Odůvodnění

vyhlášky, kterou se mění vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu

A. OBECNÁ ČÁST

1. Vysvětlení nezbytnosti navrhované právní úpravy, odůvodnění jejích hlavních principů

Návrh vyhlášky, kterou se mění vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu (dále jen „vyhláška“), je reakcí na praxi s aplikací platného právního rámce, z níž vyplynula potřeba upřesnit ustanovení k řídicímu a kontrolnímu systému, zejména v oblasti řízení bezpečnostních a provozních rizik se zvláštním zaměřením na rizika v oblasti informačních a komunikačních technologií. Svědčí o tom i vývoj tzv. Single Rulebook spravovaného Evropským orgánem pro bankovnictví, jehož součástí je také směrnice Evropského parlamentu a Rady (EU) 2015/2366 (dále jen „směrnice PSD2“). Směrnice PSD2 je v režimu maximální harmonizace, a proto je nutné reagovat na aktualizaci implementace požadavků obsažených v této směrnici, zejména v oblasti řízení bezpečnostních a provozních rizik a vyřizování stížností a reklamací, ke které v rámci Evropského systému dohledu nad finančním trhem došlo.

Evropský orgán pro bankovnictví vydal obecné pokyny týkající se řízení bezpečnostních a provozních rizik (Obecné pokyny pro řízení rizik IKT a bezpečnosti) použitelné od 30. června 2020, a to k čl. 95 směrnice PSD2. Zároveň došlo k rozšíření působnosti aktualizovaných obecných pokynů Společného výboru (JC) k vyřizování stížností v odvětví cenných papírů (ESMA) a bankovnictví (EBA) na stížnosti v oblasti platebních služeb. Vyhláška by tak měla zapracovat tyto obecné pokyny pro zajištění jednotných, účinných a efektivních postupů dohledu v rámci Evropského systému dohledu nad finančním trhem a zajištění společného, důsledného a jednotného uplatňování práva Unie.

2. Zhodnocení souladu navrhované právní úpravy se zákonem, k jehož provedení je navržena, včetně souladu se zákonným zmocněním

Vyhláška je v souladu se zákonnými zmocněními.

3. Zhodnocení souladu navrhované právní úpravy s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie a obecnými právními zásadami práva Evropské unie

Pokud jde o transpozici směrnice PSD2, vyhláška zpřesňuje transpozici čl. 95 odst. 1 a 3 týkajících se systému řízení bezpečnostních a provozních rizik a čl. 101 týkajícího se systému vyřizování stížností a reklamací.

Vyhláška je v souladu s čl. 107 (Úplná harmonizace) směrnice PSD2, podle kterého nesmí členské státy ponechat v platnosti ani zavádět ustanovení odchylující se od ustanovení této směrnice, a čl. 16 (Plná harmonizace) směrnice 2009/110/ES (dále jen „směrnice EMID“), podle kterého v míře, ve které tato směrnice stanoví harmonizaci, nesmějí členské státy zachovávat ani zavádět jiná ustanovení, než která jsou stanovena v této směrnici.

Vyhláška je slučitelná s právem Evropské unie.

4. Zhodnocení platného právního stavu a odůvodnění nezbytnosti jeho změny

Účelem vyhlášky je aktualizace způsobu plnění některých požadavků na řídicí a kontrolní systém platební instituce, instituce elektronických peněz a správce informací o platebním účtu, aktualizace způsobu plnění požadavků na systém řízení bezpečnostních a provozních rizik a systém vyřizování stížností u poskytovatele platebních služeb malého rozsahu a vydavatele elektronických peněz malého rozsahu.

Další změny jsou především technické.

5. Předpokládaný hospodářský a finanční dosah navrhované právní úpravy na státní rozpočet, ostatní veřejné rozpočty, na podnikatelské prostředí České republiky, dále sociální dopady, včetně dopadů na rodiny a dopadů na specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny, a dopady na životní prostředí

Vyhláška nemá dopad na státní rozpočet ani na ostatní veřejné rozpočty. Z navrhovaných změn nevyplývají zvýšené náklady ani pro Českou národní banku.

Vyhláška nemá negativní dopad na podnikatelské prostředí. Upřesňuje mj. systém řízení bezpečnostních a provozních rizik, zejména v oblasti informačních a komunikačních technologií, což má přispět k omezení rizik v této oblasti a zajištění bezpečnosti informací a kontinuity činnosti povinných osob. Posílení odolnosti a bezpečnosti sektoru poskytovatelů platebních služeb může pozitivně přispět k poskytování platebních služeb ve vyšším rozsahu a kvalitě. Stanovení podrobností v oblasti řízení informačních a komunikačních technologií a bezpečnosti přispěje také k vyšší předvídatelnosti při výkonu dohledu.

Zapracování obecných pokynů pro řízení rizik v oblasti informačních a komunikačních technologií a bezpečnosti a obecných pokynů pro vyřizování stížností a reklamací do návrhu vyhlášky přispěje k modernizaci tuzemského regulatorního rámce v oblasti platebních služeb, což může přispět k větší mezinárodní důvěryhodnosti sektoru poskytovatelů platebních služeb a zvýšení jejich prestiže v mezinárodním měřítku.

Vyhláška poskytne spotřebitelům větší jistotu v případě uplatňování stížností a reklamací, neboť se upřesňuje systém vyřizování stížností a reklamací, který mají povinné osoby zavést a udržovat. Posílení systému pro řízení rizik v oblasti informačních a komunikačních technologií může také přispět k větší bezpečnosti a ochraně spotřebitelů při využívání platebních služeb.

Vyhláška nemá žádné negativní sociální dopady, ani nemá žádné dopady na specifické skupiny obyvatel, na osoby sociálně slabé, ani na osoby se zdravotním postižením

a národnostní menšiny.

Vyhláška nemá žádné negativní dopady na životní prostředí.

6. Zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Vyhláška neobsahuje diskriminační ustanovení, ani nemá dopad v oblasti rovnosti mužů a žen.

7. Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

Vyhláška je v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů.

8. Zhodnocení korupčních rizik

Na základě vyhodnocení provedeného podle metodiky CIA (*Corruption Impact Assessment*) nebyla zjištěna žádná korupční rizika, která by mohla souviset s přijetím vyhlášky.

Jedním z úkolů České národní banky podle zákona o České národní bance a dalších zákonů je dohled nad osobami působícími na finančním trhu. Pro účely výkonu tohoto dohledu jsou České národní bance svěřeny kompetence správního úřadu.

