Třídící znak							
2	0	8	1	6	5	6	0

ÚŘEDNÍ SDĚLENÍ ČESKÉ NÁRODNÍ BANKY

ze dne 19. srpna 2016

k výkonu činnosti na finančním trhu – cloud computing

I. Účel a vymezení pojmů

1. Účelem tohoto úředního sdělení je informovat subjekty uvedené v článku II o přístupu České národní banky k využívání cloud computingu dohlíženými subjekty při výkonu dohledu nad finančním trhem.

2. Pro účely tohoto úředního sdělení se pod pojmem cloud computing rozumí model uplatňovaný v oblasti informačních a komunikačních systémů a technologií, který umožní získat síťový přístup ke konfigurovatelným výpočetním prostředkům (např. sítě, servery, datová úložiště, aplikace a služby), které jsou sdíleny větším množstvím uživatelů a jejichž kapacita je poskytována a opět uvolňována s minimálními nároky na jejich správu anebo na intervenci poskytovatele cloud computingu[1]. V právních předpisech finančního trhu se pojem cloud computing nevyskytuje[2].

3. Toto úřední sdělení navazuje na úřední sdělení České národní banky ze dne 10. prosince 2010 k výkonu činnosti na finančním trhu: Kvalitativní požadavky související s výkonem činnosti – základní informace a na úřední sdělení České národní banky ze dne 27. května 2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému.

II. Působnost

4. Úřední sdělení se týká banky, spořitelního a úvěrního družstva, tuzemské pojišťovny a tuzemské zajišťovny (dále jen „poskytovatel finančních služeb“).

5. Úřední sdělení je využitelné jako metodická pomůcka i dalšími osobami, které podléhají dohledu České národní banky podle zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů, pokud využívají nebo zamýšlí využívat cloud computing.

[1] Vymezení pojmu „cloud computing“ zohledňuje definici Národního ústavu pro normalizaci a technologie USA NIST (2009), která zní: „*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*“ (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf).

[2] Toto úřední sdělení zachycuje právní stav k 10. srpnu 2016. Vzhledem k možným změnám legislativy je třeba při aplikaci tohoto úředního sdělení přihlédnout k aktuálnímu právnímu stavu.

6. Úřední sdělení obsahuje informace týkající se i jiných osob, jmenovitě poskytovatelů cloud computingu.

III. Východiska, zásady

7. Právní předpisy upravující výkon činnosti na finančním trhu nezakazují využívání cloud computingu. Povinností poskytovatele finančních služeb však je zajistit soulad vykonávaných činností se všemi relevantními požadavky právních předpisů, zejména zajistit soustavně řádný a obezřetný výkon své činnosti na finančním trhu i v případě využívání cloud computingu.

8. Využívání cloud computingu v rámci řídicího a kontrolního systému poskytovatele finančních služeb[3] naplňuje veškeré znaky outsourcingu, tj. zajištění výkonu určitých funkcí nebo činností poskytovatele finančních služeb jinou osobou. V právních předpisech je „outsourcing“ označován různými pojmy, např. „externí zajištění činností“ nebo „činnosti vykonávané prostřednictvím jiné osoby“.

9. Příslušné evropské orgány a předpisy potvrzují bezrozpornost regulací outsourcingu stanovených pro sektor pojišťovnictví, sektor úvěrových institucí a sektor kapitálového trhu[4].

10. Při využívání cloud computingu poskytovatelem finančních služeb a při výkonu jeho dohledu se uplatňuje zásada přiměřenosti[5]. Podle zásady přiměřenosti není poskytovatel finančních služeb oprávněn zcela vyloučit uplatnění kteréhokoli z pravidel obsažených v právních předpisech, ale způsob jejich uplatnění by měl odpovídat povaze, rozsahu a komplexnosti dotčených činností, souvisejícím rizikům a dalším relevantním okolnostem případu.

IV. Závěrečná ustanovení

11. Podrobnější informace České národní banky ke cloud computingu jsou obsaženy v příloze tohoto úředního sdělení.

12. Vzhledem k dynamickému rozvoji informačních a komunikačních systémů a technologií je nezbytné soustavně přihlížet k vývoji prostředí, ve kterém poskytovatel finančních služeb a poskytovatel cloudových služeb podnikají, zejména k vývoji technologického a právního prostředí, k vývoji regulatorního rámce a k vývoji v oblasti uznávaných standardů a praxí ohledně cloud computingu[6].

