EBA/GL/2019/02

25. února 2019

Obecné pokyny k outsourcingu

1. Dodržování předpisů a oznamovací povinnosti

Status těchto obecných pokynů

1. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010. [1] V souladu s čl. 16 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 příslušné orgány a finanční instituce vynaloží veškeré úsilí, aby se těmito obecnými pokyny řídily.

2. Obecné pokyny formulují názor orgánu EBA na náležité postupy dohledu v rámci Evropského systému dohledu nad finančním trhem nebo na to, jak by unijní právní předpisy měly být uplatňovány v konkrétní oblasti. Příslušné orgány ve smyslu čl. 4 odst. 2 nařízení (EU) č. 1093/2010, na které se tyto obecné pokyny vztahují, by se jimi měly řídit a začlenit je do svých postupů (např. pozměněním svého právního rámce nebo dohledových postupů), včetně případů, kdy jsou obecné pokyny zaměřeny v prvé řadě na instituce a platební instituce.

Oznamovací povinnosti

3. V souladu s čl. 16 odst. 3 nařízení (EU) č. 1093/2010 musí příslušné orgány do ([dd. mm. rrrr]) orgánu EBA oznámit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést do tohoto data důvody, proč se jimi neřídí či nehodlají řídit. Neposkytnou-li příslušné orgány oznámení v této lhůtě, bude mít orgán EBA za to, že se těmito obecnými pokyny neřídí nebo nehodlají řídit. Oznámení by měla být zasílána na formuláři, který je k dispozici na internetových stránkách orgánu EBA, na adresu compliance@eba.europa.eu s označením „EBA/GL/2019/02“. Oznámení by měly předložit osoby s příslušným oprávněním oznamovat, zda se jejich příslušné orgány těmito obecnými pokyny řídí nebo hodlají řídit. Jakoukoli změnu stavu dodržování obecných pokynů je rovněž nutno oznámit orgánu EBA.

4. Oznámení budou zveřejněna na internetových stránkách orgánu EBA v souladu s čl. 16 odst. 3.

[1] Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331 15.12.2010, s. 12).

2. Předmět, oblast působnosti a definice

Předmět

5. Tyto obecné pokyny vymezují vnitřní systémy správy a řízení (řídicí a kontrolní systémy), včetně řádného řízení rizik, které by instituce, platební instituce a instituce elektronických peněz měly zavést při externím zajišťování služeb nebo činností (outsourcingu), zejména v souvislosti s outsourcingem kritických nebo důležitých funkcí.

6. Obecné pokyny vymezují, jak by vnitřní systémy zmíněné v předchozím odstavci měly být kontrolovány a monitorovány příslušnými orgány v souvislosti s článkem 97 směrnice 2013/36/EU[2] – Procesem dohledu a hodnocení (SREP), čl. 9 odst. 3 směrnice (EU) 2015/2366 [3] a čl. 5 odst. 5 směrnice 2009/110/ES[4] při plnění jejich povinnosti sledovat trvalé dodržování podmínek uděleného povolení ze strany subjektů, jimž jsou tyto obecné pokyny určeny.

Určení

7. Tyto obecné pokyny jsou určeny příslušným orgánům ve smyslu čl. 4 odst. 1 bodu 40 nařízení (EU) č. 575/2013[5], včetně Evropské centrální banky, pokud jde o záležitosti týkající se úkolů jí svěřených nařízením (EU) č. 1024/2013[6], institucím ve smyslu čl. 4 odst. 1 bodu 3 nařízení (EU) č. 575/2013, platebním institucím ve smyslu čl. 4 odst. 4 směrnice (EU) 2015/2366 a institucím elektronických peněz ve smyslu čl. 2 odst. 1 směrnice 2009/110/ES. Tyto obecné pokyny se v souladu s článkem 33 níže uvedené směrnice nevztahují na poskytovatele služeb informování o účtu, kteří poskytují pouze službu v bodě 8 přílohy I směrnice (EU) 2015/2366.

8. Pro účely těchto obecných pokynů jakýkoli odkaz na „platební instituce“ zahrnuje „instituce elektronických peněz“ a jakýkoli odkaz na „platební služby“ zahrnuje „vydávání elektronických peněz“.

---

[2] Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES.

[3] Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, o změně směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a o zrušení směrnice 2007/64/ES.

[4] Směrnice Evropského parlamentu a Rady 2009/110/ES ze dne 16. září 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností, o změně směrnic 2005/60/ES a 2006/48/ES a o zrušení směrnice 2000/46/ES.

[5] Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 176, 27.6.2013, s. 1).

[6] Nařízení Rady (EU) č. 1024/2013 ze dne 15. října 2013, kterým se Evropské centrální bance svěřují zvláštní úkoly týkající se politik, které se vztahují k obezřetnostnímu dohledu nad úvěrovými institucemi.

Oblast působnosti

9. Aniž je dotčena směrnice 2014/65/EU [7] a nařízení Komise v přenesené pravomoci (EU) 2017/565 [8] (které obsahuje požadavky týkající se outsourcingu prováděného institucemi poskytujícími investiční služby a vykonávajícími investiční činnosti i příslušné pokyny vydané Evropským orgánem pro cenné papíry a trhy k investičním službám a činnostem), měly by instituce definované v čl. 3 odst. 1 bodě 3 směrnice 2013/36/EU tyto obecné pokyny dodržovat na individuálním, subkonsolidovaném a konsolidovaném základě. Příslušné orgány mohou od uplatňování na individuálním základě upustit na základě článku 21 směrnice 2013/36/EU nebo čl. 109 odst. 1 směrnice 2013/36/EU ve spojení s článkem 7 nařízení (EU) č. 575/2013. Instituce, na které se vztahuje směrnice 2013/36/EU, by měly dodržovat tuto směrnici a tyto obecné pokyny na konsolidovaném a subkonsolidovaném základě, jak je stanoveno v článku 21 a v článcích 108 až 110 směrnice 2013/36/EU.

10. Aniž je dotčen čl. 8 odst. 3 směrnice (EU) 2015/2366 a čl. 5 odst. 7 směrnice 2009/110/ES, měly by platební instituce a instituce elektronických peněz tyto obecné pokyny dodržovat na individuálním základě.

11. Těmito obecnými pokyny by se měly řídit příslušné orgány odpovědné za dohled nad institucemi, platebními institucemi a institucemi elektronických peněz.

Definice

12. Není-li uvedeno jinak, mají pojmy použité a vymezené ve směrnici 2013/36/EU, nařízení (EU) č. 575/2013, směrnici 2009/110/ES, směrnici (EU) 2015/2366 a v obecných pokynech orgánu EBA k vnitřnímu systému správy a řízení[9] v těchto obecných pokynech stejný význam. Kromě toho se pro účely těchto obecných pokynů použijí tyto definice:

Externí zajištění služeb nebo činností (outsourcing)	znamená jakékoli ujednání mezi institucí, platební institucí nebo institucí elektronických peněz a poskytovatelem služeb, na jehož základě dotyčný poskytovatel služeb vykonává proces, službu nebo činnost, které by jinak byly prováděny samotnou institucí, platební institucí nebo institucí elektronických peněz.
Funkce	znamená procesy, služby nebo činnosti.

[7] Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU, (Úř. věst. L 173, 12.6.2014, s. 349).

[8] Nařízení Komise v přenesené pravomoci (EU) 2017/565 ze dne 25. dubna 2016, kterým se doplňuje směrnice Evropského parlamentu a Rady 2014/65/EU, pokud jde o organizační požadavky a provozní podmínky investičních podniků a o vymezení pojmů pro účely zmíněné směrnice (Úř. věst. L 87, 31.3.2017, s. 1).

[9] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

Kritická nebo důležitá funkce[10]	znamená jakoukoli funkci, která je považována za kritickou nebo důležitou, jak je stanoveno v oddílu 4 těchto obecných pokynů.
Navazující externí zadávání (“řetězový outsourcing”)	znamená situaci, kdy poskytovatel služeb v souladu s ujednáním o outsourcingu dále přenese externí zajišťování funkce na jiného poskytovatele služeb.[11]
Poskytovatel služeb	znamená třetí stranu, která na základě ujednání o outsourcingu provádí externí zajišťování procesu, služby nebo činnosti nebo jejich části.
Cloudové služby	znamenají služby poskytované za použití cloud computingu, což je model, který umožňuje pohodlný síťový přístup kdykoliv a odkudkoliv ke sdílené množině konfigurovatelných výpočetních zdrojů (např. sítím, serverům, úložištím, aplikacím a službám), které lze rychle poskytnout či uvolnit s vynaložením minimálních nároků na jejich správu anebo zásahy ze strany poskytovatele služby.
Veřejný cloud	znamená cloudovou infrastrukturu, kterou může volně využívat široká veřejnost.
Soukromý cloud	znamená cloudovou infrastrukturu, kterou může výlučně využívat jediná instituce nebo platební instituce.
Komunitní cloud	znamená cloudovou infrastrukturu, kterou může výlučně využívat konkrétní komunita institucí nebo platebních institucí, včetně několika institucí v jedné skupině.
Hybridní cloud	znamená cloudovou infrastrukturu, která se skládá ze dvou či více různých cloudových infrastruktur.
Vedoucí orgán	znamená orgán nebo orgány instituce nebo platební instituce, které jsou jmenovány podle vnitrostátních právních předpisů, jsou oprávněny stanovovat strategii, cíle a celkové směřování instituce nebo platební instituce a které kontrolují a sledují rozhodování osob ve vedení a jejímiž členy jsou osoby, které skutečně řídí činnost instituce nebo platební instituce, a vedoucí pracovníci a osoby odpovědné za řízení platební instituce.

[10] Pojem „kritická nebo důležitá funkce“ vychází z pojmu používaného podle směrnice 2014/65/EU (MiFID II) a nařízení Komise v přenesené pravomoci (EU) 2017/565, kterým se doplňuje MiFID II, a používá se pouze pro účely outsourcingu; nesouvisí s definicí „zásadních funkcí“ pro účely rámce pro ozdravné postupy a řešení krize podle vymezení na základě čl. 2 odst. 1 bodu 35 směrnice 2014/59/EU (BRRD).

[11] Posouzení se provádí podle ustanovení oddílu 3; navazující externí zadávání bylo v jiných dokumentech orgánu EBA rovněž označováno jako „řetězec externího zajištění“ nebo „řetězové externí zajištění činností“.

3. Provádění

Datum použití

13. S výjimkou odst. 63 písm. b) se tyto obecné pokyny použijí od 30. září 2019 na všechna ujednání o outsourcingu uzavřená, podrobená přezkumu nebo pozměněná k tomuto datu nebo po něm. Ustanovení odst. 63 písm. b) se použije od 31. prosince 2021.

14. Instituce a platební instituce by měly provést přezkum stávajících ujednání o outsourcingu a upravit je tak, aby byla v souladu s těmito obecnými pokyny.

15. Nebude-li přezkum ujednání o outsourcingu kritických nebo důležitých funkcí dokončen do 31. prosince 2021, měly by instituce a platební instituce o této skutečnosti informovat svoje příslušné orgány, včetně opatření plánovaných za účelem naplnění revize nebo případné ústupové strategie.

Přechodná ustanovení

16. Instituce a platební instituce by měly plně zdokumentovat všechna stávající ujednání o outsourcingu, s výjimkou ujednání o outsourcingu s poskytovateli cloudových služeb, v souladu s těmito obecnými pokyny po prvním datu obnovení každého stávajícího ujednání o outsourcingu, avšak nejpozději do 31. prosince 2021.

Zrušení

17. S účinkem od 30. září 2019 se zrušují obecné pokyny Evropského výboru orgánů bankovního dohledu (CEBS) o outsourcingu ze dne 14. prosince 2006 a doporučení orgánu EBA ohledně zajištění cloudových služeb u externích poskytovatelů[12].