Působnost a pravomoc jednotlivých útvarů při výkonu dohledu jsou v České národní bance stanoveny vnitřním předpisem, který schvaluje bankovní rada jakožto nejvyšší řídicí orgán. Informace o organizační struktuře České národní banky jsou k dispozici veřejnosti na jejích internetových stránkách. Pro řádný výkon činnosti České národní banky jsou nastaveny odpovídající vnitřní kontrolní mechanismy, které jsou pravidelně ověřovány a aktualizovány.

Vzhledem k povaze vyhlášky a rovněž vzhledem k důsledně uplatňovaným vnitřním rozhodovacím a kontrolním postupům v České národní bance lze potenciální korupční rizika prakticky vyloučit.

9. Zhodnocení dopadů na bezpečnost nebo obranu státu

Vyhláška nemá žádný dopad na bezpečnost nebo obranu státu.

10. Zhodnocení dopadů na digitální prostředí

Vyhláška není v rozporu s obecnými zásadami rozvoje digitální agendy a byla zpracována v souladu s hlavními principy jejího rozvoje, včetně zásad pro tvorbu digitálně přívětivé legislativy. Respektuje princip technologické neutrality a možnosti volby optimální kombinace vhodných technologických řešení, když ponechává na uvážení dotčeného subjektu, jaké prostředky zvolí k naplnění požadavků na systém vyřizování stížností a systém řízení bezpečnostních a provozních rizik i dalších požadavků. Významně rovněž přispívá ke zvyšování kybernetické bezpečnosti při výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu.

B. ZVLÁŠTNÍ ČÁST

Článek I

K bodu 1 (§ 1)

Aktualizuje se předmět úpravy tak, že se upřesňuje, jaké požadavky na jednotlivé skupiny povinných osob jsou ve vyhlášce upraveny.

K bodu 2 (část druhá)

Aktualizuje se část druhá, když se zejména zpřesňuje transpozice čl. 95 odst. 1 a 3 směrnice PSD2, které se týkají systému řízení bezpečnostních a provozních rizik, a čl. 101 směrnice PSD2 o systému vyřizování stížností a reklamací.

Ustanovení § 20 odst. 1 zákona, ani ve spojení s ustanoveními § 9 odst. 1 zákona, netvoří systematicky uspořádaný a věcně úplný výčet požadavků na řídicí a kontrolní systém platební instituce. Jednotlivá písmena v § 20 odst. 1 zákona nestanoví závazné vnitřní členění řídicího a kontrolního systému či samostatně stojící požadavky na zcela odlišné oblasti, ale jedná se o vybrané požadavky a pravidla různé povahy s různými vzájemnými vazbami a souvislostmi. Některá ustanovení začleněná do § 20 odst. 1 zákona, případně i ve spojení s § 9 odst. 1 zákona, jsou dále upravena, resp. konkretizována v jiných ustanoveních zákona, nebo v přímo účinných předpisech EU. Ustanovení § 20 odst. 1 zákona je tak výčtem obecných i konkrétních pravidel týkajících se řídicího a kontrolního systému, nikoliv vedle sebe stojících (nepřekrývajících se) požadavků.

Například systém vyřizování stížností a reklamací podle § 20 odst. 1 písm. j) zákona je provázán s § 20 odst. 1 písm. e) zákona (řádné administrativní postupy), s § 20 odst. 1 písm. b) zákona (organizační uspořádání, neslučitelnost funkcí), s § 20 odst. 1 písm. c) zákona (systém řízení rizik), s § 20 odst. 1 písm. d) zákona (systém vnitřní kontroly) i s § 20 odst. 1 písm. h) zákona (řízení střetu zájmů). Podobně požadavek § 20 odst. 1 písm. i) zákona týkající se kontrolních a bezpečnostních opatření je nutné vykládat společně s § 20 odst. 1 písm. a) zákona (strategické a operativní řízení), s § 20 odst. 1 písm. b) zákona (organizační uspořádání, neslučitelnost funkcí), s § 20 odst. 1 písm. c) zákona (systém řízení rizik), s § 20 odst. 1 písm. d) zákona (systém vnitřní kontroly) i s § 20 odst. 1 písm. h) zákona (řízení střetu zájmů).

Některé prvky řídicího a kontrolního systému uvedené v § 20 odst. 1 zákona jsou dále upraveny, resp. konkretizovány přímo v zákoně. Například pravidla týkající se ochrany peněžních prostředků podle § 22 zákona jsou jednou z konkretizací § 20 odst. 1 písm. e) zákona (řádné administrativní a účetní postupy). Dalším příkladem konkretizace požadavku na řádné administrativní a účetní postupy jsou pravidla týkající se uchování dokumentů a záznamů podle § 31 zákona. Podobně požadavky na oznamování podle § 28 zákona lze podřadit pod § 20 odst. 1 písm. e) zákona (řádné administrativní postupy), stejně tak je lze podřadit pod § 20 odst. 1 písm. f) zákona (systém vnější komunikace). Pokud jde o příklady přímo účinných předpisů EU týkajících se řídicího a kontrolního systému, tak například nařízení (EU) 2018/389 určuje požadavky na tzv. silné ověření klienta jako nedílné součásti

požadavků na řádné administrativní postupy platební instituce nebo nařízení (EU) 2018/389 určuje závazné bezpečné otevřené standardy komunikace jako nedílné součásti požadavků na řízení provozních rizik a bezpečnosti platební instituce.

Vyhláška na základě zmocnění podle § 20 odst. 4 zákona, resp. § 48 odst. 4 zákona a § 78 odst. 4 zákona, stanovuje způsob plnění požadavků na řídicí a kontrolní systém, pokud jde o vnitřní předpisy, schvalovací a rozhodovací procesy, systém řízení bezpečnostních a provozních rizik a systém vyřizování stížností a reklamací. Vyhláška respektuje skutečnost, že směrnice PSD2 i směrnice EMID jsou v režimu maximální harmonizace.

Způsob plnění požadavků na řídicí a kontrolní systém je tak stanoven se zaměřením na vnitřní předpisy, do nichž má povinná osoba promítnout požadavky stanovené na řídicí a kontrolní systém a postupy k jejich naplňování, a to se zohledněním své jedinečnosti i jedinečnosti své činnosti. Vnitřní předpisy by měly být pravidelně vyhodnocovány a případně upravovány a měly by vždy být v souladu s údaji, popisy a principy uvedenými v žádosti o udělení povolení k činnosti a jejích přílohách, na jejichž základě bylo povolení k činnosti uděleno, případně změněnými podle § 11 zákona, a pracovníci by podle nich měli postupovat.