---

[3] Např. § 7 zákona č. 277/2009 Sb., o pojišťovnictví, ve znění pozdějších předpisů, § 8b zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů a § 7a zákona č. 87/1995 Sb., o spořitelních a úvěrních družstvech, ve znění pozdějších předpisů.

[4] Např. bod 37 preambule Směrnice 2009/138/ES o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II), bod 18 Obecných pokynů Evropského orgánu pro bankovnictví k internal governance (řídicí a kontrolní systém) (GL 44) (EBA BS 2011 116) ve spojení s CEBS Guidelines on outsourcing (2010), str. 1 a 2 (dostupné pouze v angličtině).

[5] Např. čl. 29(3) a čl. 41(2) ve spojení s bodem 19 a bodem 31 preambule Směrnice 2009/138/ES a čl. 74(2) Směrnice 2013/36/EU o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES.

[6] Např. European Union Agency For Network And Information Security (ENISA): Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations; prosinec 2015

13. Toto úřední sdělení nabývá účinnosti dnem vyhlášení ve Věstníku České národní banky.

Viceguvernér
Ing. Mojmír Hampl, MSc., Ph.D. v. r.

Příloha

Sekce regulace a mezinárodní spolupráce na finančním trhu
Odpovědný zaměstnanec:
Ing. Věra Mazánková, tel. 224 412 821

(https://www.enisa.europa.eu/publications/cloud-in-finance); Australian Prudential Regulation Authority (APRA): Information paper on outsourcing involving shared computing services, including cloud; červenec 2015 (http://www.apra.gov.au/mediareleases/pages/15_17.aspx).

Příloha

Podrobnější informace o přístupu České národní banky ke cloud computingu

Obecné informace

1. Povinnou součástí řídicího a kontrolního systému poskytovatele finančních služeb je informační a komunikační systém[1], který je přiměřený, funkční a efektivní jako celek i v jednotlivých součástech.

2. Pokud se poskytovatel finančních služeb rozhodne některou funkci nebo činnost, kterou by jinak mohl vykonávat sám, zajišťovat na základě vzájemného ujednání prostřednictvím jiné osoby za použití cloud computingu, jedná se o outsourcing[2].

3. I v případě využívání outsourcingu zajišťuje řídicí a kontrolní systém poskytovatele finančních služeb soustavně řádný a obezřetný výkon činností včetně plnění právních povinností poskytovatele finančních služeb např. pokud jde o řízení rizik, mechanismy vnitřní kontroly, toky informací, pravidla ochrany osobních údajů a zajišťování kybernetické bezpečnosti.

Přiměřenost

4. S ohledem na povahu zpracovávaných dat a operací, míru komplexnosti využívání cloud computingu, konkrétní osobu poskytovatele cloud computingu a další relevantní skutečnosti a okolnosti lze přiměřeně zmírnit nebo modifikovat plnění regulatorních požadavků na outsourcing[3]. To platí i pro uplatňování požadavků právních předpisů na řetězení outsourcingu[4]. Zmírnění nebo modifikace jsou akceptovatelné např. jde-li o informační a komunikační systémy na podporu spolupráce a sdílení informací pouze v rámci poskytovatele finančních služeb anebo v rámci skupiny, jejímž je členem, nebo o uložení nebo zpracovávání veřejně dostupných dat. Pokud by však byl výsledný stav, i s přihlédnutím k zásadě přiměřenosti, v nesouladu s povinnostmi poskytovatele finančních služeb stanovenými právními předpisy, poskytovatel finačních služeb k využití cloud computingu v dané oblasti by neměl přistoupit.

