EBA/GL/2019/02

25. veljače 2019.

Smjernice za eksternalizaciju

1. Obveze usklađivanja i izvješćivanja

Status ovih smjernica

1. Ovaj dokument sadržava smjernice izdane na temelju članka 16. Uredbe (EU) br. 1093/2010[1]. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela i financijske institucije moraju ulagati napore da se usklade s tim smjernicama.

2. U smjernicama se iznosi EBA-ino stajalište o odgovarajućim nadzornim praksama unutar Europskog sustava financijskog nadzora ili o tome kako bi se pravo Unije trebalo primjenjivati u određenom području. Nadležna tijela određena člankom 4. stavkom 2. Uredbe (EU) br. 1093/2010 na koja se smjernice primjenjuju trebaju se s njima uskladiti tako da ih na odgovarajući način uključe u svoje prakse (npr. izmjenama svojeg pravnog okvira ili nadzornih postupaka), uključujući u slučajevima kada su smjernice prvenstveno upućene institucijama i institucijama za platni promet.

Zahtjevi u pogledu izvješćivanja

3. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela moraju obavijestiti EBA-u o tome da su usklađena ili da se namjeravaju uskladiti s ovim smjernicama ili, u suprotnom, navesti razloge za neusklađenost do ([dd.mm.gggg.]). U slučaju izostanka obavijesti unutar tog roka, EBA će smatrati da nadležna tijela nisu usklađena. Obavijesti se dostavljaju slanjem popunjenog obrasca dostupnog na internetskim stranicama EBA-e na adresu compliance@eba.europa.eu s naznakom „EBA/GL/2019/02”. Obavijesti trebaju dostaviti osobe s odgovarajućim ovlastima za izvješćivanje o usklađenosti u ime svojih nadležnih tijela. Bilo koja promjena statusa usklađenosti mora se isto tako prijaviti EBA-i.

4. Obavijesti će se objaviti na internetskim stranicama EBA-e, u skladu s člankom 16. stavkom 3.

[1] Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ, (SL L 331, 15. 12. 2010., str. 12.).

2. Predmet, područje primjene i definicije

Predmet

5. U ovim se smjernicama navode mehanizmi internog upravljanja, uključujući dobro upravljanje rizicima, koje institucije, institucije za platni promet i institucije za elektronički novac trebaju primjenjivati pri eksternalizaciji funkcija, posebno kad je riječ o eksternalizaciji ključnih ili važnih funkcija.

6. U smjernicama se navodi kako nadležna tijela trebaju provjeravati i pratiti mehanizme iz prethodnog stavka, u kontekstu članka 97. Direktive 2013/36/EU [2] o postupku nadzorne provjere i ocjene (SREP), članka 9. stavka 3. Direktive (EU) 2015/2366 [3], članka 5. stavka 5. Direktive 2009/110/EZ[4], ispunjavanjem svoje dužnosti praćenja stalne usklađenosti subjekata na koje se ove smjernice odnose s uvjetima njihova odobrenja za rad.

Adresati

7. Ove smjernice upućene su nadležnim tijelima utvrđenima člankom 4. stavkom 1. točkom 40. Uredbe (EU) br. 575/2013[5], uključujući Europsku središnju banku u pogledu pitanja povezanih sa zadaćama koje su joj dodijeljene Uredbom (EU) br. 1024/2013[6], institucijama utvrđenima člankom 4. stavkom 1. točkom 3. Uredbe (EU) br. 575/2013, institucijama za platni promet utvrđenima člankom 4. stavkom 4. Direktive (EU) 2015/2366 te institucijama za elektronički novac u smislu članka 2. stavka 1. Direktive 2009/110/EZ. Pružatelji usluga informiranja o računu koji isključivo pružaju uslugu iz točke 8. Priloga I. Direktivi (EU) 2015/2366 nisu uključeni u područje primjene ovih smjernica, u skladu s člankom 33. te Direktive.

---

[2] Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ.

