr informací ohledně smluv uzavřených s poskytovateli ICT služeb (dále jen „prováděcí nařízení o registru“).

[2] Viz čl. 3 odst. 19, 20, 23 a 28 nařízení DORA.

[3] Viz čl. 2 nařízení DORA.

[4] Viz čl. 3 odst. 21 nařízení DORA.

[5] Viz čl. 28 odst. 2 nařízení DORA.

[6] Detail nařízení DORA může v této souvislosti působit až trochu komicky – smlouva musí být dle nařízení písemná a vyhotovená v jednom dokumentu s tím, že tento dokument musí být stranám dostupný v papírové podobě nebo v podobě dokumentu v jiném formátu, který lze stáhnout, je trvalý a přístupný. Viz čl. 30 odst. 1 nařízení DORA.

[7] Viz čl. 30 nařízení DORA.

[8] Viz např. čl. 66 a 74 preambule nařízení DORA.

[9] Viz čl. 28 odst. 3 nařízení DORA.

[10] Viz čl. 3 prováděcího nařízení o registru.

[11] Viz čl. 28 odst. 1 nařízení DORA.

© EPRAVO.CZ – Sběrka zákonů, judikatura, právo | www.epravo.cz

Další články:

- [Kupní smlouva k nemovité věci bez určení kupní ceny: Nejvyšší soud koriguje katastrální praxi](#)
- [Společnost s podíly 50:50 – právní rizika patových situací a jejich smluvní řešení](#)
- [Byznys a paragrafy, díl 34: Jednání za společnost – prokura](#)
- [Jak nastavit smlouvy s dodavateli podle nové právní úpravy kybernetické bezpečnosti?](#)
- [Jak soutěžní právo reaguje na pohlcování startupů technologickými giganty aneb fenomén](#)

vražedných akvizic

- Žaloba na fair exit vůči společníkům s. r. o. jednajícím ve shodě
- Reklamáce 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?