Podle nařízení (EU) upravujících Evropské orgány dohledu, například nařízení (EU) č. 1093/2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), má dotčená instituce vynaložit veškeré úsilí, aby se řídila obecnými pokyny a doporučeními vydanými Evropským orgánem pro bankovnictví, Evropským orgánem pro cenné papíry a trhy, Evropským orgánem pro pojišťovnictví a zaměstnanecké penzijní pojištění nebo Společným výborem evropských orgánů dohledu a určenými poskytovatelům platebních služeb, které jsou relevantní pro poskytování platebních služeb. Ve vnitřních předpisech by proto měly být tyto obecné pokyny a doporučení zohledněny. Dotčená instituce také má jasným a podrobným způsobem podávat zprávu o tom, zda se těmito obecnými pokyny nebo doporučeními řídí, je-li tato povinnost informování v konkrétních obecných pokynech či doporučení uvedena.

V případech, kdy obecné pokyny a doporučení interpretačně upřesňují ustanovení obsažená v přímo účinných předpisech EU nebo v předpisech EU, které jsou transponovány právním předpisem, bude ČNB nicméně důsledně ve vztahu k dotčeným povinným osobám vyžadovat plnění těchto požadavků v souladu s výkladem obsaženým v těchto obecných pokynech a doporučeních, bude-li to zároveň v souladu s národní právní úpravou. Povinná osoba by měla být schopna prokázat, že vynaložila veškeré úsilí, aby se ve vnitřních předpisech obecnými pokyny a doporučeními relevantními pro poskytování platebních služeb řídila. V případě, že se relevantními obecnými pokyny a doporučeními neřídí, měla by být schopna věcně odůvodnit, že smyslu či požadavků vyplývajících z obecných pokynů a doporučení dosáhla jinými postupy, či že tyto pokyny a doporučení nejsou pro ni relevantní.

ČNB při výkonu dohledu posuzuje, zda systém povinné osoby pro sledování, vyhodnocování a aktualizaci vnitřních předpisů zajišťuje, že vnitřní předpisy jako celek i jednotlivě jsou v souladu s právními předpisy, požadavky stanovenými v právně závazných aktech (např. rozhodnutích České národní banky) i – v rámci režimu popsaného výše – obecnými pokyny a doporučeními uvedenými shora. V rámci toho ČNB vždy posuzuje, zda systém povinné osoby pro sledování, vyhodnocování a aktualizaci vnitřních předpisů zajišťuje také soustavný

soulad vnitřní předpisové základny jako celku i jednotlivých vnitřních předpisů s požadavky zákona na vnitřní předpisy povinné osoby, zda vnitřní předpisy jako celek i jednotlivě jsou s ohledem na činnosti povinné osoby jednoznačné, úplné, ucelené, bezrozporné a soustavně aktuální (funkce compliance). ČNB při výkonu dohledu také posuzuje, jak jsou stanoveny postupy výkonu dalších činností povinné osoby a další vnitřní pravidla, zejména zda nenarušují řádné a obezřetné poskytování platebních služeb, například pravidla pro zajištění ochrany peněžních prostředků klientů, systém motivování a odměňování pracovníků, systém vnitřního hlášení (interní reportování) a jeho funkčnost, systém výběru pověřených zástupců, pravidla pro určení, posouzení, řízení a zmírnění či prevenci střetu zájmů. ČNB při výkonu dohledu dále posuzuje, zda je zajištěno, že povinná osoba volí, zapracovává do vnitřních předpisů a uplatňuje při své činnosti vhodně a dostatečně uznávané a osvědčené principy a postupy vydávané uznávanými vydavateli a využívané při činnostech obdobné povahy (uznávané standardy řádných postupů). ČNB se k uznávaným standardům vyjádřila v Úředním sdělení k výkonu činnosti na finančním trhu: Kvalitativní požadavky související s výkonem činnosti – základní informace (částka 18/2010 Věst. ČNB).

Vyhláška stanovuje, aby se v rámci činnosti povinné osoby schvalování a podepisování dokumentů řídilo jasně stanovenými pravidly a aby bylo možné schvalovací a rozhodovací procesy zaznamenávat, uchovávat, zpětně vysledovat a rekonstruovat. Zaznamenání, uchovávání a zpětná vysledovatelnost a rekonstruovatelnost určitých informací, skutečností, dat, procesů apod. je předpokladem zejména pro kontrolní činnosti tak, aby bylo možno dané skutečnosti či informace „vystopovat“ do minulosti (*vysledovat*), a toto zajistit v kvalitě, rozsahu, struktuře atd. potřebné pro případné zpětné prověření dané skutečnosti či informace ve všech jejích fázích v minulosti (*rekonstruovat*). Podle povahy dané skutečnosti či informace se *vysledovatelností* rozumí vytvoření „paměťové stopy“ tak, aby bylo možno dané skutečnosti či informace dohledat a určit jejich původce i uživatele od jejich počátku nebo po stanovené období do minulosti. *Rekonstruovatelností* se rozumí zajištění všech nutných předpokladů – podle povahy dané skutečnosti či informace – pro její obnovu, znovuvytvoření, zopakování, navrácení, napodobení, reprodukci apod., jakož i jejich průkaznost, prokazatelnost, doložitelnost. Doba potřebná pro uchovávání a od ní se odvíjející doba, po kterou lze určité informace vysledovat a rekonstruovat, závisí na požadavcích stanových právními předpisy pro uchování informací, zejména § 31 zákona a dále například lhůty stanovené předpisy v oblasti boje proti praní peněz a financování terorismu, účetnictví, ochrany spotřebitele a daní.

Vyhláška se v rámci systému řízení bezpečnostních a provozních rizik, mezi něž mj. patří riziko právní (legal risk), riziko praní peněz a financování terorismu (ML/TF risk), riziko jednání (conduct risk), riziko podvodů (fraud risk), riziko třetích stran (third-party risk), zaměřuje na rizika v oblasti informačních a komunikačních technologií a bezpečnosti. Jde o rizika ztráty v důsledku narušení důvěrnosti dat, integrity systémů a dat nebo dostupnosti systémů a dat nebo v důsledku neschopnosti změnit informační a komunikační systémy v přiměřeném čase a s přiměřenými náklady, pokud se mění prostředí nebo činnosti. Důvěrnost *(confidentiality)* vyjadřuje zajištění toho, že informace je přístupná jen těm, kteří jsou oprávněni k ní mít přístup. Integrita *(integrity)* je zabezpečení přesnosti a kompletnosti informace a metod jejího zpracování. Dostupnost *(availability)* je zajištění toho, že informace

a s nimi spojená aktiva jsou uživatelům přístupná v době, kdy je požadují. Dále jde o bezpečnostní rizika vyplývající z nedostatečnosti nebo selhání vnitřních procesů nebo z vnějších událostí, včetně kybernetických útoků, nebo z nedostatečného fyzického zabezpečení. Pokud jde o řízení bezpečnostních a provozních incidentů v oblasti platebního styku, postupy pro jejich klasifikaci upravují obecné pokyny Evropského orgánu pro bankovnictví k oznamování významných incidentů podle směrnice (EU) 2015/2366 o platebních službách na vnitřním trhu (PSD2) (EBA/GL/2017/10).