[12] Doporučení ohledně zajištění cloudových služeb u externích poskytovatelů (EBA/REC/2017/03).

4. Obecné pokyny k outsourcingu

Hlava I – Proporcionalita: uplatnění ve skupině a institucionální systémy ochrany

1 Proporcionalita

18. Instituce, platební instituce a příslušné orgány by při dodržování těchto obecných pokynů nebo dohledu nad jejich dodržováním měly přihlížet k zásadě proporcionality. Zásada proporcionality má zajistit, aby systémy správy a řízení, včetně těch, které se týkají outsourcingu (externího zajištění služeb nebo činností), odpovídaly individuálnímu rizikovému profilu, povaze a obchodnímu modelu instituce nebo platební instituce a rozsahu a složitosti jejich činností tak, aby bylo efektivně dosaženo cílů regulačních požadavků.

19. Při uplatňování požadavků stanovených v těchto obecných pokynech by instituce a platební instituce měly přihlížet ke složitosti externě zajišťovaných funkcí, rizikům vyplývajícím z ujednání o outsourcingu, kritické významnosti nebo důležitosti externě zajišťované funkce a potenciálnímu dopadu outsourcingu na kontinuitu jejich činností.

20. Při uplatňování zásady proporcionality by měly instituce, platební instituce[13] a příslušné orgány přihlížet ke kritériím vymezeným v hlavě I obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení v souladu s čl. 74 odst. 2 směrnice 2013/36/EU.

2 Využívání outsourcingu skupinami a institucemi, které jsou členy institucionálního systému ochrany

21. Podle čl. 109 odst. 2 směrnice 2013/36/EU by se tyto obecné pokyny měly používat také na subkonsolidovaném a konsolidovaném základě, s přihlédnutím k obezřetnostnímu rozsahu konsolidace.[14] Za tímto účelem by mateřské podniky v EU nebo mateřský podnik v členském státě měly zajistit, aby vnitřní systémy, procesy a mechanismy správy a řízení v jejich dceřiných společnostech, včetně platebních institucí, byly jednotné, náležitě integrované a přiměřené pro účely účinného uplatňování těchto obecných pokynů na všech příslušných úrovních.

---

[13] Platební instituce by měly rovněž zohlednit obecné pokyny Evropského orgánu pro bankovnictví podle směrnice o platebních službách (PSD2) k informacím poskytovaným při udělování povolení platebním institucím a institucím elektronických peněz a registraci poskytovatelů služeb informování o účtu, které jsou k dispozici na internetových stránkách orgánu EBA na adrese https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

[14] Viz čl. 4 odst. 1 body 47 a 48 nařízení (EU) ohledně rozsahu konsolidace.

22. Instituce a platební instituce podle odstavce 21 a instituce, které jako členové institucionálního systému ochrany používají centrálně poskytované systémy správy a řízení, by měly dodržovat následující:

    a. v případě, že takové instituce nebo platební instituce mají ujednání o outsourcingu s poskytovateli služeb v rámci skupiny nebo institucionálního systému ochrany[15], nese vedoucí orgán takových institucí nebo platebních institucí i u těchto ujednání o outsourcingu plnou odpovědnost za splnění všech regulačních požadavků a účinné uplatňování těchto obecných pokynů;

    b. v případě, že tyto instituce nebo platební instituce externě zajišťují provozní úkoly funkcí vnitřní kontroly u poskytovatele služeb v rámci skupiny nebo institucionálního systému ochrany, měly by za účelem monitorování a auditu ujednání o outsourcingu instituce zajistit, aby i u těchto ujednání o outsourcingu byly tyto provozní úkoly účinně prováděny, a to i prostřednictvím příslušných obdržených zpráv.

23. Instituce a platební instituce v rámci skupiny, které nebyly uděleny žádné výjimky na základě článku 109 směrnice 2013/36/EU a článku 7 nařízení (EU) č. 575/2013, instituce, které jsou ústředním subjektem nebo jsou trvale přidružené k ústřednímu subjektu, kterému nebyly uděleny žádné výjimky na základě článku 21 směrnice 2013/36/EU, nebo instituce, které jsou členy institucionálního systému ochrany, by měly vedle ustanovení odstavce 22 přihlížet k následujícímu:

    a. v případě, že je provozní monitorování outsourcingu centralizované (např. jako součást rámcové smlouvy o monitorování ujednání o outsourcingu), měly by instituce a platební instituce zajistit, aby bylo přinejmenším u externě zajišťovaných kritických nebo důležitých funkcí možné nezávislé monitorování poskytovatele služeb i náležitý dohled ze strany každé instituce nebo platební instituce, a to i prostřednictvím přijímaných zpráv, které budou předloženy nejméně jednou ročně a na žádost centralizované monitorovací funkce a které budou obsahovat alespoň shrnutí hodnocení rizik a monitorování výsledků. Kromě toho by instituce a platební instituce měly od centralizované monitorovací funkce obdržet shrnutí relevantních zpráv o auditu outsourcingu kritických nebo důležitých funkcí a na požádání i úplnou zprávu o auditu;

    b. instituce a platební instituce by měly zajistit, že bude jejich vedoucí orgán řádně informován o příslušných plánovaných změnách týkajících se poskytovatelů služeb, které jsou monitorovány centrálně, a o potenciálním dopadu těchto změn na kritické nebo důležité zajišťované funkce, včetně shrnutí analýzy rizik zahrnující právní rizika, dodržování regulačních požadavků a dopadu na úrovně služeb, aby mohly posoudit dopad těchto změn;

[15] Podle čl. 113 odst. 7 nařízení o kapitálových požadavcích (CRR) institucionální systém ochrany znamená smluvní nebo právními předpisy stanovenou dohodu o závazku, která chrání instituce, jež jsou členem systému, a zejména zajišťuje jejich likviditu a platební schopnost, aby nedošlo k úpadku, pokud to je nezbytné.

c. v případě, že se tyto instituce a platební instituce v rámci skupiny, instituce přidružené k ústřednímu subjektu nebo instituce, které jsou součástí institucionálního systému ochrany, spoléhají na centrální posouzení ujednání o outsourcingu, které bylo provedeno před samotným outsourcingem, jak se uvádí v oddílu 12, měla by každá instituce a platební instituce obdržet shrnutí takového posouzení a zajistit, aby zohledňovala její specifickou strukturu a rizika v rámci rozhodovacího procesu;

d. v případě, že je v rámci skupiny nebo institucionálního systému ochrany zřízena a centrálně vedena evidence všech existujících ujednání o outsourcingu, jak je uvedeno v oddílu 11, měly by mít příslušné orgány, všechny instituce a platební instituce možnost získat svoji individuální dokumentaci bez zbytečného prodlení. Tato evidence by měla obsahovat všechna ujednání o outsourcingu, včetně ujednání o outsourcingu s poskytovateli služeb uvnitř skupiny nebo institucionálního systému ochrany;

e. v případě, že se takové instituce a platební instituce spoléhají na plán odstoupení pro kritické nebo důležité funkce, který je ustanoven na úrovni skupiny, v rámci institucionálního systému ochrany nebo ze strany ústředního subjektu, měly by všechny instituce a platební instituce obdržet shrnutí plánu a být ujištěny o tom, že lze plán účinně provést.

24. Pokud byly uděleny výjimky podle článku 21 směrnice 2013/36/EU nebo čl. 109 odst. 1 směrnice 2013/36/EU ve spojení s článkem 7 nařízení (EU) č. 575/2013, měla by být ustanovení těchto obecných pokynů uplatněna mateřským podnikem v členském státě na tento samotný podnik a na jeho dceřiné společnosti, nebo ústředním subjektem a jeho přidruženými společnostmi jako celkem.

25. Instituce a platební instituce, které jsou dceřinými společnostmi mateřského podniku v EU nebo mateřského podniku v členském státě, jemuž nebyly uděleny žádné výjimky na základě článku 21 směrnice 2013/36/EU nebo čl. 109 odst. 1 směrnice 2013/36/EU ve spojení s článkem 7 nařízení (EU) č. 575/2013, by měly zajistit, aby tyto obecné pokyny individuálně dodržovaly.

Hlava II – Posouzení ujednání o outsourcingu

3 Externí zajištění služeb nebo činností (outsourcing)

26. Instituce a platební instituce by měly určit, zda spadá ujednání s třetí stranou do definice externího zajištění služeb nebo činností. V rámci tohoto posouzení by mělo být zohledněno, zda je funkce (nebo její část) externě zajišťovaná u poskytovatele služeb vykonávána poskytovatelem služeb opakovaně nebo průběžně a zda by tato funkce (nebo její část) normálně spadala do oblasti působnosti funkcí, které by byly nebo mohly být realisticky vykonávány institucemi nebo platebními institucemi, a to i v případě, že instituce nebo platební instituce tuto funkci v minulosti sama nevykonávala.

27. Pokud ujednání s poskytovatelem služeb zahrnuje více funkcí, měly by instituce a platební instituce v rámci svého posouzení zvážit všechny aspekty ujednání, např. jestliže poskytovaná služba zahrnuje poskytování hardwaru pro uchování údajů a zálohování údajů, měly by být oba aspekty posouzeny společně.

28. Obecně by instituce a platební instituce neměly za outsourcing považovat následující:

    a. funkci, kterou má podle právních předpisů vykonávat poskytovatel služeb, např. povinný audit;

    b. služby poskytování informací o trhu (např. poskytování údajů společnostmi Bloomberg, Moody's, Standard & Poor's, Fitch);

    c. globální síťové infrastruktury (např. Visa, MasterCard);

    d. systémy zúčtování a vypořádání mezi zúčtovacími institucemi, ústředními protistranami a institucemi zajišťujícími vypořádání a jejich členy;

    e. globální infrastruktury poskytující údaje o finančních transakcích, které jsou předmětem dohledu vykonávaného příslušnými orgány;

    f. služby korespondenčního bankovnictví; a

    g. získávání služeb, které by jinak instituce nebo platební instituce neposkytovaly (např. poradenství od architekta, poskytnutí právního stanoviska a zastoupení u soudu a správních orgánů, úklid, zahradní práce a údržba prostor instituce nebo platební instituce, zdravotní služby, servis podnikových vozů, stravování, služby prodejních automatů, kancelářské služby, cestovní služby, služby podatelen, recepční, sekretářky a spojovatelky), zboží (např. plastové karty, čtečky karet, kancelářské potřeby, osobní počítače, nábytek) nebo dodávky veřejných služeb (např. elektřiny, plynu, vody, telefonních linek).

4 Kritické nebo důležité funkce

29. Instituce a platební instituce by měly vždy považovat funkci za kritickou nebo důležitou v následujících situacích:[16]

    a. v případě, že by její nesprávné plnění nebo neplnění vážně ohrozily:

        i. trvalé splňování podmínek vyplývajících z jejich povolení či jiných povinností podle směrnice 2013/36/EU, nařízení (EU) č. 575/2013, směrnice 2014/65/EU,

[16] Viz rovněž článek 30 nařízení Komise v přenesené pravomoci (EU) č. 2017/565 ze dne 25. dubna 2016, kterým se doplňuje směrnice Evropského parlamentu a Rady 2014/65/EU, pokud jde o organizační požadavky a provozní podmínky investičních podniků a o vymezení pojmů pro účely zmíněné směrnice.

směrnice (EU) 2015/2366 a směrnice 2009/110/ES a jejich regulačních povinností;

ii. jejich finanční výkonnost; nebo

iii. zdraví či kontinuitu jejich bankovních a platebních služeb a činností;

b. v případě, že jsou externě zajišťovány provozní úkoly funkcí vnitřní kontroly, pokud není při posouzení určeno, že by neposkytování externě zajišťované funkce nebo nesprávné poskytování externě zajišťované funkce nemělo mít nepříznivý dopad na účinnost funkce vnitřní kontroly;

c. jestliže mají v úmyslu externě zajišťovat bankovní činnosti nebo platební služby v rozsahu, který by vyžadoval povolení[17] ze strany příslušného orgánu, jak se uvádí v oddílu 12.1.