Posuzování orgánem dohledu

5. Česká národní banka posuzuje při výkonu dohledu nad poskytovatelem finančních služeb, který využívá nebo zamýšlí využívat cloud computing, včetně případného využívání cloud computingu poskytovatelem finančních služeb na základě smluvního ujednání v rámci skupiny, jejímž je členem, zda poskytovatel finančních služeb

   a) ve svých strategiích[5] vymezuje dostatečně jasně a konkrétně celkový přístup a hlavní zásady využívání cloud computingu,

   b) ve svých strategiích, zásadách a navazujících předpisech a postupech patřičně zohledňuje specifika vyplývající z povahy cloud computingu včetně zohlednění jejich vlivu na

      1. plnění právních povinností poskytovatele finančních služeb včetně plnění povinností vůči klientům a povinnosti zajištění kontinuity výkonu činností a

[1] Např. čl. 41(2) Směrnice 2009/138/ES, § 23 ve spojení s § 7 odst. 1 písm. d) vyhlášky č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry.
[2] Např. čl. 49 Směrnice 2009/138/ES ve spojení s bodem 28 preambule, § 12 odst. 1 vyhlášky č. 163/2014 Sb.
[3] Např. čl. 49(2) Směrnice 2009/138/ES a čl. 258 Nařízení Evropského parlamentu a Rady (EU) č. 35/2015, kterým se doplňuje směrnice Evropského parlamentu a Rady 2009/138/ES o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II), § 12 a příloha č. 6 a 7 vyhlášky č. 163/2014 Sb.
[4] Např. čl. 274(4) písm. l) Nařízení č. 35/2015, příloha č. 7 bod 8 vyhlášky č. 163/2014 Sb.
[5] Např. čl. 258(2) a (3) Nařízení č. 35/2015, § 18 odst. 1 písm. d) a f) a odst. 2 písm. d) vyhlášky č. 163/2014 Sb.

2. schopnost poskytovatele finančních služeb prokázat plnění svých právních povinností České národní bance včetně doložení uplatňovaných postupů.

6. Česká národní banka zejména posuzuje, zda poskytovatel finančních služeb

   a) patřičně zohledňuje vliv specifik cloud computingu na rozsah, obsah, vysledovatelnost a rekonstruovatelnost informací o řídících a kontrolních procesech poskytovatele cloud computingu,

   b) patřičně zohledňuje vliv specifik cloud computingu na kontrolní činnosti (kontrolovatelnost) a audit outsourcovaných procesů, které provádí poskytovatel cloud computingu, poskytovatel finančních služeb nebo jimi určené nebo akceptované jiné kompetentní osoby,

   c) rozpoznává, posuzuje a adekvátně zohledňuje všechny další významné vlivy specifik cloud computingu, která jsou relevantní pro posouzení rizik souvisejících s daným outsourcingem,

   d) patřičně zohledňuje, že s rostoucí komplexností využívaného cloud computingu obvykle klesá transparentnost a možnosti účinných kontrol takto zabezpečovaných funkcí nebo činností poskytovatelem finančních služeb a přijme vhodná opatření k omezení s tím souvisejících rizik anebo jejich dopadů včetně zvážení možností pojištění, nebo rozhodne o omezení daného outsourcingu a

   e) rozpoznává, posuzuje a adekvátně zohledňuje vliv specifik cloud computingu ve všech fázích životního cyklu[6] daného outsourcingu.

7. Česká národní banka rovněž posuzuje naplnění dalších předpokladů řádného a obezřetného využívání cloud computingu poskytovatelem finančních služeb, zejména zda poskytovatel finančních služeb

   a) posoudil dopady zavedení služeb cloud computingu do stávajícího organizačního uspořádání, stanovených postupů a činností s cílem rozpoznat nová rizika, kterým může být vystaven[7],

   b) patřičně zohledňuje, že využíváním outsourcingu není dotčena konečná odpovědnost poskytovatele finančních služeb za řádný a obezřetný výkon činnosti, a zda za účelem plnění svých právních povinností soustavně disponuje dostatečnými odbornými kapacitami, které uplatňuje pro přípravu, zavedení, řízení a kontrolu celkového využívání cloud computingu i jednotlivých případů jeho využívání,

   c) pravidelně vyhodnocuje, zda jeho vnitřní předpisy upravující oblast cloud computingu a jím skutečně vykonávané činnosti jsou v souladu s právními předpisy, ze kterých mu vyplývají povinnosti, včetně těch povinností, které nejsou v dohledové působnosti České národní banky; jedná se např. o oblast ochrany osobních údajů a kybernetické bezpečnosti,

   d) disponuje ve všech fázích životního cyklu outsourcingového vztahu dostatečnými informacemi o řídících a kontrolních procesech relevantních pro posouzení všech rizik vyplývajících z využívání cloud computingu a rovněž dokumenty a informacemi o vnitřních postupech a opatřeních zavedených u poskytovatele cloud computingu k omezení rizik a zda tyto dokumenty a ostatní dostupné informace umožňují poskytovateli finančních služeb průběžnou identifikaci a hodnocení rizik podstupovaných v souvislosti