V části druhé jsou do ustanovení o systému vyřizování stížností a reklamací zapracovány obecné pokyny Společného výboru (JC/2018/35) k vyřizování stížností v odvětví cenných papírů a bankovnictví, které byly od 1. května 2019 rozšířeny na poskytovatele služeb podle směrnice PSD2. Tyto pokyny harmonizují požadavky podle čl. 101 směrnice PSD2 na přiměřené a účinné postupy pro řešení stížností za účelem vyřizování stížností uživatelů platebních služeb. Prošetřování stížností a reklamací je nutné provádět s náležitou péčí, například by nemělo docházet k potlačování nebo upřednostňování některých stížností a reklamací. V komunikaci s uživatelem ohledně dotčené stížnosti nebo reklamace by neměly být používány komplikované slovní obraty, příliš odborné výrazy nebo vysvětlení jen formou odkazů na různé právní předpisy.

K bodu 3 (§ 27 odst. 4)

Zavádí se legislativní zkratka „hybridní platební instituce“ pro platební instituci, která vykonává i jiné podnikatelské činnosti než činnost, k jejímuž výkonu je oprávněna na základě povolení uděleného podle zákona. Tato legislativní zkratka je v platném znění vyhlášky č. 7/2018 Sb. uvedena v § 2, který je součástí části druhé, jejíž nové znění předložená vyhláška obsahuje.

K bodu 4 (§ 34 odst. 1)

Stanovují se pravidla pro výpočet kapitálu, a to obdobně jako v případě kapitálu platební instituce odkazem na příslušná ustanovení nařízení (EU) 575/2013, pro které je v § 27 odst. 1 zavedena legislativní zkratka „nařízení“. Naplňuje se tak zmocnění v § 74 odst. 6 zákona.

K bodu 5 (§ 34 odst. 4)

Pojem „hybridní instituce elektronických peněz“, který není ve vyhlášce č. 7/2018 Sb. vymezen ani zaveden jako legislativní zkratka, se nahrazuje textem „instituce elektronických peněz, která vykonává i jiné podnikatelské činnosti než činnost, k jejímuž výkonu je oprávněna na základě povolení uděleného podle zákona“.

K bodu 6 (příloha)

Doplňuje se příloha, která obsahuje podrobnosti k řízení rizik v oblasti informačních a komunikačních technologií a bezpečnosti.

V příloze je obsaženo upřesnění některých pravidel vyplývajících z unijních předpisů a transponovaných ustanoveními § 4, které plně odpovídá výkladu obsaženému v obecných pokynech Evropského orgánu pro bankovnictví pro řízení rizik v oblasti informačních a komunikačních technologií a bezpečnosti (EBA/GL/2019/04). Tyto obecné pokyny upřesňují opatření k řízení rizik, která musí podle čl. 95 odst. 2 směrnice PSD2 přijmout

poskytovatelé platebních služeb k řízení provozních a bezpečnostních rizik, ve smyslu rizik v oblasti informačních a komunikačních technologií a bezpečnosti (dále jen „rizika IKT a bezpečnosti“), souvisejících s jimi poskytovanými platebními službami. Tyto obecné pokyny obsahují i požadavky týkající se bezpečnosti informací, včetně kybernetické bezpečnosti, a to v rozsahu, v němž jsou tyto informace uchovávány v informačních a komunikačních systémech (dále jen „IKT systémy“). Vzhledem k tomu, že tyto obecné pokyny jsou klíčové pro poskytovatele platebních služeb a jsou součástí tzv. Single rulebook EU, je v příloze dodrženo i řazení jednotlivých bodů těchto obecných pokynů. K mezisektorové harmonizaci řízení rizik v oblasti informačních a komunikačních technologií a bezpečnosti by mělo v budoucnu přispět nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014, jehož návrh Evropská komise předložila v září 2020 společně se změnou směrnice PSD2. Výše uvedený návrh nařízení mj. obsahuje požadavky, které jsou dosud adresovány jen prostřednictvím obecných pokynů EBA (EBA/GL/2019/04) úvěrovým institucím a poskytovatelům platebních služeb.

Bod 1 přílohy týkající se přiměřenosti vychází z toho, že systém řízení provozních a bezpečnostních rizik je vlastní, jedinečný vnitřní systém povinné osoby, přizpůsobený individuálním požadavkům a podmínkám této povinné osoby. Tato skutečnost vylučuje přenositelnost systému řízení provozních a bezpečnostních rizik na jiného poskytovatele či existenci univerzálního systému řízení provozních a bezpečnostních rizik využitelného více povinnými osobami. ČNB při výkonu dohledu uplatňuje zásadu přiměřenosti, tj. zohlednění konkrétních individuálních podmínek a parametrů odrážejících zaměření a uspořádání výkonu činnosti dané povinné osoby, jako je např. typ, složitost, technologická náročnost, míra závislosti na třetích stranách a další podstatné parametry modelu podnikání, druhy služeb, místa a formy jejich distribuce, objem, velikost a složitost operací, využívání třetích osob, výkon případných dalších činností, začlenění povinné osoby do podnikatelského uskupení atd. a s tím spojená přímo podstupovaná a další možná rizika. Uplatnění zásady přiměřenosti však nemůže narušit řádný a obezřetný výkon činnosti povinné osoby, zejména nemůže být narušen plynulý výkon činnosti a trvalé fungování povinné osoby, tzn. kontinuita činnosti. Z toho důvodu je nutné například mít dostatek pracovníků, jež zabezpečí potřebnou zastupitelnost nejen na pozicích přímo ovlivňujících poskytování platebních služeb. Bez ohledu na způsob, jakým povinná osoba koncipuje systém řízení provozních a bezpečnostních rizik, je vždy nutné, aby všechna rozhodnutí, opatření, změny, kontroly apod. týkající se IKT systémů a shromažďovaných informací, které je třeba chránit, tzn. informačních aktiv, byla zaznamenávána za účelem případného vysledování a rekonstruovatelnosti.