[3] Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ.

[4] Direktiva 2009/110/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o osnivanju, obavljanju djelatnosti i bonitetnom nadzoru poslovanja institucija za elektronički novac te o izmjeni direktiva 2005/60/EZ i 2006/48/EZ i stavljanju izvan snage Direktive 2000/46/EZ.

[5] Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.).

[6] Uredba Vijeća (EU) br. 1024/2013 od 15. listopada 2013. o dodjeli određenih zadaća Europskoj središnjoj banci u vezi s politikama bonitetnog nadzora kreditnih institucija.

8. Za potrebe ovih smjernica, sva upućivanja na „institucije za platni promet" uključuju i „institucije za elektronički novac", a sva upućivanja na „platne usluge" uključuju i „izdavanje elektroničkog novca".

Područje primjene

9. Ne dovodeći u pitanje Direktivu 2014/65/EU[7] i Delegiranu uredbu Komisije (EU) 2017/565[8] (koja sadržava zahtjeve u pogledu eksternalizacije koju provode institucije koje pružaju investicijske usluge i provode investicijske aktivnosti, kao i relevantne smjernice koje je izdalo Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala u pogledu investicijskih usluga i aktivnosti), institucije utvrđene člankom 3. stavkom 1. točkom 3. Direktive 2013/36/EU trebaju se uskladiti s ovim smjernicama na pojedinačnoj, potkonsolidiranoj i konsolidiranoj osnovi. Nadležna tijela mogu dopustiti izuzeće od primjene na pojedinačnoj osnovi na temelju članka 21. Direktive 2013/36/EU ili članka 109. stavka 1. Direktive 2013/36/EU u vezi s člankom 7. Uredbe (EU) br. 575/2013. Institucije koje podliježu odredbama Direktive 2013/36/EU trebaju se uskladiti s tom Direktivom i ovim smjernicama na potkonsolidiranoj i konsolidiranoj osnovi kako je utvrđeno u članku 21. i člancima od 108. do 110. Direktive 2013/36/EU.

10. Ne dovodeći u pitanje članak 8. stavak 3. Direktive (EU) 2015/2366 i članak 5. stavak 7. Direktive 2009/110/EZ, institucije za platni promet i institucije za elektronički novac trebaju biti usklađene s ovim smjernicama na pojedinačnoj osnovi.

11. Nadležna tijela odgovorna za nadzor institucija, institucija za platni promet i institucija za elektronički novac trebaju postupati u skladu s ovim smjernicama.

Definicije

12. Ako nije drukčije naznačeno, pojmovi upotrijebljeni i utvrđeni u Direktivi 2013/36/EU, Uredbi (EU) br. 575/2013, Direktivi 2009/110/EZ, Direktivi (EU) 2015/2366 i Smjernicama EBA-e o internom upravljanju[9] imaju isto značenje u ovim smjernicama. Osim toga, za potrebe ovih smjernica primjenjuju se sljedeće definicije:

Eksternalizacija	znači ugovor bilo koje vrste sklopljen između neke institucije, institucije za platni promet ili institucije za elektronički novac i pružatelja usluge, na temelju kojeg taj pružatelj usluge obavlja određeni postupak, uslugu ili aktivnost koje bi u suprotnome obavljala sama institucija,

[7] Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (SL L 173, 12. 6. 2014., str. 349.).

[8] Delegirana uredba Komisije (EU) 2017/565 od 25. travnja 2016. o dopuni Direktive 2014/65/EU Europskog parlamenta i Vijeća u vezi s organizacijskim zahtjevima i uvjetima poslovanja investicijskih društava te izrazima definiranima za potrebe te Direktive (SL L 87, 31. 3. 2017., str. 1.).