30. V případě institucí by měla být zvláštní pozornost věnována posouzení kritické významnosti nebo důležitosti funkcí, jestliže se outsourcing týká funkcí souvisejících s hlavními liniemi podnikání a kritických funkcí podle vymezení v čl. 2 odst. 1 bodě 35 a čl. 2 odst. 1 bodě 36 směrnice 2014/59/EU[18] a určeny institucemi s použitím kritérií vymezených v článcích 6 a 7 nařízení Komise v přenesené pravomoci (EU) 2016/778.[19] Funkce, které jsou nezbytné k provádění hlavních linií podnikání nebo kritických funkcí, by měly být pro účely těchto obecných pokynů považované za kritické nebo důležité funkce, pokud není při posuzování institucí určeno, že by neposkytování externě zajišťované funkce nebo nesprávné poskytování externě zajišťované funkce nemělo mít nepříznivý dopad na provozní kontinuitu hlavní linie podnikání nebo kritické funkce.

31. Při posuzování toho, zda se ujednání o outsourcingu týká funkce, která je kritická nebo důležitá, by instituce a platební instituce měly spolu s výsledkem hodnocení rizik uvedeným v oddílu 12.2 přihlížet alespoň k následujícím faktorům:

a. zda ujednání o outsourcingu přímo souvisí s poskytováním bankovních činností nebo platebních služeb[20], k nimž mají povolení;

b. potenciální dopad případného narušení externě zajišťované funkce nebo soustavného neposkytování služby poskytovatelem služby na dohodnutých úrovních služeb na jejich:

---

[17] Viz činnosti uvedené v příloze I směrnice 2013/36/EU.

[18] Směrnice Evropského parlamentu a Rady 2014/59/EU ze dne 15. května 2014, kterou se stanoví rámec pro ozdravné postupy a řešení krize úvěrových institucí a investičních podniků a kterou se mění směrnice Rady 82/891/EHS a směrnice 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EU, 2012/30/EU a 2013/36/EU a nařízení (EU) č. 1093/2010 a (EU) č. 648/2012 (Úř. věst. L 173, 12.6.2014, s. 190).

[19] Nařízení Komise v přenesené pravomoci (EU) 2016/778 ze dne 2. února 2016, kterým se doplňuje směrnice Evropského parlamentu a Rady 2014/59/EU, pokud jde o okolnosti a podmínky, za nichž lze úplně nebo částečně odložit úhradu mimořádných následných příspěvků, o kritéria pro určení činností, služeb a operací v souvislosti se zásadními funkcemi a o kritéria pro určení oborů podnikání a souvisejících služeb v souvislosti s hlavními liniemi podnikání (Úř. věst. L 131, 20.5.2016, s. 41).

[20] Viz činnosti uvedené v příloze I směrnice 2013/36/EU.

i. krátkodobou a dlouhodobou finanční odolnost a životaschopnost, případně včetně aktiv, kapitálu, nákladů, financování, likvidity, příjmů a ztrát;

ii. kontinuitu činnosti a provozní odolnost;

iii. operační riziko, včetně rizika chování, informačních a komunikačních technologií (IKT) a právního rizika;

iv. rizika poškození pověsti;

v. případné ozdravné plány a plány řešení krize, způsobilost k řešení krize a provozní kontinuitu při včasném zásahu, obnově nebo řešení krize;

c. potenciální dopad ujednání o outsourcingu na jejich schopnost:

i. identifikovat, monitorovat a řídit všechna rizika;

ii. plnit všechny právní a regulační požadavky;

iii. provádět vhodné audity týkající se externě zajišťované funkce;

d. potenciální dopad na služby poskytované klientům;

e. všechna ujednání o outsourcingu, souhrnnou expozici instituce nebo platební instituce vůči stejnému poskytovateli služeb a potenciální kumulativní dopad ujednání o outsourcingu ve stejné oblasti podnikání;

f. rozsah a složitost dotčené oblasti podnikání;

g. možnost, že by navrhované ujednání o outsourcingu bylo možné rozšířit, aniž by došlo k nahrazení nebo revizi související dohody;

h. schopnost převést ujednání o outsourcingu na jiného poskytovatele služeb, je-li to nezbytné nebo žádoucí, a to smluvně i v praxi, včetně předpokládaných rizik, překážek bránících kontinuitě činnosti, nákladů a časového rámce pro takový převod („nahraditelnost“);

i. schopnost znovu včlenit externě zajišťovanou funkci do instituce nebo platební instituce, je-li to nezbytné nebo žádoucí;

j. ochrana údajů a potenciální dopad porušení důvěrnosti informací nebo nezajištění dostupnosti a integrity údajů na instituci nebo platební instituci a její klienty, mimo jiné včetně dodržování nařízení (EU) 2016/679[21].

[21] Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně údajů).

Hlava III – Rámec správy a řízení

5 Řádné systémy správy a řízení a riziko třetí strany

32. Jako součást celkového rámce vnitřní kontroly[22], včetně mechanismů vnitřní kontroly[23], by měly mít instituce a platební instituce ucelený rámec řízení rizik v celé instituci, který zahrnuje všechny linie podnikání a vnitřní oddělení. Podle tohoto rámce by instituce a platební instituce měly určovat a řídit všechna svoje rizika, včetně rizik způsobených ujednáními s třetími stranami. Rámec řízení rizik by měl rovněž institucím a platebním institucím umožňovat přijímat informovaná rozhodnutí o podstupování rizik a zajišťovat, aby byla vhodně prováděna opatření k řízení rizik, a to i v souvislosti s kybernetickými riziky.[24]

33. Instituce a platební instituce by s přihlédnutím k zásadě proporcionality v souladu s oddílem 1 měly určit, hodnotit, monitorovat a řídit všechna rizika vyplývající z ujednání s třetími stranami, jimž jsou nebo mohou být vystaveny, bez ohledu na to, zda jsou tato ujednání ujednáními o outsourcingu, či nikoli. Rizika, zejména operační rizika, která vyplývají ze všech ujednání s třetími stranami, včetně ujednání zmíněných v odstavcích 26 a 28, by měla být hodnocena v souladu s oddílem 12.2.

34. Instituce a platební instituce by měly zajistit, aby splňovaly všechny požadavky nařízení (EU) 2016/679, a to včetně svých ujednání s třetími stranami a ujednání o outsourcingu.

6 Řádné systémy správy a řízení a outsourcing

35. Externí zajištění funkcí nesmí vést k přenesení povinností vedoucího orgánu. Instituce a platební instituce zůstávají plně odpovědnými za dodržování všech svých regulačních povinností, včetně schopnosti dohlížet na externí zajištění kritických nebo důležitých funkcí.

36. Vedoucí orgán nese vždy plnou odpovědnost přinejmenším za:

    a. zajištění toho, že instituce nebo platební instituce průběžně splňuje podmínky, které musí dodržovat, aby jí bylo ponecháno povolení, včetně případných podmínek stanovených příslušným orgánem;

    b. vnitřní organizaci instituce nebo platební instituce;

    c. určení, posouzení a řízení střetu zájmů;

---

[22] Instituce se odkazují na hlavu V obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení.

[23] Viz rovněž článek 11 směrnice 2015/2366 (PSD2).

[24] Viz rovněž obecné pokyny Evropského orgánu pro bankovnictví k informačním a komunikačním technologiím a řízení bezpečnostních rizik (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) a základní prvky G7 pro řízení kybernetických rizik třetí strany ve finančním sektoru (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

d. stanovení strategií a politiky instituce nebo platební instituce (např. obchodní model, ochota podstupovat rizika, rámec řízení rizik);

e. dohled na běžné řízení instituce nebo platební instituce, včetně řízení všech rizik spojených s outsourcingem; a

f. kontrolní úlohu vedoucího orgánu v rámci jeho kontrolní funkce, včetně dohledu a monitorování rozhodování vedení.

37. Outsourcing by neměl vést ke snížení požadavků na způsobilost, které jsou uplatňovány na členy vedoucího orgánu instituce, vedoucí pracovníky, osoby odpovědné za řízení platební instituce a osoby v klíčových funkcích. Instituce a platební instituce by měly mít odpovídající způsobilost a dostatečné a vhodné odborné zdroje k zajištění řádného řízení a dohledu, pokud jde o ujednání o outsourcingu.

38. Instituce a platební instituce by měly:

a. jasně určit odpovědnost za dokumentaci, řízení a kontrolu ujednání o outsourcingu;

b. přidělit dostatečné zdroje k zajištění dodržování všech právních a regulačních požadavků, včetně těchto obecných pokynů a dokumentace a monitorování všech ujednání o outsourcingu;

c. s přihlédnutím k oddílu 1 těchto obecných pokynů zřídit funkci outsourcingu nebo určit vedoucího pracovníka, který je přímo odpovědný vedoucímu orgánu (např. osoba v klíčové funkci v rámci kontrolní funkce) a nese odpovědnost za řízení rizik souvisejících s ujednáními o outsourcingu a za dohled nad těmito riziky vykonávaný v rámci vnitřní kontroly instituce a za dohled nad dokumentací k ujednání o outsourcingu. Malé a méně složité instituce nebo platební instituce by měly přinejmenším zajistit jasné rozdělení úkolů a povinností ohledně řízení a kontroly ujednání o outsourcingu a mohou funkci outsourcingu přidělit členovi vedoucího orgánu instituce nebo platební instituce.

39. Instituce a platební instituce by si měly vždy zachovávat dostatečný obsah a neměly by se stávat „prázdnou skořápkou“ nebo „subjektem typu poštovní schránka“. Za tímto účelem by měly:

a. vždy splňovat všechny podmínky svého povolení[25], včetně toho, že vedoucí orgán účinně vykonává svoje povinnosti, jak stanovuje odstavec 36 těchto obecných pokynů;

[25] Viz rovněž regulační technické normy podle čl. 8 odst. 2 směrnice 2013/36/EU o informacích, které mají být poskytnuty pro udělení povolení k výkonu činnosti úvěrových institucí a prováděcí technické normy podle čl. 8 odst. 3 směrnice 2013/36/EU o standardních formulářích, šablonách a postupech pro poskytování informací požadovaných pro udělení povolení k výkonu činnosti úvěrových institucí (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

V případě platebních institucí viz obecné pokyny Evropského orgánu pro bankovnictví k informacím, které mají být poskytnuty pro udělení povolení k výkonu činnosti platebních institucí a institucí elektronických peněz a k registraci poskytovatelů služeb informování o účtu podle směrnice (EU) 2015/2366 (PSD2) (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

b. zachovat jasný a transparentní organizační rámec a strukturu umožňující jim zajistit dodržování právních a regulačních požadavků;

c. v případě externího zajištění funkcí vnitřní kontroly (např. v případě outsourcingu v rámci skupiny nebo outsourcingu v rámci institucionálních systémů ochrany) vykonávat náležitý dohled a být schopny řídit rizika vyplývající z externího zajištění kritických nebo důležitých funkcí; a

d. mít dostatečné zdroje a kapacity k zajištění dodržování ustanovení písmene a) až c).