Jde-li o strategické a operativní řízení a organizační uspořádání, kterého se týkají body 2 až 9 přílohy, je kromě personálního zajištění důležité také finanční zajištění provozu IKT systémů a řízení rizik s tím spojených. Proto je nutné, aby na tuto oblast byl vyčleněn dostatečný objem prostředků. Objem prostředků se bude odvíjet od požadavku na adekvátní rámec vnitřní správy a řízení a vnitřní kontroly pro riziko IKT a bezpečnosti a požadavku na odbornou způsobilost a zkušenosti pracovníků v oblasti informačních a komunikačních technologií a bezpečnosti. Důležité je také jasné vymezení rolí. Ty představují soubor dovedností a úrovní oprávnění k výkonu definované činnosti nebo k provádění úkolu.

Například v oblasti řízení rizik jde o roli vedoucího pracovníka, který řídí, kontroluje a řeší rizika spojená se svěřenou oblastí (gestor v řízení rizik), přičemž konkrétní rizika jsou v působnosti konkrétních jemu podřízených pracovníků. V případě, že řešení konkrétního rizika přesahuje působnosti dotčeného pracovníka, přenáší toto na roli o úroveň výše.

Celková strategie je pojem běžně používaný v řízení a představuje výstup strategického řízení. Jde o dlouhodobý plán vytvořený k dosažení určitého cíle nebo cílů. V praxi se jedná zpravidla o formalizovaný dokument, který obsahuje popis prvních dvou fází strategického cyklu, tj. popis mise organizace, její vize a strategických cílů a harmonogram jejich realizace. Při vstupu do sektoru je celková strategie představena v obchodním plánu, jehož reálnost (životaschopnost) a udržitelnost i při řádném a obezřetném výkonu povolených činností a zajištění kontinuity činnosti je klíčová pro získání povolení k činnosti.

Podobně akční plán je pojem běžně používaný v řízení. Představuje plán jednotlivých kroků, které musí být vykonány, aby bylo dosaženo vytčeného cíle. Akční plán nemá žádnou normovanou nebo danou podobu, může tedy vypadat různě. Aby splnil svůj účel, musí obsahovat veškeré náležitosti, které jsou důležité pro rozdělení práce a dosažení vytčeného cíle. Jde o seznam kroků – aktivit, které je třeba udělat k dosažení cíle, přiřazení odpovědnosti konkrétních osob za konkrétní aktivity, celkový časový horizont a hlavní milníky, termíny splnění konkrétních aktivit, rozpočet akčního plánu, přiřazení dalších zdrojů k jednotlivým aktivitám (například další lidé, materiál, pracovní pomůcky, subdodávky), další podmínky, omezení a rizika nutné pro splnění cílů, popis cílů a popis toho, jak bude dokázáno jejich dosažení. Rozsah a forma akčního plánu se volí vždy dle situace a rozsahu akce, která se plánuje. Může mít podobu jednoduchého seznamu nebo několikastránkového dokumentu, který bude podléhat pravidelným aktualizacím.

Základním rámcem je stanovení strategie v oblasti informačních a komunikačních technologií (bod 6 přílohy). Její naplňování se pak děje vytýčením jednotlivých akčních plánů, které se při větší komplexnosti mohou rozdělit do jednotlivých portfolií (tzv. portfolio management). Protože akční plány jsou obvykle řízeny projektově, je žádoucí, aby o dosažení nebo naopak nedodržení všech zásadních milníků projektu byly informovány vedoucí osoby povinné osoby, aby se včas předešlo případnému nesplnění projektu nebo milníku, který může poskytovat například službu v rámci jiného akčního plánu – projektu.

Ujednání s externími poskytovateli (bod 8 přílohy) jsou podrobná do té míry, že z nich jasně plyne, jak IKT systémy pracují za „dobrých časů“ i při mimořádných situacích. Povinná osoba by se měla soustředit na jasné a přesné definice obdržených služeb, způsoby jejich měření a vyhodnocování následované případnými sankcemi při nedodržení parametrů popsaných služeb, na testování kontinuity služeb a ochranu dat. Také by si měla zajistit možnost přezkoumat procesy externího poskytovatele, a to i na místě, pokud je to možné, aby tak mohla dostát své zodpovědnosti, které se delegováním výkonu činnosti na externí poskytovatele nezbavila. Pro naplnění požadavků v této oblasti je žádoucí řídit se obecnými pokyny k outsourcingu vydanými Evropským orgánem pro bankovnictví (EBA/GL/2019/02).

Specifikace životního cyklu dat [bod 8 písm. a) přílohy] představuje jasně definovaný rámec způsobu, jak se data do IKT systémů dostávají, jak se chrání, jak se klasifikují, jak je přístup

k nim řízen, jak lze s nimi pracovat, jak se archivují, jak jsou případně deklasifikována a ničena.

Pokud jde o systém řízení rizik IKT a bezpečnosti (body 10 až 24 přílohy), je tento nedílnou součástí systému řízení rizik pokrývajícího všechna rizika, kterým je povinná osoba vystavena. Pro určení míry ochoty povinné osoby přistupovat k rizikům se běžně také používá pojem „rizikový apetit". Povinná osoba má být schopna určit, které obchodní funkce, procesy a informační aktiva jsou nezbytné pro její činnosti, a které tedy musí být nejvíce chráněny.

Obchodní funkce jsou kontinuálně vykonávané činnosti povinné osoby, které naplňují její účel a vycházejí ze strategických cílů povinné osoby, a způsob, jakým je dosahováno těchto cílů, tj. realizace činnosti. Obchodní funkce lze rozdělit na dvě kategorie, a to na hlavní obchodní funkce a podpůrné obchodní funkce. Hlavní obchodní funkcí je například poskytování platebních služeb, podpůrnou obchodní funkcí je například vedení účetnictví povinné osoby. Zpravidla obě kategorie mají své IKT systémy nebo alespoň samostatné komponenty IKT systémů.

Míra ochoty povinné osoby přistupovat k rizikům, tzv. rizikový apetit, [bod 13 písm. a) přílohy] se kvantitativně nejčastěji určuje pomocí akceptovatelné ztráty povinné osoby podle jednotlivých oblastí rizik (např. tržní riziko, operační riziko, riziko compliance, IKT riziko) a následně se převádí na míru rizika porovnatelnou s vypočtenou hodnotou identifikovaného rizika. K tomu se většinou používá tzv. cost-benefit analýza, a to takovým způsobem, aby hodnota identifikovaného rizika po odečtení omezujících opatření byla právě rovna nebo nižší než je hodnota rizikového apetitu v dané oblasti rizik. V případě kvalitativního určení rizikového apetitu tento postup není možný. Zde je však potřebné rizikový apetit povinné osoby jasně vysvětlit, aby mohla být vyhodnocena jeho relevantnost ve vztahu k opatřením omezujícím původní inherentní rizika.