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

	institucija za platni promet ili institucija za elektronički novac.
Funkcija	znači bilo koji postupak, bilo koja usluga ili aktivnost.
Ključna ili važna funkcija[10]	znači svaka funkcija koja se smatra ključnom ili važnom u skladu s odjeljkom 4. ovih smjernica.
Podeksternalizacija	znači situacija u kojoj pružatelj usluge u okviru određenog ugovora o eksternalizaciji eksternaliziranu funkciju povjerava nekom drugom pružatelju usluga.[11]
Pružatelj usluga	znači treća strana koja obavlja određeni eksternalizirani postupak, uslugu ili aktivnost, ili dijelove postupka, usluge ili aktivnosti, u okviru ugovora o eksternalizaciji.
Usluge računarstva u oblaku	znači usluge koje se pružaju putem računarstva u oblaku, odnosno model kojim se na zahtjev omogućuje široko rasprostranjen, pogodan mrežni pristup zajedničkom skupu podesivih računalnih resursa (npr. mreže, poslužitelji, uređaji za pohranu podataka, aplikacije i usluge), koji se mogu trenutačno pribaviti i otpustiti uz minimalnu upravljačku aktivnost ili prisutnost pružatelja usluge.
Javni oblak	znači infrastruktura za usluge računarstva u oblaku kojoj može pristupiti šira javnost.
Privatni oblak	znači infrastruktura za usluge računarstva u oblaku kojoj može pristupiti samo jedna institucija ili institucija za platni promet.
Zajednički oblak	znači infrastruktura za usluge računarstva u oblaku dostupna samo određenoj skupini institucija ili institucija za platni promet, uključujući nekoliko institucija iz jedne grupe.
Hibridni oblak	znači infrastruktura za usluge u oblaku sastavljena od dviju ili više različitih infrastruktura za usluge u oblaku.
Upravljačko tijelo	znači tijelo ili tijela institucije ili institucije za platni promet koja se imenuju u skladu s nacionalnim pravom, a ovlaštena su za utvrđivanje strategije, ciljeva i općeg smjera institucije ili institucije za platni promet te nadgledaju i prate donošenje odluka uprave i uključuju osobe koje stvarno vode poslovanje institucije ili institucije za platni promet te

[10] Formulacija „ključna ili važna funkcija” temelji se na formulaciji iz Direktive 2014/65/EU (MiFID II) i Delegirane uredbe Komisije (EU) 2017/565 o dopuni Direktive MiFID II i upotrebljava se samo za potrebe eksternalizacije; nije povezana s definicijom „ključnih funkcija” za potrebe okvira oporavka i sanacije koje su definirane u članku 2. stavku 1. točki (35) Direktive 2014/59/EU.

[11] Za procjenu se primjenjuju odredbe iz odjeljka 3.; podeksternalizacija se u drugim dokumentima EBA-e naziva i „lanac eksternalizacije” ili „lančana eksternalizacija”.

	direktore i osobe odgovorne za upravljanje institucijom za platni promet.

3. Provedba

Datum primjene

13. Uz iznimku stavka 63. točke (b), ove se smjernice primjenjuju od 30. rujna 2019. na sve ugovore o eksternalizaciji sklopljene, revidirane ili izmijenjene na taj datum ili nakon njega. Stavak 63. točka (b) primjenjuje se od 31. prosinca 2021.

14. Institucije i institucije za platni promet trebaju na odgovarajući način revidirati i izmijeniti postojeće ugovore o eksternalizaciji kako bi osigurale njihovu usklađenost s ovim smjernicama.

15. Ako se revizija ugovora o eksternalizaciji ključnih ili važnih funkcija ne dovrši do 31. prosinca 2021., institucije i institucije za platni promet trebaju obavijestiti svoje nadležno tijelo o tome i o mjerama planiranima za dovršetak revizije ili mogućoj izlaznoj strategiji.

Prijelazne odredbe

16. Institucije i institucije za platni promet trebaju dopuniti dokumentaciju o svim postojećim ugovorima o eksternalizaciji, osim o ugovorima o eksternalizaciji s pružateljima usluga računarstva u oblaku, u skladu s ovim smjernicama nakon datuma prvog produljenja svakog postojećeg ugovora o eksternalizaciji, a najkasnije do 31. prosinca 2021.