[6] Životní cyklus zahrnuje tyto fáze a prvky: příprava smluvního vztahu, vlastní smlouva - kontrakt, provozování a využívání služby, ukončení smluvního vztahu; viz např. obecné pokyny EIOPA k řídicímu a kontrolnímu systému (EIOPA-BoS-14/253), bod 1.116.

[7] Např. čl. 44(1) a (2) písm. e) a f) Směrnice 2009/138/ES, čl. 258 a 260(1)písm. f) a g) Nařízení č. 35/2015, bod 1.3, 1.26, 1.34 d) a 2.121, 2.3 a 2.6 obecných pokynů EIOPA-BoS-14/253, § 34 odst. 1 vyhlášky č. 163/2014 Sb.

s využíváním cloud computingu, hodnocení poskytovatele cloud computingu a jím poskytovaných služeb a také hodnocení efektivity daného outsourcingu,

e) disponuje právem provést přímo nebo zadat kontrolu nebo audit procesů významných pro bezpečnost a dostupnost dat, služeb a outsourcovaných činností na místě u poskytovatele cloud computingu,

f) má ve všech fázích životního cyklu outsourcingového vztahu možnost průběžně a bez zbytečných omezení kontaktovat určené pracovníky poskytovatele cloud computingu, kteří jsou plně kompetentní a poskytovatelem cloud computingu předem pověřeni poskytnout vysvětlení a informace ohledně vnitřních procesů a postupů poskytovatele cloud computingu souvisejících s outsourcovanými funkcemi, daty a službami, a to včetně vysvětlení informací, nálezů a nápravných opatření týkajících se auditních zpráv interního auditora poskytovatele cloud computingu nebo externího posuzovatele cloud computingu, pokud jsou relevantní pro daný outsourcing,

g) má stanoveny a soustavně uplatňuje postupy pro rozpoznávání a řízení rizik spjatých s cloud computingem s tím, že tyto postupy umožňují zajištění zpětné vysledovatelnosti a rekonstruovatelnosti postupů skutečně uplatněných,

h) zajistil provedení analýzy rizik využívání cloud computingu, která je pravidelně a při každé případné významné změně týkající se využívání cloud computingu aktualizována, a zda v analýze rizik jsou rozpoznána specifická rizika cloud computingu minimálně v oblastech organizačních, technických a compliance,

i) využívá analýzu rizik pro účely
   1. přípravy smluvního vztahu,
   2. řízení rizik operačních[8], reputačních, koncentrace a dalších rizik souvisejících s cloud computingem a jeho využíváním a
   3. kontroly poskytovatele outsourcingu např. v oblasti bezpečnostních zásad, bezpečnostního monitoringu a řízení bezpečnostních incidentů,

j) vytvořil bezpečnostní zásady pro cloud computing, ve kterých upřesní hlavní zásady a postupy pro zajištění důvěrnosti, integrity a dostupnosti informací,

k) je informován, ve kterých zemích jsou nebo mohou být uložena jeho data, a rozpoznává a zohledňuje rizika umístění dat,

l) je obeznámen s postupy poskytovatele cloud computingu pro řešení odezvy na případný výskyt událostí (bezpečnostních incidentů), které by ohrozily nebo narušily bezpečnost informačních systémů nebo bezpečnost dat poskytovatele finančních služeb,

m) se ujistil, že pracovní postupy v oblasti bezpečnosti přístupu k informacím u poskytovatele cloud computingu jsou alespoň na úrovni postupů, které by použil poskytovatel finančních služeb v souladu se svými zásadami pro řídicí a kontrolní systém, pokud by činnost zajišťoval sám,

n) zná podmínky přístupu pracovníků poskytovatele cloud computingu k datům poskytovatele finančních služeb včetně aplikovaných opatření a kontrol dodržování stanovených podmínek a zda zajistil, že budou minimalizovány na nezbytně nutnou míru případy, kdy pracovníci poskytovatele cloud computingu budou přistupovat k datům poskytovatele finančních služeb (servisní úkony),

o) zajistil, že poskytovatel cloud computingu zaznamenává události, které ohrozily nebo narušily bezpečnost informačních systémů, a umožňuje poskytovateli finančních služeb