Protože vystavení povinné osoby vůči rizikům a jejich omezování je jedním ze základních požadavků vnitřního řízení, je obvyklé, že vedoucí pracovník je o této oblasti pravidelně informován [bod 13 písm. e) přílohy]. Výjimkou nebývá týdenní nebo měsíční hlášení. Cílem je zjistit, jestli se přijatá opatření osvědčila či jestli nemusejí být zavedena další opatření. Častým zdrojem informací o účinnosti opatření bývají tzv. systémy SIEM *(Security Information and Event Management).* Hlášení z těchto systémů bývají dobrým indikátorem nedostatečnosti nebo naopak adekvátnosti přijatých opatření.

Informační aktiva (bod 16 přílohy) představují shromážděné informace, které je třeba chránit. Ochrana shromážděných informací je významná, neboť informace jsou důležité jak pro poskytování služeb povinnou osobou uživatelům, tak pro podporu obchodních funkcí povinné osoby, pracovníků, třetích stran, externích poskytovatelů a pro vazby na jiné interní a externí systémy a procesy. Do této kategorie patří i platformy pro uchovávání a přenos těchto informací a práci s nimi. Je nutné zavést systém jednoznačné zodpovědnosti za každé informační aktivum. Obvykle je informační aktivum přiřazeno organizačnímu útvaru nebo osobě, která toto aktivum v rámci povinné osoby využívá nejvíce. Důvodem takového postupu je zvýšení zainteresovanosti pracovníků na chodu povinné osoby, zvýšení množství rizikových scénářů, které je dotčená osoba schopna identifikovat vůči tomuto aktivu, zvýšení schopnosti dotčené osoby chránit přidělené informační aktivum, posílení schopnosti dotčené

osoby najít alternativní cesty pro zajištění plynulého výkonu činnosti v případě výpadku jí přiřazeného informačního aktiva.

Z informačních aktiv povinná osoba vždy musí být schopna řídit ta informační aktiva, která podporují její kritické funkce (u ostatních, tj. těch, která nepodporují kritické funkce, požadavek tak striktní není). Řízení informačních aktiv *(information assets management)* je proces určení těchto aktiv, jejich klasifikace, vyhodnocení a řízení možných rizik, která mohou tato aktiva ohrozit, zavedení opatření k jejich ochraně a jejich pravidelná kontrola. Přezkoumávání přiměřenosti klasifikace informačních aktiv (bod 19 přílohy) a správné zařazení informačních aktiv podle jejich důležitosti je zásadní z hlediska rozpoznávání rizik, které se s nimi pojí, a z hlediska přijímání opatření na ochranu těchto aktiv. Obecně je v zájmu povinné osoby, aby informační aktiva, která mají vyšší míru klasifikace, byla uchovávána na více místech, aby v případě neoprávněného přístupu k tomuto místu byla případná ztráta co nejnižší.

Pokud jde o průběžné sledování hrozeb a zranitelností (bod 21 přílohy), je vhodné časté sledování bezpečnostních fór a stránek společností, které se zabývají problematikou bezpečnosti, hrozeb a zranitelností v oblasti informačních a komunikačních technologií, a následné aplikování nalezených zjištění, doporučení a nástrojů do informačního prostředí povinné osoby. Tato činnost je kontinuální, a tudíž vyžaduje každodenní sledování, neboť bezpečnostní situace se může vyvíjet velmi rychle, především při kybernetických útocích velkého rozsahu. Scénáře rizik jsou scénáře, které realizují hrozby při využití konkrétních zranitelností. Tyto scénáře vycházejí z konkrétního informačního prostředí povinné osoby a v mnoha případech se právě na scénářích rizik ukáže, jestli je existující zranitelnost zneužitelná interním nebo externím útočníkem.

Oznamování výsledků vyhodnocování rizik vedoucímu pracovníkovi (bod 24 přílohy) je důležité, neboť vedoucí pracovník má oprávnění a povinnost přikročit k realizaci opatření, pokud bylo rozpoznáno nové riziko nebo bylo zjištěno, že stávající riziko není ošetřeno adekvátním způsobem. Vedoucí pracovník určuje prioritu realizace opatření, a to podle rizikového apetitu, který je povinná osoba ochotna akceptovat, a v souvislosti s náklady, které s opatřeními souvisí.

V případě vnitřního auditu v oblasti rizik IKT a bezpečnosti (body 25 až 27 přílohy) je nutné mít na paměti, že při přezkoumávání souladu všech činností povinné osoby, které souvisejí s informačními a komunikačními technologiemi a bezpečností, s externími požadavky nejde jen o požadavky stanovené právními předpisy, ale například také pravidly platebních systémů nebo smluvními ujednáními. Při výkonu funkce vnitřního auditu je také důležitá nezávislost pracovníků na auditovaných činnostech. Neměly by například nastat případy, kdy povinná osoba využívá pro poskytování platebních služeb externí poskytovatele, kteří zároveň provádějí audit poskytovaných služeb. Na rozdíl od funkce compliance orientované na soustavný soulad povinné osoby se všemi relevantními právními předpisy, zajišťování funkce vnitřního auditu odpovídá za poskytování plně nezávislého a objektivního ujištění, prováděného výběrově na základě analýzy všech rizik včetně rizika provozního, resp. rizika compliance.

Uplatňování rizikově orientovaného přístupu při výkonu funkce vnitřního auditu (bod 25 přílohy) je důležité z důvodu potenciálně velmi rozsáhlé agendy, která může být předmětem vnitřního auditu. Z tohoto důvodu není realistické, aby pracovníci, kteří zajišťují funkci vnitřního auditu, byli schopni v průběhu jednoho roku prověřit všechny oblasti činnosti povinné osoby. Je však nutné zaměřit vnitřní audit v průběhu roku na nejkritičtější agendy a činit tak opakovaně i v dalších letech. Zároveň je potřeba, aby i méně kritické agendy byly v určitých periodách prověřovány. Chce-li mít povinná osoba jistotu, že žádná z vykonávaných činností není zanedbávána, není na závadu přidělit zdroje na více pracovníků zajišťujících funkci vnitřního auditu.

Plán auditů by měl zohlednit inherentní rizika v oblasti informačních a komunikačních technologií (bod 26 přílohy). Je vhodné mít systém pro stanovení inherentního rizika u všech činností a oblastí povinné osoby, včetně inherentních rizik IKT a bezpečnosti, a tento systém využít jako jeden ze vstupů při určení rizikového apetitu povinné osoby a opatření reagujících na konkrétní rozpoznaná rizika.

Primárními třemi cíli v oblasti bezpečnosti informací (bod 28 přílohy) je ochránit informace povinné osoby a uživatelů z hlediska důvěrnosti, integrity a dostupnosti. Politika bezpečnosti informací je rozpracováním těchto cílů do větší míry detailu tak, aby tato politika byla ucelená ve všech oblastech informačních a komunikačních technologií a procesů s nimi souvisejícími.