40. Při outsourcingu by instituce a platební instituce měly přinejmenším zajistit, aby:

a. mohly přijímat a provádět rozhodnutí týkající se jejich obchodních činností a kritických nebo důležitých funkcí, včetně těch, které jsou zajišťovány externě;

b. zajišťovaly řádný průběh svého podnikání a bankovních a platebních služeb, které poskytují;

c. rizika související se současnými a plánovanými ujednáními o outsourcingu byla řádně určena, vyhodnocena, řízena a zmírňována, včetně rizik týkající se informačních a komunikačních technologií a finančních technologií;

d. byla zavedena vhodná opatření k zachování důvěrnosti údajů a dalších informací;

e. byl udržován vhodný tok relevantních informací mezi institucí nebo platební institucí a poskytovateli služeb;

f. v souvislosti s externím zajišťováním kritických nebo důležitých funkcí byly schopny v přiměřeném časovém rámci provést přinejmenším jedno z následující opatření:

i. převést funkci na alternativní poskytovatele služeb;

ii. znovu funkci včlenit do instituce nebo platební instituce; nebo

iii. přestat vykonávat obchodní činnosti, které závisejí na takové funkci.

g. v případě, že jsou osobní údaje zpracovány poskytovateli služeb nacházejícími se v EU a/nebo třetích zemích, byla zavedena odpovídající opatření a údaje byly zpracovány v souladu s nařízením (EU) 2016/679.

7 Zásady pro outsourcing

41. Vedoucí orgán instituce nebo platební instituce[26], který má platná ujednání o outsourcingu nebo plánuje taková ujednání uzavřít, by měl schválit, pravidelně přezkoumávat a aktualizovat písemné zásady pro outsourcing a zajistit jejich provádění podle potřeby na individuálním, subkonsolidovaném a konsolidovaném základě. V případě institucí by zásady pro outsourcing měly být v souladu s oddílem 8 obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení a zejména by měly zohledňovat požadavky stanovené v oddílu 18 (nové produkty a významné změny) uvedených obecných pokynů. Platební instituce mohou rovněž sladit svoje zásady s oddíly 8 a 18 obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení.

42. Zásady by měly obsahovat hlavní fáze životního cyklu ujednání o outsourcingu a stanovit principy, povinnosti a procesy související s outsourcingem. Tyto zásady by zejména měly zahrnovat přinejmenším:

    a. povinnosti vedoucího orgánu v souladu s odstavcem 36, včetně jeho případného zapojení do rozhodování o externím zajištění kritických nebo důležitých funkcí;

    b. zapojení linií podnikání, funkcí vnitřní kontroly a dalších osob, pokud jde o ujednání o outsourcingu;

    c. plánování ujednání o outsourcingu, včetně:

        i. vymezení obchodních požadavků týkajících se ujednání o outsourcingu;

        ii. kritérií, včetně těch, která jsou uvedena v oddílu 4, a procesů pro určení kritických nebo důležitých funkcí;

        iii. určení, posouzení a řízení rizik podle oddílu 12.2;

        iv. hloubkových kontrol potenciálních poskytovatelů služeb, včetně opatření požadovaných podle oddílu 12.3;

        v. postupů pro určení, posouzení, řízení a zmírnění potenciálního střetu zájmů v souladu s oddílem 8;

        vi. plánování kontinuity činnosti v souladu s oddílem 9;

        vii. procesu schvalování nových ujednání o outsourcingu;

    d. provádění, monitorování a řízení ujednání o outsourcingu, včetně:

[26] Viz rovněž obecné pokyny Evropského orgánu pro bankovnictví k bezpečnostním opatřením v souvislosti s operačními a bezpečnostními riziky platebních služeb podle směrnice PSD2, které jsou dostupné na adrese: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

i. průběžného hodnocení výkonnosti poskytovatele služeb v souladu s oddílem 14;

ii. postupů pro oznamování změn a reagování na změny ujednání o outsourcingu nebo poskytovatele služeb (např. jeho finanční situace, organizační nebo vlastnické struktury, navazujícícho externího zadávání činností nebo služeb);

iii. nezávislého přezkumu a auditu dodržování právních a regulačních požadavků a předpisů;

iv. procesů obnovení;

e. dokumentaci a vedení evidence s přihlédnutím k požadavkům v oddílu 11;

f. ústupové strategie a procesů ukončení, včetně požadavku doloženého ústupového plánu pro každou kritickou nebo důležitou funkci, které má být externě zajištěna, pokud je ústup považován za možný s přihlédnutím k případnému přerušení služeb nebo neočekávanému ukončení smlouvy o externím zajištění služeb nebo činností.

43. Zásady pro outsourcing by měly rozlišovat následující:

a. externí zajištění kritických nebo důležitých funkcí a jiná ujednání o outsourcingu;

b. externí zajištění u poskytovatelů služeb, kteří získali povolení příslušného orgánu, a u poskytovatelů služeb, kteří toto povolení nemají;

c. ujednání o outsourcingu v rámci skupiny, ujednání o outsourcingu v rámci téhož institucionálního systému ochrany (včetně subjektů plně vlastněných individuálně nebo kolektivně institucemi v rámci takového institucionálního systému ochrany) a externí zajištění u subjektů mimo skupinu; a

d. externí zajištění u poskytovatelů služeb nacházejících se v členském státě a ve třetích zemích.

44. Instituce a platební instituce by měly zajistit, aby jejich zásady zahrnovaly identifikaci následujících potenciálních účinků ujednání o outsourcingu kritických nebo důležitých funkcí a aby bylo v rozhodovacím procesu zohledněno následující:

a. rizikový profil instituce;

b. schopnost dohlížet na poskytovatele služeb a řídit rizika;

c. opatření k zajištění kontinuity činnosti; a

d. výkon jejich obchodních činností.

8 Střet zájmů

45. Instituce v souladu s hlavou IV oddílem 11 obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení[27] a platební instituce by měly určit, posoudit a řídit střety zájmů týkající se jejich ujednání o outsourcingu.

46. Pokud outsourcing vyvolává vážný střet zájmů, a to i mezi subjekty ve stejné skupině nebo ve stejném institucionálním systému ochrany, měly by instituce a platební instituce přijmout odpovídající opatření k řízení takového střetu zájmů.

47. Jsou-li funkce poskytovány poskytovatelem služeb, který je součástí skupiny nebo členem institucionálního systému ochrany nebo který je vlastněn institucí, platební institucí, skupinou nebo institucemi, jež jsou členy institucionálního systému ochrany, měly by být podmínky, včetně finančních podmínek, pro externě zajišťovanou službu stanoveny za obvyklých podmínek. Do ceny služeb však lze promítnout synergie vyplývající z poskytování stejných nebo podobných služeb několika institucím v rámci skupiny nebo institucionálního systému ochrany, pokud je poskytovatel služeb i nadále životaschopný jako samostatný subjekt; v rámci skupiny by tomu tak mělo být bez ohledu na selhání jiného subjektu ze skupiny.

9 Plány kontinuity činnosti

48. Instituce v souladu s požadavky podle čl. 85 odst. 2 směrnice 2013/36/EU a hlavy VI obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení[28] a platební instituce by měly zavést, udržovat a pravidelně testovat vhodné plány kontinuity činnosti týkající se externě zajišťovaných kritických nebo důležitých funkcí. Instituce a platební instituce v rámci skupiny nebo institucionálního systému ochrany se mohou opírat o centrálně stanovené plány kontinuity činnosti týkající se jejich externě zajišťovaných funkcí.

49. Plány kontinuity činnosti by měly zohledňovat možnou událost, kdy dojde ke zhoršení kvality poskytování externě zajišťované kritické nebo důležité funkce na nepřijatelnou úroveň nebo kdy takové poskytování selže. Takové plány by měly rovněž přihlížet k potenciálnímu dopadu platební neschopnosti nebo jiného selhání poskytovatelů služeb a případných politických rizik v jurisdikci poskytovatele služeb.

[27] Platební instituce mohou rovněž sladit svoje zásady s uvedenými obecnými pokyny.

[28] K dispozici na adrese: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

10 Funkce interního auditu

50. Činnosti funkce interního auditu[29] by měly v souladu s přístupem založeném na posouzení rizik zahrnovat nezávislý přezkum externě zajišťovaných činností. Plán auditu[30] a program auditu by měly rovněž zahrnovat zejména ujednání o outsourcingu kritických nebo důležitých funkcí.

51. Pokud jde o proces outsourcingu, funkce interního auditu by měla přinejmenším ověřit:

    a. že je rámec instituce nebo platební instituce pro outsourcing, včetně zásad pro outsourcing, správně a účinně prováděn a je v souladu s platnými zákony a právními předpisy, strategií v oblasti rizik a rozhodnutími vedoucího orgánu;

    b. přiměřenost, kvalitu a účinnost posouzení kritické významnosti nebo důležitosti funkcí;

    c. přiměřenost, kvalitu a účinnost hodnocení rizik u ujednání o outsourcingu a to, že jsou rizika i nadále v souladu se strategií instituce v oblasti rizik;

    d. vhodné zapojení orgánů správy a řízení; a

    e. vhodné monitorování a řízení ujednání o outsourcingu.

11 Požadavky týkající se dokumentace

52. Jako součást svého rámce řízení rizik by instituce a platební instituce měly vést a aktualizovat evidenci informací o všech ujednáních o outsourcingu na úrovni instituce a případně na subkonsolidované a konsolidované úrovni, jak je stanoveno v oddílu 2, a měly by řádně zdokumentovat veškerá stávající ujednání o outsourcingu a rozlišovat přitom externí zajištění kritických nebo důležitých funkcí a jiná ujednání o outsourcingu. S přihlédnutím k vnitrostátním právním předpisům by instituce měly vést dokumentaci ukončených ujednání o outsourcingu v rámci evidence a podklady pro příslušné období.

53. S přihlédnutím k hlavě I těchto obecných pokynů a za podmínek stanovených v odst. 23 písm. d) může být pro instituce a platební instituce v rámci skupiny, instituce trvale přidružené k ústřednímu subjektu nebo instituce, které jsou členy stejného institucionálního systému ochrany, evidence vedena centrálně.

---

[29] Ohledně povinností funkce interního auditu se instituce odkazují na oddíl 22 obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-) a platební instituce se odkazují na obecný pokyn č. 5 obecných pokynů Evropského orgánu pro bankovnictví k udělování povolení platebním institucím (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

[30] Viz rovněž obecné pokyny Evropského orgánu pro bankovnictví k procesu dohledu a hodnocení: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing

54. Evidence by měla obsahovat alespoň následující informace pro všechna existující ujednání o outsourcingu:

    a. číslo jednací každého ujednání o outsourcingu;

    b. datum počátku a případně datum příštího obnovení smlouvy, datum ukončení a/nebo výpovědní lhůty pro poskytovatele služeb a pro instituci nebo platební instituci;

    c. stručný popis externě zajištěné funkce, včetně údajů, které jsou externě zajišťovány, a toho, zda jsou osobní údaje (např. uvedením ano nebo ne ve zvláštním datovém poli) předávány nebo zda je jejich zpracování externě zajištěno u poskytovatele služeb;

    d. kategorie přidělená institucí nebo platební institucí, která odráží povahu funkce tak, jak je popsáno v písmenu c) (např. informační technologie (IT), kontrolní funkce), a která by měla usnadnit identifikaci různých druhů ujednání;

    e. jméno poskytovatele služeb, registrační číslo společnosti, identifikátor právnické osoby (je-li k dispozici), sídlo a jiné příslušné kontaktní údaje a jméno jeho případné mateřské společnosti;

    f. země, ve které/kterých bude služba vykonávána, včetně umístění údajů (tj. země nebo regionu);

    g. zda je či není (ano/ne) externě zajišťovaná funkce považovaná za kritickou nebo důležitou, včetně případného stručného shrnutí důvodů, proč je externě zajišťovaná funkce považovaná za kritickou nebo důležitou;

    h. v případě externího zajištění u poskytovatele cloudových služeb model cloudové služby a modely zavedení, tj. veřejné/soukromé/hybridní/komunitní, a konkrétní povaha údajů, které budou uchovávány, a místa (tj. země nebo regiony), kde takové údaje budou uloženy;

    i. datum posledního posouzení kritické významnosti nebo důležitosti externě zajišťované funkce.