[8] Operační riziko zahrnuje např. riziko právní, riziko compliance, riziko outsourcingu, riziko systémů, riziko modelů, riziko nedostatků nebo selhání osob nebo procesů atd.

získání všech informací, které se týkají událostí, které ohrozily nebo narušily bezpečnost dat poskytovatele finančních služeb,

p) má zajištěno, že dojde-li při zpracování dat, mimo rámec servisních úkonů, ke zpřístupnění jeho dat pracovníkovi poskytovatele cloud computingu nebo jiné osobě pro něj činné (řetězový outsourcing), jsou mu neprodleně ohlášeny jako bezpečnostní incident,

q) se zaměřil v pohotovostních plánech zejména na situaci omezení přístupu k vlastním datům a přesun vlastních dat zpět nebo k jinému poskytovateli outsourcingu,

r) zahrnul do svých pohotovostních plánů i případ neočekávaného ukončení činností poskytovatele služby cloud computingu,

s) zajišťuje aktuální, pravidelné odborné a také nezávislé posouzení a ujištění o řídících a kontrolních procesech[9], které zahrnují identifikaci, popis a posouzení všech rizik podstupovaných poskytovatelem finančních služeb v souvislosti s využíváním cloud computingu, zda při tomto posuzování a ujištění o cloud computingu využívá všech dostupných možností a forem vč. využití poznatků z vlastních kontrolních činností poskytovatele cloud computingu a externího nezávislého posouzení provedeného u poskytovatele cloud computingu podle mezinárodně uznávaných standardů z oblasti řízení rizik informačních a komunikačních systémů a technologií,

t) má každé provedené odborné nezávislé ujištění o řídících a kontrolních procesech doloženo odpovídající dokumentací splňující požadavky na zpětnou vysledovatelnost a rekonstruovatelnost a zda má trvale k dispozici dokumentaci týkající se tohoto ujištění, zejména zprávu o zjištěních, a je schopen poskytnout tuto dokumentaci na vyžádání České národní bance[10] tak, aby byla použitelná pro účely výkonu dohledu České národní banky vyplývající z příslušných právních předpisů, a

u) smluvní dokumentace umožňuje poskytovateli finančních služeb jednostranně ukončit outsourcingový vztah.

8. Česká národní banka rovněž posuzuje, zda poskytovatel finančních služeb zajistil další předpoklady pro efektivní výkon dohledu daného outsourcingu Českou národní bankou s přihlédnutím ke specifikům cloud computingu. V tom také, zda poskytovatel finančních služeb

   a) sdělil v rámci plnění své ohlašovací povinnosti o outsourcingu[11] České národní bance také informaci o osobě nebo osobách poskytujících poskytovateli cloud computingu nezávislé odborné externí posouzení a ujištění o cloud computingu; účelem je včasné informování České národní banky o osobě, kterou poskytovatel cloud computingu určil jako externího posuzovatele cloud computingu, a

   b) zajistil přímou případnou výměnu informací mezi poskytovatelem outsourcingu a Českou národní bankou a další vyžádanou spolupráci poskytovatele cloud computingu s Českou národní bankou včetně určení kontaktních osob poskytovatele cloud computingu pro takové účely a další pravidla potřebná pro efektivní výkon dohledu.

[9] Např. čl. 41(1) třetí pododstavec Směrnice 2009/138/ES ve spojení s čl. 258(6) a čl. 266 Nařízení č. 35/2015.
[10] Např. čl. 35(1) Směrnice 2009/138/ES.
[11] Např. čl. 49(3) Směrnice 2009/138/ES, § 107 vyhlášky č. 163/2014 Sb.