Pokud jde o hlavní role v oblasti řízení bezpečnosti informací (bod 29 přílohy), je vhodné definovat povinnosti pro vedoucího pracovníka, pracovníka, v jehož působnosti je bezpečnost, pracovníka v čele útvaru, který má v působnosti IKT systémy, uživatele, externí poskytovatele a další třetí strany a další osoby, například správce a vývojáře IKT systémů, osoby zajišťující aplikační nebo bezpečnostní textování, pracovníky, kteří zajišťují vnitřní audit v oblasti informačních a komunikačních technologií.

Míra detailu dokumentů vzniklých na základě politiky bezpečnosti (bod 30 přílohy) by měla být taková, aby umožňovala dotčeným pracovníkům podle nich postupovat. V takovém případě již nemusí být vyhotovovány dokumenty s větší mírou detailu. Výjimkou z tohoto pravidla jsou dokumenty vztahující se ke konkrétní technologii povinné osoby. ČNB při výkonu dohledu dostatečnost míry detailu dokumentů, nezbytnou pro jejich aplikovatelnost, posuzuje.

V souvislosti s postupy pro kontrolu logického přístupu a jeho anomálií (bod 31 přílohy) je potřebné zavést efektivní způsob kontroly záznamů pro přístupy k informačním aktivům. Pro tento účel se jako vhodné jeví používat specializovaný software, který upozorní na anomálie v tomto přístupu. Vstupem do tohoto systému jsou matice účtů, rolí a oprávnění vůči informačním aktivům, která umožní rozpoznat anomálie. Pro vyšší bezpečnost v oblasti interních úniků informací je vhodné používat systém pro detekci nebo prevenci úniku dat *(Data Loss Prevention, DLP).*

Jde-li o opatření pro fyzickou bezpečnost (bod 33 přílohy), je třeba mít na paměti, že i při přesunu technologií a dat do datových center je zajištění fyzické bezpečnosti informačních aktiv povinností povinné osoby. Je tudíž v jejím zájmu, aby jí budoucí poskytovatel datového

centra ještě před uzavřením smlouvy poskytl závazná pravidla a opatření, která v oblasti fyzické bezpečnosti zabezpečuje. Jen tak se povinná osoba může informovaně rozhodnout, zdali jsou pro ni tato pravidla a opatření akceptovatelná. Povinná osoba by také měla mít smluvně zajištěno, že může provádět fyzickou kontrolu dodržování těchto pravidel a opatření, a že má přístup k auditním zprávám ověřujícím aplikaci těchto pravidel a opatření.

Kvůli schopnosti povinné osoby identifikovat potenciální zranitelnosti [bod 36 písm. a) přílohy] je důležité, kromě pravidelné aktualizace systémového software povinné osoby, také sledovat nejnovější zranitelnosti v oblasti softwarového vývoje, neboť to umožňuje rychle reagovat na jejich výskyt, provádět potřebné změny softwaru a zamezovat tak zneužití těchto zranitelností. Pokud takovou změnu nelze provést rychle a povinná osoba by tak byla vystavena zvýšenému riziku, je nutné zavést kompenzační opatření, která v případě realizovaného rizika minimalizují dopad na informační aktiva a služby poskytované povinnou osobou.

Pro zabezpečení základní konfigurace všech síťových komponent [bod 36 písm. b) přílohy] je potřebné mít bezpečně uloženou konfiguraci všech kritických síťových prvků a pravidelně kontrolovat, zdali nedošlo ke změně nastavení těchto prvků. V případě zjištění rozdílu v těchto konfiguracích je nutné bez zbytečného odkladu zahájit šetření s cílem zjistit zdroj této změny.

Povinná osoba stanoví, zdokumentuje a uplatňuje postupy, které zamezují výskytu bezpečnostních incidentů v IKT systémech a službách v oblasti informačních a komunikačních technologií a minimalizují jejich dopad na poskytování služeb v této oblasti. Jde mimo jiné o zavedení segmentace sítě, systémů prevence ztráty dat a šifrování síťového provozu, a to v souladu s klasifikací dat [bod 36 písm. c) přílohy]. Pokud jde o zavedení segmentace sítě, je očekáváno, že povinná osoba vytvoří takové virtuální sítě, které omezí přístupy uživatelů přímo k informačním aktivům na serverech a současně vymezí přístupy konkrétních privilegovaných uživatelů jen na určené servery. Ohledně zavedení systémů prevence ztráty dat je očekáváno, že se povinná osoba nespokojí s maticí přístupů pro své uživatele z hlediska jejich rolí, ale zavede systém schopný identifikovat, monitorovat a chránit data *(data loss prevention, DLP).* Umožní jí to detekovat úmyslné nebo neúmyslné neautorizované pokusy uživatelů zkopírovat nebo zaslat citlivé údaje mimo informační systém povinné osoby a těmto pokusům zabránit. K šifrování síťového provozu by mělo být přistoupeno jak při poskytování služeb uživatelům, tak v interní síti. Toto šifrování by však nemělo znemožnit fungování dalších bezpečnostních systémů a technologií povinné osoby, např. DLP.

V souvislosti se zavedením ochrany koncových bodů jako jsou servery, pracovní stanice a mobilní zařízení [bod 36 písm. d) přílohy] by povinná osoba neměla umožňovat jejich přístup do interní sítě, pokud výše uvedená zařízení nesplňují standardy bezpečného nastavení, bezpečných komunikačních protokolů, ochrany proti malwaru apod. Jedním z opatření může být například určení geolokace pro přístup koncových bodů.

Smyslem požadavku na zavedení mechanismů pro ověření integrity softwaru, firmwaru a dat [bod 36 písm. e) přílohy] je, aby povinná osoba počítala se situací, že se neautorizovaná osoba pokusí změnit výše uvedená data. Povinná osoba by proto měla zavést mechanismy, např.

pomocí tvorby a ověřování digitálního otisku textu *(hash)*, který odhalí takovéto změny co nejdříve.

Pokud jde o šifrování uložených a přenášených dat, a to v souladu s klasifikací dat [bod 36 písm. f) přílohy], povinná osoba by měla zajistit, že se citlivé údaje vždy nacházejí na zašifrovaných úložištích a v případě nepovoleného externího přístupu k takovému úložišti nehrozí ztráta důvěrnosti uložených dat.