55. V případě externího zajištění kritických nebo důležitých funkcí by evidence měla obsahovat alespoň následující doplňující informace:

    a. instituce, platební instituce nebo jiné podniky v oblasti působnosti obezřetnostní konsolidace nebo institucionálního systému ochranu, které využívají outsourcing;

    b. zda poskytovatel služeb nebo dílčí poskytovatel služeb je či není součástí skupiny nebo členem institucionálního systému ochrany nebo je vlastněn institucemi nebo platebními institucemi v rámci skupiny nebo je vlastněn členy institucionálního systému ochrany;

    c. datum posledního hodnocení rizik a stručné shrnutí hlavních výsledků;

d. fyzická osoba nebo rozhodovací orgán (např. vedoucí orgán) v instituci nebo platební instituci, které schválily ujednání o outsourcingu;

e. rozhodné právo smlouvy o externím zajištění služeb nebo činností;

f. datum posledního a příštího plánovaného auditu, je-li to relevantní;

g. případně jména veškerých subdodavatelů, jimž je významná část podstatné nebo důležité funkce dále externě zadána, včetně země, kde jsou subdodavatelé registrováni, kde bude služba poskytována, a případně místo (tj. země nebo region), kde budou údaje uchovány;

h. výsledek posouzení nahraditelnosti poskytovatele služeb (snadno nahraditelný, obtížně nahraditelný nebo nahrazení nemožné), možnosti znovu včlenit kritickou nebo důležitou funkci do instituce nebo platební instituce nebo dopadu ukončení kritické nebo důležité funkce;

i. identifikace alternativních poskytovatelů služeb v souladu s písmenem h);

j. zda externě zajištěná kritická nebo důležitá funkce podporuje obchodní operace, které jsou z časového hlediska kritické;

k. odhadované roční rozpočtové náklady.

56. Instituce a platební instituce by měly na žádost zpřístupnit příslušnému orgánu úplnou evidenci všech existujících ujednání o outsourcingu[31] nebo její stanovené části, jako jsou informace o všech ujednáních o outsourcingu, která spadají do jedné z kategorií uvedených v odst. 54 písm. d) těchto obecných pokynů (např. všechna ujednání o outsourcingu IT). Instituce a platební instituce by měly tyto informace poskytnout ve zpracovatelné elektronické podobě (např. v běžně používaném formátu databáze, souboru CSV).

57. Instituce a platební instituce by měly na žádost zpřístupnit příslušnému orgánu veškeré informace nezbytné k tomu, aby příslušný orgán mohl vykonávat účinný dohled nad dotčenou institucí nebo platební institucí, popřípadě včetně kopie smlouvy o externím zajištění služeb nebo činností.

58. Instituce, aniž je dotčen čl. 19 odst. 6 směrnice (EU) 2015/2366, a platební instituce by měly náležitě a včas informovat příslušné orgány nebo s příslušnými orgány navázat v souvislosti s dohledem dialog o plánovaném externím zajištění kritických nebo důležitých funkcí a/nebo o případech, kdy se externě zajištěná funkce stala kritickou nebo důležitou, a poskytnout alespoň informace uvedené v odstavci 54.

[31] Viz také obecné pokyny Evropského orgánu pro bankovnictví k procesu dohledu a hodnocení, které jsou k dispozici na adrese: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

59. Instituce a platební instituce [32] by měly včas informovat příslušné orgány o podstatných změnách a/nebo závažných událostech týkajících se jejich ujednání o outsourcingu, které by mohly mít významný dopad na nepřetržité zajišťování obchodních činností institucí nebo platebních institucí.

60. Instituce a platební instituce by měly řádně zdokumentovat posouzení provedená podle hlavy IV a výsledky průběžného monitorování (např. výkonnost poskytovatele služeb, dodržování sjednaných úrovní služeb, další smluvní a regulační požadavky, aktualizace hodnocení rizik).

Hlava IV – Proces externího zajištění služeb nebo činností

12 Analýza před provedením outsourcingu

61. Před uzavřením ujednání o outsourcingu by instituce a platební instituce měly:

    a. posoudit, zda se ujednání o outsourcingu týká kritické nebo důležité funkce podle vymezení v hlavě II;

    b. posoudit, zda jsou splněny podmínky dohledu pro outsourcing stanovené v oddílu 12.1;

    c. zjistit a vyhodnotit všechna případná rizika ujednání o outsourcingu v souladu s oddílem 12.2;

    d. provést příslušnou hloubkovou kontrolu potenciálního poskytovatele služeb v souladu s oddílem 12.3;

    e. určit a posoudit střet zájmů, který může outsourcing způsobit, v souladu s oddílem 8.

12.1 Podmínky dohledu v případě outsourcingu

62. Instituce a platební instituce by měly zajistit, aby k externímu zajištění funkcí bankovních činností[33] nebo platebních služeb v případě, že výkon takové funkce vyžaduje povolení nebo registraci příslušným orgánem v členském státě, kde získaly povolení, u poskytovatele služeb nacházejícího se ve stejném nebo jiném členském státě docházelo pouze při splnění jedné z následujících podmínek:

        a. poskytovatel služeb má povolení nebo je registrován u příslušného orgánu k výkonu takových bankovních činností nebo platebních služeb; nebo

---

[32] Viz rovněž obecné pokyny Evropského orgánu pro bankovnictví k oznamování významných incidentů podle směrnice o platebních službách na vnitřním trhu (PSD2), dostupné na adrese: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

[33] Viz článek 9 směrnice o kapitálových požadavcích (CRD) ohledně zákazu výkonu podnikatelské činnosti spočívající v přijímání vkladů nebo jiných splatných prostředků od veřejnosti jinými podniky nebo osobami než úvěrovými institucemi.

b. poskytovatel služeb má jinak povoleno vykonávat tyto bankovní činnosti nebo platební služby v souladu s příslušným vnitrostátním právním rámcem.

63. Instituce a platební instituce by měly zajistit, aby k externímu zajištění funkcí bankovních činností nebo platebních služeb v případě, že výkon takové funkce vyžaduje povolení nebo registraci příslušným orgánem v členském státě, kde získaly povolení, u poskytovatele služeb nacházejícího se v třetí zemi docházelo pouze při splnění následujících podmínek:

a. poskytovatel služeb má povolení nebo je registrován k poskytování takové bankovní činnosti nebo platební služby v třetí zemi a vykonává nad ním dohled relevantní příslušný orgán v takové třetí zemi (označovaný jako „orgán dohledu“);

b. mezi příslušnými orgány odpovědnými za dohled nad institucí a orgány dohledu odpovědnými za dohled nad poskytovatelem služeb existuje příslušná smlouva o spolupráci, např. ve formě memoranda o porozumění nebo dohody kolegií; a

c. dohoda o spolupráci zmíněná v bodě b) by měla zajistit, aby příslušné orgány mohly přinejmenším:

i. na požádání získat informace nezbytné k výkonu svých úkolů v oblasti dohledu podle směrnice 2013/36/EU, nařízení (EU) č. 575/2013, směrnice (EU) 2015/2366 a směrnice 2009/110/ES;

ii. získat odpovídající přístup k údajům, dokumentům, prostorám nebo pracovníkům v třetí zemi relevantním pro výkon jejich pravomocí v oblasti dohledu;

iii. co nejdříve získat od orgánu dohledu v třetí zemi informace pro vyšetřování zjevných porušení požadavků směrnice 2013/36/EU, nařízení (EU) č. 575/2013, směrnice (EU) 2015/2366 a směrnice 2009/110/ES; a

iv. spolupracovat s relevantními orgány dohledu v třetí zemi na výkonu rozhodnutí v případě porušení platných regulačních požadavků a vnitrostátního práva v členském státě. Spolupráce by měla mimo jiné zahrnovat to, že příslušné orgány dostanou od orgánů dohledu v třetí zemi co nejdříve informace o potenciálních porušeních platných regulačních požadavků.

12.2 Hodnocení rizik ujednání o outsourcingu

64. Instituce a platební instituce by měly posoudit potenciální dopad ujednání o outsourcingu na jejich operační riziko, měly by přihlížet k výsledkům posouzení při rozhodování o tom, zda by funkce měla být externě zajištěna u poskytovatele služeb, a měly by před uzavřením ujednání o outsourcingu přijmout vhodná opatření s cílem zabránit dalším zbytečným operačním rizikům.

65. Hodnocení by mělo zahrnovat případné scénáře možných rizikových událostí, včetně událostí operačního rizika vysoké závažnosti. V rámci analýzy scénářů by instituce a platební instituce měly posoudit potenciální dopad selhání nebo nedostatků služeb, včetně rizik způsobených procesy, systémy, lidmi nebo externími událostmi. Instituce a platební instituce by s přihlédnutím k zásadě proporcionality zmíněné v oddíle 1 měly zdokumentovat provedenou analýzu a její výsledky a měly by odhadnout, v jakém rozsahu by ujednání o outsourcingu zvýšilo nebo snížilo jejich operační riziko. S přihlédnutím k hlavě I mohou malé a málo složité instituce a platební instituce používat kvalitativní přístupy k hodnocení rizik, zatímco velké a složité instituce by měly mít sofistikovanější přístup, zahrnující použití interních a externích údajů, jsou-li k dispozici, k poskytnutí vstupních informací při analýze scénářů.

66. V rámci hodnocení rizik by instituce a platební instituce měly rovněž přihlížet k očekávaným přínosům a nákladům navrhovaného ujednání o outsourcingu, včetně zvážení případných rizik, která bude možné omezit nebo řídit, a rizik, která mohou v důsledku navrhovaného ujednání o outsourcingu vyvstat, přičemž zohlední alespoň:

    a. rizika koncentrace, včetně těch, která vyplývají:

        i. z externího zajištění u dominantního poskytovatele služeb, který není snadno nahraditelný; a

        ii. z více ujednání o outsourcingu se stejným poskytovatelem služeb nebo úzce propojenými poskytovateli služeb;

    b. souhrnná rizika vyplývající z externího zajištění několika funkcí v instituci nebo platební instituci nebo v případě skupin institucí nebo institucionálních systémů ochrany souhrnná rizika na konsolidovaném základě nebo na základě institucionálního systému ochrany;

    c. v případě významných institucí riziko nutnosti zakročit, tj. riziko, které může vyplynout z potřeby poskytnout finanční podporu poskytovateli služeb v nouzi nebo převzít jeho obchodní operace; a

    d. opatření prováděná institucí nebo platební institucí a poskytovatelem služeb za účelem řízení a zmírnění rizik.

67. Pokud ujednání o outsourcingu zahrnuje možnost, aby poskytovatel služeb externě zadával kritické nebo důležité funkce dalším poskytovatelům služeb, měly by instituce a platební instituce zohlednit:

    a. rizika související s tímto navazujícím externím zadáváním, včetně dalších rizik, která mohou vzniknout, pokud se subdodavatel nachází v třetí zemi nebo jiné zemi než poskytovatel služeb;

b. riziko, že dlouhé a složité řetězce navazujícího externího zadávání služeb nebo činností sníží schopnost institucí nebo platebních institucí dohlížet na externě zajišťované kritické nebo důležité funkce a schopnost příslušných orgánů nad nimi účinně vykonávat dohled.