Ohledně průběžného zjišťování, zda změny stávajícího provozního prostředí ovlivňují stávající bezpečnostní opatření nebo vyžadují přijetí dalších opatření (bod 37 přílohy), by povinná osoba měla postupovat tak, že před každou změnou týkající se poskytovaných služeb, interních procesů, oblasti informačních aktiv a IKT systémů provede kontrolu platnosti a rozsahu registru stávajících rizik a jejich omezování bezpečnostními opatřeními. Případně povinná osoba identifikuje nové hrozby, zranitelnosti a na ně navazující rizika, která bude snižovat nebo jinak ošetřovat novými opatřeními.

Rámec pro testování bezpečnosti informací, který má povinná osoba stanovit a uplatňovat (bod 42 přílohy), tvoří pravidla, postupy a způsoby testování bezpečnosti, které povinná osoba pravidelně provádí svými pracovníky nebo externími poskytovateli. Je přitom důležité, aby osoby, které provádějí textování, nebyly samy zodpovědné za implementaci bezpečnostních opatření v povinné osobě.

Pokud jde o program odborné přípravy v oblasti bezpečnosti (bod 49 přílohy), povinná osoba by měla zavést sérii školení s různým stupněm detailu informací v závislosti na cílové skupině pracovníků včetně pracovníků externích poskytovatelů. Cílem je zvýšit bezpečnostní povědomí o potenciálních hrozbách a rizicích, kterým je povinná osoba vystavena, a opatřeních, které povinná osoba zavedla, včetně způsobů chování vyžadovaných od pracovníků pro zachování bezpečnosti informačních aktiv na co nejvyšší úrovni.

Povinná osoba (bod 50 přílohy) má zdokumentováno, jak provozuje, sleduje a kontroluje svá IKT aktiva.

Sledování a řízení životních cyklů IKT aktiv (bod 55 přílohy) vyžaduje, aby povinná osoba věnovala zvláštní pozornost technologiím a softwaru, které již nejsou podporovány ze strany výrobce. Jejich používáním se totiž může dostat do situace spojené s riziky, která již nepůjde uspokojivě omezit jinými opatřeními. Platí to však i obráceně. Není vhodné nasazovat, jen z důvodu modernosti nebo momentálního trendu, časem a zkušenostmi neprověřená IKT aktiva.

Smyslem opatření k omezení rizika neúmyslné nebo úmyslné změny IKT systémů během vývoje a zavádění v produkčním prostředí (bod 69 přílohy) je provádět vývoj za pomoci nástrojů, které zajistí, že schválený zdrojový kód není možné změnit bez identifikace toho, kdo takovou změnu provedl a následně na příslušné řídicí úrovni schválil. Obdobně v případě již jednou schváleného zdrojového kódu se nesmí stát, že tento kód bude jakkoliv nekontrolovaně měněn, což by následně mohlo vést ke změně funkcionality s negativním dopadem na následně vzniklou aplikaci a na poskytovanou funkcionalitu.

V souvislosti s testováním a schvalováním IKT systémů před jejich prvním použitím (bod 70 přílohy) by si povinná osoba měla stanovit rámec testování, který bude vždy uplatňovat, aby

dosáhla nejvyšší užitečnosti, bezpečnosti a spolehlivosti používaného softwaru. V případně vlastního vývoje může jít například o tzv. unit testování, integrační testování, systémové testování, uživatelské akceptační testování. U nakoupeného softwaru jde například o výkonnostní testování, bezpečnostní testování, regresní testování.

Platební instituce má používat testovací prostředí, které přiměřeně odráží její produkční prostředí (bod 70 přílohy). Pro testování je potřebné mít data co nejvíce podobná reálným datům, aby bylo možné v testování obsáhnout všechny eventuality, které generovaná data nemohou poskytnout. To však není možné plně realizovat, neboť pracovníci zajišťující testování nebudou mít stejnou zodpovědnost jako jiní zainteresovaní pracovníci povinné osoby, a to například ve vztahu k důvěryhodnosti klientských dat. Proto se zpravidla přikročí k anonymizaci dat, aby testování mohlo být co nejrealističtější, ale zároveň nemohlo dojít k úniku dat uživatelů.

Postupy povinné osoby pro pořízení a vývoj IKT systémů by měly zahrnovat také IKT systémy vyvinuté nebo řízené obchodními funkcemi a koncovými uživateli mimo organizaci v oblasti informačních a komunikačních technologií (bod 74 přílohy). Důvodem je skutečnost, že pracovníci zpravidla mívají možnost nad rámec existujících IKT systémů přicházet s vlastními inovacemi, které zjednoduší jejich práci a které se z nějakého důvodu nemohly dostat do IKT systémů. I o takových aplikacích je nutné vědět a řídit jejich vývoj a používání, neboť mohou být zdrojem rizik, například úniku informací povinné osoby.

Povinná osoba řídí kontinuitu činností (bod 77 přílohy). Stanovuje si podmínky, za kterých je pro ni výhodné kontinuálně poskytovat své služby. Na základě těchto podmínek vytvoří sadu plánů, které jí umožní reagovat na přerušení činnosti, aniž by dané podmínky porušila a vystavila se tak ztrátě, které se ve svém plánovacím procesu vystavit nechtěla.

Analýza dopadu na podnikatelskou činnost *(Business Impact Analysis, BIA)* je součástí řízení kontinuity činností (bod 78 přílohy). Z ní by měly jasně vyplynout vztahy mezi obchodními funkcemi, kritickými činnostmi, informačními aktivy, IKT systémy apod. a potenciálně realizovanou ztrátou vyplývající z přerušení fungování některého výše uvedeného procesu, aktiva nebo systému. Jedním z výstupů této analýzy je i identifikace scénářů, kdy mohou nejvážnější výpadky v činnosti nastat.

Ze srovnání IKT systémů a služeb v oblasti informačních a komunikačních technologií s analýzou dopadu na podnikatelskou činnost může vyplynout, že stávající architektura IKT systémů a služeb nenaplňuje podmínky stanovené povinnou osobou na kontinuitu činností. V takovém případě je nutné přikročit k jejich odpovídající změně, například cestou redundance některých kritických komponent, a tím naplnit požadavek na sladění IKT systémů a služeb v oblasti informačních a komunikačních technologií s analýzou dopadu na podnikatelskou činnost (bod 79 přílohy).

Plány reakce a obnovy by měly zohledňovat alternativní možnosti v případech, kdy obnova nemusí být z krátkodobého hlediska proveditelná (bod 85 přílohy). Povinná osoba by měla zvážit alternativní možnosti poskytování služeb nebo alespoň vypořádání již iniciovaných transakcí. K tomu lze využít cesty odlišné od hlavních IKT systémů povinné osoby. Lze

použít dokumentaci procesů pro jednotlivé obchodní funkce, informace o transakcích zaslané úvěrovým institucím apod.

Článek II

Účinnost vyhlášky se navrhuje od 1. července 2022.