68. Při hodnocení rizik před provedením outsourcingu a během průběžného monitorování výkonnosti poskytovatele služeb by instituce a platební instituce měly přinejmenším:

a. identifikovat a klasifikovat příslušné funkce a související údaje a systémy, pokud jde o citlivost a požadovaná bezpečnostní opatření;

b. provést důkladnou, na posouzení rizik založenou analýzu funkcí a souvisejících údajů a systémů, u kterých se zvažuje outsourcing nebo které již jsou externě zajišťované, a řešit potenciální rizika, zejména operační rizika, včetně právního rizika, rizika informačních a komunikačních technologií, rizika nedodržení předpisů a rizika poškození pověsti, a omezení dohledu v souvislosti se zeměmi, kde externě zajišťované služby jsou nebo mohou být poskytovány a kde údaje jsou nebo pravděpodobně budou uloženy;

c. zvážit důsledky toho, kde se poskytovatel služeb nachází (v EU nebo mimo EU);

d. zvážit politickou stabilitu a bezpečnostní situaci dotčené jurisdikce, včetně:

i. platných právních předpisů, včetně právních předpisů o ochraně údajů;

ii. platných ustanovení týkajících se vymáhání práva; a

iii. ustanovení insolvenčního zákona, která by se použila v případě selhání poskytovatele služeb, a zejména případná omezení, která by nastala v souvislosti s naléhavě nutnou obnovou dat instituce nebo platební instituce;

e. vymezit a zvolit vhodnou úroveň ochrany důvěrnosti dat, kontinuitu externě zajišťovaných činností a integritu a sledovatelnost dat a systémů v souvislosti se zamýšleným externím zajištěním služeb nebo činností. Instituce a platební instituce by rovněž měly zvážit případná zvláštní opatření zaměřená na přenášená data, data v paměti a klidová data, jako je použití šifrovacích technologií ve spojení s vhodnou klíčovou strukturou řízení;

f. zvážit, zda je poskytovatel služeb dceřinou nebo mateřskou společností instituce, je zahrnut do oblasti působnosti účetní konsolidace nebo je členem institucionálního systému ochrany nebo vlastněn institucemi, které jsou členy institucionálního systému ochrany, a pokud ano, pak v jakém rozsahu dotyčná instituce ovládá nebo má schopnost ovlivnit jeho jednání podle oddílu 2.

12.3 Hloubková kontrola

69. Před uzavřením ujednání o outsourcingu a s ohledem na operační rizika související s funkcí, která má být externě zajištěna, by instituce a platební instituce měly při výběru a hodnocení zajistit, aby byl poskytovatel služeb vhodný.

70. Pokud jde o kritické nebo důležité funkce, měly by instituce a platební instituce zajistit, aby měl poskytovatel služeb dobrou obchodní pověst, náležité a dostatečné schopnosti, odborné znalosti, kapacitu, zdroje (např. lidské, IT, finanční), organizační strukturu a povolení nebo registrace případně vyžadované právními předpisy k tomu, aby vykonával kritické nebo důležité funkce spolehlivě a odborně a plnil svoje povinnosti během doby platnosti navrhované smlouvy.

71. Dalšími faktory, které by při provádění hloubkové kontroly potenciálního poskytovatele služeb měly být zváženy, jsou mimo jiné:

    a. jeho obchodní model, povaha, rozsah, složitost, finanční situace, vlastnická struktura a struktura skupiny;

    b. dlouhodobé vztahy s poskytovateli služeb, kteří již byli podrobeni hodnocení a poskytují služby dané instituci nebo platební instituci;

    c. zda je poskytovatel služeb mateřskou nebo dceřinou společností instituce nebo platební instituce, je součástí účetní konsolidace instituce nebo je členem stejného institucionálního systému ochrany nebo vlastněn institucemi, které jsou členy stejného institucionálního systému ochrany jako dotčená instituce;

    d. zda nad poskytovatelem služeb vykonávají dohled příslušné orgány.

72. Pokud outsourcing zahrnuje zpracování osobních nebo důvěrných údajů, měly by mít instituce a platební instituce jistotu, že poskytovatel služeb provádí odpovídající technická a organizační opatření na ochranu údajů.

73. Instituce a platební instituce by měly přijmout vhodná opatření k zajištění toho, aby poskytovatelé služeb jednali způsobem, který je v souladu s jejich hodnotami a kodexem chování. Instituce a platební instituce by měly mít zejména u poskytovatelů služeb nacházejících se v třetích zemích a v souvislosti s jejich případnými subdodavateli jistotu, že poskytovatel služeb jedná eticky a společensky odpovědně a dodržuje mezinárodní normy týkající se lidských práv (např. Evropskou úmluvu o lidských právech), ochrany životního prostředí a vhodných pracovních podmínek, včetně zákazu dětské práce.

13 Smluvní fáze

74. Práva a povinnosti instituce, platební instituce a poskytovatele služeb by měly být jasně přiděleny a vymezeny v písemné smlouvě.

75. Smlouva o externím zajištění kritických nebo důležitých funkcí by měla uvádět přinejmenším:

    a. jasný popis externě zajišťované funkce, která má být poskytována;

    b. datum počátku a případné datum ukončení smlouvy a výpovědní lhůty pro poskytovatele služeb a instituci nebo platební instituci;

    c. rozhodné právo smlouvy;

    d. finanční závazky smluvních stran;

    e. zda je povoleno navazující externí zadávání kritické nebo důležité funkce či jejich podstatných částí, a pokud ano, podmínky stanovené v oddílu 13.1, které musí navazující externí zadávání splňovat;

    f. místa (tj. regiony nebo země), kde bude kritická nebo důležitá funkce poskytována a/nebo kde budou uchovávány a zpracovány příslušné údaje, včetně možného místa uložení údajů, a podmínky, které musí být splněny, včetně požadavku informovat instituci nebo platební instituci v případě, že poskytovatel služeb navrhne změnit uvedená místa;

    g. případně ustanovení týkající se přístupnosti, dostupnosti, integrity, ochrany a bezpečnosti příslušných údajů uvedená v oddílu 13.2;

    h. právo instituce nebo platební instituce průběžně monitorovat výkonnost poskytovatele služeb;

    i. dohodnuté úrovně služeb, které by měly zahrnovat přesné kvantitativní a kvalitativní výkonnostní cíle pro externě zajišťovanou funkci, aby umožňovaly včasné monitorování, a tudíž i přijetí vhodných nápravných opatření bez zbytečného prodlení v případě, že dohodnuté úrovně služeb nejsou splněny;

    j. povinnost poskytovatele služeb podávat zprávy instituci nebo platební instituci, včetně informování o případném vývoji, který může mít podstatný dopad na schopnost poskytovatele služeb účinně vykonávat kritickou nebo důležitou funkci podle dohodnutých úrovní služeb a v souladu s příslušnými zákony a regulačními požadavky, a případně povinnost předložit zprávy funkce interního auditu poskytovatele služeb;

    k. zda by měl poskytovatel služeb uzavřít povinné pojištění určitých rizik, a případně požadované úrovně pojistného krytí;

    l. požadavky provádět a testovat pohotovostní plány;

m. ustanovení, která zajišťují, aby byly údaje vlastněné institucí nebo platební institucí přístupné v případě platební neschopnosti, řešení krize nebo ukončení obchodních operací poskytovatele služeb;

n. povinnost poskytovatele služeb spolupracovat s příslušnými orgány a orgány příslušnými k řešení krize instituce nebo platební instituce, včetně jiných jimi určených osob;

o. v případě institucí jasný odkaz na pravomoci vnitrostátního orgánu příslušného k řešení krize, zejména na články 68 a 71 směrnice 2014/59/EU o ozdravných postupech a řešení krize (BRRD), a zejména popis „hmotněprávních povinností“ souvisejících se smlouvou ve smyslu článku 68 uvedené směrnice;

p. neomezené právo institucí, platebních institucí a příslušných orgánů provádět kontrolu a audit poskytovatele služeb, a to zejména v souvislosti s externím zajišťováním kritické nebo důležité funkce podle oddílu 13.3;

q. práva na ukončení uvedená v oddílu 13.4.

13.1 Navazující externí zadávání kritických nebo důležitých funkcí

76. Smlouva o externím zajištění služeb nebo činností by měla stanovit, zda je povoleno navazující externí zadávání kritických nebo důležitých funkcí nebo jejich podstatných částí.

77. Pokud je navazující externí zadávání kritických nebo důležitých funkcí povoleno, instituce a platební instituce by měly určit, zda je část funkce, která by měla být návazně externě zadána, jako taková kritickou nebo důležitou (tj. zda se jedná o podstatnou část kritické nebo důležité funkce), a pokud ano, zanést ji do evidence.

78. Je-li povoleno navazující externí zadávání kritických nebo důležitých funkcí, písemná smlouva by měla:

a. vymezit případné druhy činností, které jsou vyloučeny z navazujícího externího zadávání;

b. určit podmínky, které musí být dodržovány v případě navazujícího externího zadávání;

c. stanovit, že je poskytovatel služeb je povinen dohlížet na služby, které zadal subdodavateli, aby se zajistilo, že jsou soustavně plněny veškeré smluvní povinnosti mezi poskytovatelem služeb a institucí nebo platební institucí;

d. požadovat, aby si poskytovatel služeb před navazujícím externím zadáváním údajů předem vyžádal od instituce nebo platební instituce konkrétní nebo obecný písemný souhlas;[34]

e. zahrnovat povinnost poskytovatele služeb informovat instituci nebo platební instituci o případném plánovaném navazujícím externím zadávání nebo podstatných změnách takového navazujícího externího zadávání, zejména v případě, že to může ovlivnit schopnost poskytovatele služeb plnit povinnosti vyplývající ze smlouvy o externím zajištění služeb nebo činností. To zahrnuje plánované významné změny subdodavatelů a lhůtu pro oznámení; lhůta pro oznámení, která má být stanovena, by měla zejména umožňovat instituci nebo platební instituci využívající outsourcing provést alespoň hodnocení rizik navrhovaných změn a vznést proti změnám námitku před nabytím účinnosti plánovaného navazujícího externího zadání nebo podstatné změny navazujícího externího zadávání;

f. zajistit v případě potřeby, aby instituce nebo platební instituce měla právo vznést námitku proti zamýšlenému navazujícímu externímu zadávání nebo jeho podstatným změnám nebo aby byl vyžadován výslovný souhlas;

g. zajistit, aby instituce nebo platební instituce měla smluvní právo vypovědět smlouvu v případě neoprávněného navazujícího externího zadávání, např. v případě, že navazující externí zadávání výrazně zvyšuje rizika pro instituci nebo platební instituci, nebo v případě, že poskytovatel služeb provede navazující externí zadání, aniž by informoval instituci nebo platební instituci.

79. Instituce a platební instituce by měly s navazujícím externím zadáváním souhlasit pouze v případě, že se subdodavatel zaváže:

    a. dodržovat všechny příslušné zákony, regulační požadavky a smluvní povinnosti; a

    b. udělit instituci, platební instituci a příslušnému orgánu stejná smluvní práva na přístup a audit, jaká jsou udělena poskytovatelem služeb.

80. Instituce a platební instituce by měly zajistit, aby poskytovatel služeb řádně dohlížel na subdodavatele v souladu se zásadami stanovenými institucí nebo platební institucí. Pokud by navrhované navazující externí zadávání mohlo mít významné nepříznivé účinky na ujednání o outsourcingu kritické nebo důležité funkce nebo by mohlo vést k významnému zvýšení rizika, včetně případů, kdy nejsou splněny podmínky v odstavci 79, měly by instituce nebo platební instituce uplatnit své právo vznést námitku proti navazujícímu externímu zadávání, pokud bylo takové právo sjednáno, a/nebo vypovědět smlouvu.

[34] Viz článek 28 nařízení (EU) 2016/679.

13.2 Zabezpečení údajů a systémů

81. Instituce a platební instituce by měly zajistit, aby poskytovatelé služeb v relevantních případech dodržovali příslušné normy pro bezpečnost IT.

82. V relevantních případech (např. v souvislosti s externím zajištěním cloudových služeb nebo jiných informačních a komunikačních technologií) by měly instituce a platební instituce ve smlouvě o outsourcingu vymezit požadavky na bezpečnost údajů a systémů a průběžně monitorovat jejich dodržování.

83. V případě externího zajištění u poskytovatelů cloudových služeb a jiných ujednání o outsourcingu, při kterých dochází k nakládání s osobními nebo důvěrnými údaji nebo k předávání osobních nebo důvěrných údajů, by měly instituce a platební instituce zvolit na posouzení rizik založený přístup k místům (tj. zemi nebo regionu) uložení údajů a zpracování údajů a k faktorům informační bezpečnosti.

84. Aniž by byly dotčeny požadavky nařízení (EU) 2016/679, měly by instituce a platební instituce při externím zajišťování služeb nebo činností (zejména ve třetích zemích) přihlížet k rozdílům ve vnitrostátních právních předpisech týkajících se ochrany údajů. Instituce a platební instituce by měly zajistit, aby smlouva o externím zajištění služeb nebo činností obsahovala povinnost poskytovatele služeb chránit důvěrné, osobní nebo jinak citlivé informace a dodržovat všechny právní požadavky týkající se ochrany údajů, které se na instituci nebo platební instituci vztahují (např. případné dodržování ochrany osobních údajů a bankovního tajemství nebo podobné právní povinnosti zachovat mlčenlivost o údajích klienta).

13.3 Právo na přístup, informace a audit

85. Instituce a platební instituce by měly v rámci písemného ujednání o outsourcingu zajistit, aby funkce interního auditu mohla provést přezkum externě zajišťované funkce s použitím přístupu založeného na posouzení rizik.

86. Bez ohledu na kritickou významnost nebo důležitost externě zajišťované funkce by písemná ujednání o outsourcingu mezi institucemi a poskytovateli služeb měla odkazovat na pravomoci příslušných orgánů a orgánů příslušných k řešení krize ohledně shromažďování informací, a pravomoc vyšetřovat podle čl. 63 odst. 1 písm. a) směrnice 2014/59/EU a čl. 65 odst. 3 směrnice 2013/36/EU, pokud jde o poskytovatele služeb v členském státě, a měla by rovněž zajistit taková práva ve vztahu k poskytovatelům služeb v třetích zemích.

87. Pokud jde o externí zajišťování kritických nebo důležitých funkcí, měly by instituce a platební instituce zajistit, aby jim a jejich příslušným orgánům, včetně orgánů příslušných k řešení krize, a jakékoliv jiné osobě určené jimi nebo příslušnými orgány udělil poskytovatel služeb v rámci písemné smlouvy o externím zajištění služeb nebo činností následující:

    a. plný přístup do všech relevantních firemních prostor (např. sídla a provozních středisek), včetně celé škály příslušných zařízení, systémů, sítí, informací a údajů

používaných při poskytování externě zajišťované funkce, včetně souvisejících finančních informací, personálu a externích auditorů poskytovatele služeb („právo na přístup a informace“); a

b. neomezená práva provádět v souvislosti s ujednáním o outsourcingu kontroly a audity („právo na audit“) umožňující jim monitorovat ujednání o outsourcingu a zajistit dodržování všech příslušných regulačních a smluvních požadavků.

88. V případě externího zajištění funkcí, které nejsou podstatné ani důležité, by měly instituce a platební instituce na základě přístupu založeného na posouzení rizik zajistit právo na přístup a právo na audit, která jsou vymezena v odst. 87 písm. a) a b) a v oddílu 13.3, a to s přihlédnutím k povaze externě zajišťované funkce a k souvisejícím operačním rizikům a rizikům poškození pověsti, k její nastavitelnosti, potenciálnímu dopadu na nepřetržitý výkon jejích činností a smluvnímu období. Instituce a platební instituce by měly přihlédnout k tomu, že se funkce mohou postupem času stát kritickými nebo důležitými.

89. Instituce a platební instituce by měly zajistit, aby smlouva o externím zajištění služeb nebo činností nebo jiná smluvní ujednání nebránila účinnému výkonu práva na přístup a práva na audit touto institucí a platební institucí, příslušnými orgány nebo třetími stranami jimi určenými k výkonu těchto práv.

90. Instituce a platební instituce by měly vykonávat své právo na přístup a právo na audit, na základě přístupu založeného na posouzení rizik stanovit četnost auditu a oblasti, které budou předmětem auditu, a dodržovat relevantní, obecně uznávané vnitrostátní a mezinárodní auditorské standardy.[35]

91. Aniž by byla dotčena jejich konečná odpovědnost v souvislosti s ujednáními o outsourcingu, mohou instituce a platební instituce používat:

a. hromadné kontroly organizované společně s jinými klienty stejného poskytovatele služeb, které jsou vykonávány jimi samotnými, těmito klienty nebo třetí stranou, kterou určí, aby byly auditní zdroje využívány efektivněji a aby se snížilo organizační zatížení klientů i poskytovatele služeb;

b. osvědčení vydaná třetí stranou a zprávy o auditu předložené třetí stranou nebo zprávy o vnitřním auditu zpřístupněné poskytovatelem služeb.

92. V případě externího zajišťování kritických nebo důležitých funkcí by instituce a platební instituce měly posoudit, zda jsou osvědčení vydaná třetí stranou a zprávy zmíněné v odst. 91 písm. b) vhodné a postačují ke splnění jejich regulačních povinností, a neměly by se v průběhu času spoléhat pouze na tyto zprávy.

[35] V případě institucí se odkazuje na oddíl 22 obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení: https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889

93. Instituce a platební instituce by měly použít metodu uvedenou v odst. 91 písm. b) pouze tehdy, když:

    a. jsou spokojeny s plánem auditu pro externě zajišťovanou funkci;

    b. zaručí, že do oblasti působnosti osvědčení nebo zprávy o auditu spadají systémy (tj. procesy, aplikace, infrastruktura, datová centra atd.) a kontroly, které instituce nebo platební instituce označí za klíčové, a dodržování příslušných regulačních požadavků;

    c. budou průběžně důkladně posuzovat obsah osvědčení nebo zpráv o auditu a ověřovat, zda zprávy nebo osvědčení nejsou zastaralé;

    d. zajistí, aby klíčové systémy a kontroly byly zahrnuty v budoucích verzích osvědčení nebo zprávy o auditu;

    e. jsou spokojeny se způsobilostí strany, která provádí osvědčení nebo audit (např. pokud jde o střídání společností provádějících osvědčení nebo audit, kvalifikaci, odborné znalosti, opakované provádění či ověření důkazních informací uvedených v auditorském spisu);

    f. jsou přesvědčeny, že jsou osvědčení vydávána a audity prováděny podle všeobecně uznávaných příslušných profesních standardů a zahrnují test provozní účelnosti zavedených klíčových kontrol;

    g. mají smluvní právo požadovat rozšíření oblasti působnosti osvědčení nebo zpráv o auditu o další příslušné systémy a kontroly, přičemž počet a četnost takových žádostí o úpravu oblasti působnosti by měl být přiměřený a oprávněný z pohledu řízení rizik; a

    h. ponechají si smluvní právo provádět podle svého uvážení individuální audity týkající se externího zajišťování kritických nebo důležitých funkcí.

94. V souladu s obecnými pokyny Evropského orgánu pro bankovnictví k posuzování rizik IKT v rámci procesu dohledu a hodnocení by měly instituce v relevantních případech zajistit, aby mohly provádět testování narušení bezpečnosti s cílem vyhodnotit účinnost zavedených kybernetických a interních IKT bezpečnostních opatření a procesů.[36] S přihlédnutím k hlavě I by měly mít platební instituce rovněž interní mechanismy kontroly IKT, včetně opatření týkajících se kontroly bezpečnosti IKT a opatření ke zmírnění rizik.

95. Instituce, platební instituce, příslušné orgány a auditoři nebo třetí strany jednající jménem instituce, platební instituce nebo příslušných orgánů by měly plánovanou kontrolu na místě oznámit poskytovateli služeb s přiměřeným předstihem, ledaže by včasné předchozí oznámení

[36] Viz rovněž obecné pokyny Evropského orgánu pro bankovnictví k riziku IKT: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

nebylo nemožné z důvodu mimořádné situace nebo krize nebo by to vedlo k situaci, kdy audit přestane být účinný.

96. Při provádění auditů v prostředí s více klienty by se mělo dbát na zajištění, aby se předešlo rizikům, která by ohrožovala prostředí jiného klienta (např. dopad na úrovně služeb, dostupnost údajů, aspekty důvěrnosti informací), nebo aby došlo ke zmírnění takových rizik.

97. Je-li ujednání o outsourcingu po technické stránce výrazně složité, například v případě externího zajišťování cloudových služeb, měla by instituce nebo platební instituce ověřit, že osoby, které provádějí audit, ať již se jedná o její interní auditory, auditory provádějící hromadné kontroly nebo externí auditory jednající jejím jménem, mají odpovídající a příslušné dovednosti a znalosti pro účinné provádění příslušných auditů a/nebo hodnocení. Totéž platí pro pracovníky instituce nebo platební instituce, kteří provádějí kontrolu osvědčení vydaných třetí stranou nebo auditů prováděných poskytovateli služeb.

13.4 Práva na ukončení

98. Ujednání o outsourcingu by mělo instituci nebo platební instituci výslovně poskytovat možnost ujednání ukončit v souladu s platnými právními předpisy, a to i v následujících situacích:

    a. jestliže poskytovatel externě zajišťovaných funkcí porušuje platné zákony, právní předpisy nebo smluvní ustanovení;

    b. jestliže jsou zjištěny překážky, které mohou změnit výkon externě zajišťované funkce;

    c. jestliže existují podstatné změny ovlivňující ujednání o outsourcingu nebo poskytovatele služeb (např. navazující externí zadávání služeb nebo činností nebo změny subdodavatelů);

    d. jestliže se vyskytnou nedostatky týkající se řízení a zabezpečení důvěrných, osobních nebo jinak citlivých údajů nebo informací; a

    e. když příslušný orgán instituce nebo platební instituce vydá pokyn, např. v případě, že příslušný orgán v důsledku ujednání o outsourcingu ztratí postavení umožňující mu vykonávat účinný dohled nad institucí nebo platební institucí.

99. Ujednání o outsourcingu by mělo usnadnit převod externě zajišťované funkce na jiného poskytovatele služeb nebo její opětovné včlenění do instituce nebo platební instituce. Za tímto účelem by mělo písemné ujednání o outsourcingu:

    a. jasně vymezovat povinnosti stávajícího poskytovatele služeb v případě převodu externě zajišťované funkce na jiného poskytovatele služeb nebo zpět na instituci nebo platební instituci, včetně nakládání s údaji;

b. stanovit odpovídající přechodné období, během kterého by poskytovatel služeb po ukončení ujednání o outsourcingu pokračoval v poskytování externě zajišťované funkce, aby se snížilo riziko narušení; a

c. obsahovat povinnost poskytovatele služeb poskytnout instituci nebo platební instituci pomoc při řádném převodu funkce v případě ukončení smlouvy o externím zajištění služeb nebo činností.

14 Dohled nad externě zajišťovanými funkcemi

100. Instituce a platební instituce by měly průběžně monitorovat výkonnost poskytovatelů služeb ve vztahu ke všem ujednáním o outsourcingu, a to na základě přístupu založeného na posouzení rizik a se zaměřením zejména na externí zajištění kritických nebo důležitých funkcí, včetně zajištění dostupnosti, integrity a zabezpečení údajů a informací. Dojde-li k podstatné změně rizika, povahy nebo rozsahu externě zajišťované funkce, měly by instituce a platební instituce znovu posoudit kritickou významnost nebo důležitost takové funkce v souladu s oddílem 4.

101. Instituce a platební instituce by měly při monitorování a řízení ujednání o outsourcingu využívat patřičné dovednosti, vynakládat řádnou péči a postupovat s náležitou svědomitostí.

102. Instituce by měly pravidelně aktualizovat svoje hodnocení rizik podle oddílu 12.2 a měly by vedoucímu orgánu pravidelně podávat zprávy o rizicích zjištěných v souvislosti s externím zajišťováním kritických nebo důležitých funkcí.

103. Instituce a platební instituce by měly s přihlédnutím k oddílu 12.2 těchto obecných pokynů monitorovat a řídit svoje interní rizika koncentrace, která jsou způsobena ujednáními o outsourcingu.

104. Instituce a platební instituce by měly průběžně zajišťovat, aby ujednání o outsourcingu se zaměřením zejména na externě zajišťované kritické nebo důležité funkce splňovala příslušné výkonnostní normy a normy kvality v souladu s jejich zásadami tím, že:

a. zajistí, aby dostávaly od poskytovatelů služeb příslušné zprávy;

b. vyhodnotí výkonnost poskytovatelů služeb s použitím nástrojů, jako jsou klíčové ukazatele výkonnosti (KPI), klíčové ukazatele kontroly, zprávy o dodání služby, čestná prohlášení a nezávislé kontroly; a

c. přezkoumají všechny další příslušné informace získané od poskytovatele služeb, včetně zpráv o opatřeních k zajištění kontinuity činnosti a testování.

105. Instituce by měly přijmout vhodná opatření, pokud zjistí nedostatky v poskytování externě zajišťované funkce. Instituce a platební instituce by se zejména měly zabývat jakýmikoli náznaky, že by poskytovatelé služeb mohli vykonávat externě zajišťované kritické nebo důležité

funkce neefektivně nebo že by případně nedodržovali platné zákony a regulační požadavky. Jsou-li zjištěny nedostatky, instituce a platební instituce by měly přijmout vhodná nápravná opatření. Taková opatření mohou v případě potřeby zahrnovat ukončení smlouvy o externím zajištění služeb nebo činností s okamžitou účinností.

15 Ústupové strategie

106. Instituce a platební instituce by měly mít při externím zajišťování kritických nebo důležitých funkcí zdokumentovanou ústupovou strategii (tzv. exit strategii), která je v souladu s jejich zásadami pro outsourcing a plány kontinuity činnosti [37], s přihlédnutím přinejmenším k možnosti:

a. ukončení ujednání o outsourcing;

b. selhání poskytovatele služeb;

c. zhoršení kvality poskytované funkce a skutečná nebo potenciální narušení obchodní činnosti způsobená nevhodným poskytováním funkce nebo neposkytnutím funkce;

d. podstatných rizik vyplývajících pro vhodné a nepřetržité uplatňování funkce.

107. Instituce a platební instituce by měly zajistit, aby byly schopny od ujednání o outsourcingu odstoupit bez nepřípustného narušení svých obchodních činností, aniž by došlo ke snížení úrovně dodržování regulačních požadavků z jejich strany a aniž by to bylo na úkor kontinuity a kvality poskytování služeb klientům. Za tímto účelem by měly:

a. vypracovat a provádět ústupové plány, které jsou komplexní, zdokumentované a v případě potřeby dostatečně prověřené (např. provedením analýzy potenciálních nákladů, dopadů, zdrojů a časových důsledků převodu externě zajišťované služby na alternativního poskytovatele); a

b. stanovit alternativní řešení a vypracovat plány přechodu, které umožní instituci nebo platební instituci převzít externě zajišťované funkce a údaje od poskytovatele služeb a převést je na alternativní poskytovatele nebo zpět na dotyčnou instituci nebo platební instituci nebo přijmout jiná opatření, která zajistí nepřetržité poskytování kritické nebo důležité funkce nebo obchodní činnosti řízeným a dostatečně prověřeným způsobem, a to s přihlédnutím k problémům, které mohou vzniknout kvůli umístění údajů, a provést nezbytná opatření pro zajištění kontinuity činnosti během fáze přechodu.

[37] Instituce v souladu s požadavky podle čl. 85 odst. 2 směrnice 2013/36/EU a hlavy VI obecných pokynů Evropského orgánu pro bankovnictví k vnitřnímu systému správy a řízení a platební instituce by měly mít vhodné plány kontinuity činnosti týkající se externě zajišťovaných kritických nebo důležitých funkcí.

108. Při vytváření ústupových strategií by instituce a platební instituce měly:

a. stanovit cíle ústupové strategie;

b. provést analýzu dopadů, která je úměrná riziku externě zajišťovaných procesů, služeb nebo činností, aby se zjistilo, jaké lidské a finanční zdroje by byly zapotřebí k provedení ústupového plánu a jak dlouho by to trvalo;

c. rozvrhnout úlohy, povinnosti a dostatečné zdroje za účelem řízení ústupových plánů a přechodových činností;

d. definovat kritéria úspěšnosti předání externě zajišťovaných funkcí a údajů; a

e. definovat ukazatele, které budou používány k monitorování ujednání o outsourcingu (uvedené v oddílu 14), včetně ukazatelů vycházejících z nepřijatelných úrovní služeb, jež slouží jako spouštěcí mechanismus pro zahájení ústupové strategie.

Hlava V – Obecné pokyny k externímu zajištění služeb nebo činností (outsourcingu) určené příslušným orgánům

109. Při stanovování vhodných metod pro sledování toho, zda instituce a platební instituce dodržují podmínky původního povolení, by příslušné orgány měly usilovat o zjištění, zda ujednání o outsourcingu představují podstatnou změnu podmínek a povinností původního povolení uděleného institucím a platebním institucím.

110. Příslušné orgány by měly mít jistotu, že mohou účinně vykonávat dohled nad institucemi a platebními institucemi, včetně toho, že by instituce nebo platební instituce v rámci svého ujednání o outsourcingu zajistily, aby měli poskytovatelé služeb povinnost příslušnému orgánu a instituci udělit právo na audit a právo na přístup v souladu s oddílem 13.3.

111. Analýza rizik outsourcingu by měla být prováděna alespoň v rámci procesu dohledu a hodnocení (SREP) nebo u platebních institucí v rámci jiných procesů dohledu, včetně žádostí ad hoc, nebo během kontrol na místě.

112. V návaznosti na informace uvedené v evidenci, jak je zmíněno v oddílu 11, mohou příslušné orgány, zejména u kritických nebo důležitých ujednání o outsourcingu, požádat instituce a platební instituce o další informace, jako je např.:

a. podrobná analýza rizik;

b. zda má poskytovatel služeb plán kontinuity činnosti, který je vhodný pro služby poskytované instituci nebo platební instituci využívající outsourcing;

c. ústupová strategie, která se použije v případě, že některá ze stran ukončí ujednání o outsourcingu, nebo v případě narušení poskytování služeb; a

d. zdroje a opatření pro vhodné monitorování externě zajišťovaných činností.

113. Kromě informací požadovaných v oddílu 11 mohou příslušné orgány požadovat, aby instituce a platební instituce poskytly podrobné informace o jakémkoliv ujednání o outsourcingu, a to dokonce i tehdy, když se dotčená funkce nepovažuje za kritickou nebo důležitou.

114. Příslušné orgány by měly s použitím přístupu založeného na posouzení rizik posoudit následující:

a. zda instituce a platební instituce vhodně monitorují a řídí zejména kritická nebo důležitá ujednání o outsourcingu;

b. zda instituce a platební instituce poskytují dostatečné zdroje pro účely monitorování a řízení ujednání o outsourcingu;

c. zda instituce a platební instituce určují a řídí všechna příslušná rizika; a

d. zda instituce a platební instituce určují, posuzují a řádně řídí střety zájmů týkající se ujednání o outsourcingu, např. v případě outsourcingu v rámci skupiny nebo outsourcingu v rámci téhož institucionálního systému ochrany.

115. Příslušné orgány by měly zajistit, aby instituce a platební instituce z EU/EHP nefungovaly jako „prázdná skořápka“, což zahrnuje i situace, kdy instituce používají transakce typu back-to-back nebo transakce v rámci skupiny k převedení části tržního rizika a úvěrového rizika na subjekt mimo EU/EHP, a měly by zajistit, aby byly zavedeny vhodné systémy správy a řízení a systémy řízení rizik pro účely identifikace a řízení svých rizik.

116. Při posuzování by příslušné orgány měly zohlednit veškerá rizika, zejména pak:[38]

a. operační rizika[39], která představuje ujednání o outsourcingu;

b. rizika poškození pověsti;

c. v případě významných institucí riziko nutnosti zakročit, pokud by instituce byla případně nucena finančně vypomoct poskytovateli služeb;

d. rizika koncentrace v rámci instituce, a to i na konsolidovaném základě, která vyplývají z více ujednání o outsourcingu s jediným poskytovatelem služeb nebo úzce

[38] V případě institucí, na které se vztahuje směrnice 2013/36/EU, viz rovněž obecné pokyny Evropského orgánu pro bankovnictví k procesu dohledu a hodnocení (SREP): https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Viz rovněž obecné pokyny Evropského orgánu pro bankovnictví k riziku IKT: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

propojenými poskytovateli služeb nebo z více ujednání o outsourcingu ve stejné oblasti podnikání;

e. rizika koncentrace na úrovni odvětví, např. když více institucí nebo platebních institucí využívá jediného poskytovatele služeb nebo malou skupinu poskytovatelů služeb;

f. v jakém rozsahu instituce nebo platební instituce, která využívají outsourcing, ovládá poskytovatele služeb nebo má schopnost ovlivnit jeho jednání, omezení rizik, které může být důsledkem vyšší úrovně kontroly, a zda je poskytovatel služeb zahrnut do konsolidovaného dohledu nad skupinou; a

g. střet zájmů mezi institucí a poskytovatelem služeb.

117. Jsou-li zjištěna rizika koncentrace, příslušné orgány by měly sledovat vývoj takových rizik a vyhodnotit jejich potenciální dopad na jiné instituce a platební instituce i na stabilitu finančního trhu; příslušné orgány by měly podle potřeby informovat orgán příslušný k řešení krize o nových potenciálně kritických funkcích[40], které byly během tohoto posouzení zjištěny.

118. Jsou-li zjištěny problémy, které vedou k závěru, že instituce nebo platební instituce přestala mít stabilní systém správy a řízení nebo že nedodržuje regulační požadavky, měly být příslušné orgány přijmout vhodná opatření, která mohou zahrnovat omezení rozsahu nebo zákaz externě zajišťovaných funkcí nebo požadavek ukončit jedno nebo více ujednání o outsourcingu. S přihlédnutím k potřebě instituce nebo platební instituce vykonávat nepřetržitě svou činnost by mohlo být ukončení smluv vyžadováno zejména v případě, že není možné dohled a prosazování regulačních požadavků zajistit jinými způsoby.

119. Příslušné orgány by měly mít jistotu, že jsou schopny vykonávat účinný dohled, a to zejména tehdy, když instituce a platební instituce externě zajišťují kritické nebo důležité funkce, které jsou prováděny mimo EU/EHP.

[40] Jak je vymezeno v čl. 2 odst. 1 bodu 35 směrnice o ozdravných postupech a řešení krize (BRRD).