Stavljanje izvan snage

17. Smjernice Odbora europskih nadzornih tijela za bankarstvo (CEBS) o eksternalizaciji od 14. prosinca 2006. i Preporuke EBA-e za eksternalizaciju pružateljima usluga računarstva u oblaku[12] stavljaju se izvan snage od 30. rujna 2019.

[12] Preporuke za eksternalizaciju pružateljima usluga računarstva u oblaku (EBA/REC/2017/03).

4. Smjernice za eksternalizaciju

Glava I. – Proporcionalnost: primjena unutar grupe i institucionalni sustavi zaštite

1 Proporcionalnost

18. Institucije, institucije za platni promet i nadležna tijela trebaju pri usklađivanju ili nadzoru usklađenosti s ovim Smjernicama uzeti u obzir načelo proporcionalnosti. Cilj je načela proporcionalnosti osigurati usklađenost sustava upravljanja, uključujući one povezane s eksternalizacijom, s pojedinačnim profilom rizičnosti, vrstom i poslovnim modelom institucije ili institucije za platni promet te veličinom i složenošću njezine djelatnosti kako bi se osiguralo učinkovito ispunjenje regulatornih zahtjeva.

19. Prilikom primjene zahtjeva iz ovih Smjernica, institucije i institucije za platni promet trebaju uzeti u obzir složenost eksternaliziranih funkcija, rizike koji proizlaze iz ugovora o eksternalizaciji, ključnost ili važnost eksternalizirane funkcije i mogući učinak eksternalizacije na kontinuitet njihovih djelatnosti.

20. Prilikom primjene načela proporcionalnosti, institucije, institucije za platni promet[13] i nadležna tijela trebaju uzeti u obzir kriterije iz Glave I. Smjernica EBA-e o internom upravljanju, u skladu s člankom 74. stavkom 2. Direktive 2013/36/EU.

2 Eksternalizacija koju provode grupe i institucije koje su članice institucionalnog sustava zaštite

21. U skladu s člankom 109. stavkom 2. Direktive 2013/36/EU, ove se Smjernice primjenjuju i na potkonsolidiranoj i konsolidiranoj osnovi, uzimajući u obzir bonitetni opseg konsolidacije[14]. U tu svrhu matična društva iz EU-a ili matično društvo u državi članci trebaju osigurati da su sustavi, postupci i mehanizmi internog upravljanja u njihovim društvima kćerima, uključujući institucije za platni promet, dosljedni, pravilno integrirani i prikladni za učinkovitu primjenu ovih Smjernica na svim relevantnim razinama.

---

[13] Institucije za platni promet trebaju proučiti i Smjernice EBA-e na temelju PSD2 o informacijama koje treba dostaviti u svrhu izdavanja odobrenja institucijama za platni promet i institucijama za elektronički novac i za registraciju pružatelja usluga informiranja o računu, koje su dostupne na internetskim stranicama EBA-e na sljedećoj poveznici: 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] Vidjeti članak 4. stavak 1. točke (47) i (48) Uredbe (EU) br. 575/2013 u pogledu opsega konsolidacije.

22. Institucije i institucije za platni promet, u skladu sa stavkom 21., kao i institucije koje, kao članice institucionalnog sustava zaštite, upotrebljavaju centralizirane sustave upravljanja trebaju poštovati sljedeće:

    a. ako te institucije ili institucije za platni promet imaju ugovore o eksternalizaciji s pružateljima usluga unutar grupe ili institucionalnog sustava zaštite[15], upravljačko tijelo tih institucija ili institucija za platni promet i za te ugovore o eksternalizaciji zadržava punu odgovornost za usklađivanje sa svim regulatornim zahtjevima i za učinkovitu primjenu ovih Smjernica;

    b. ako te institucije ili institucije za platni promet eksternaliziraju operativne zadatke kontrolnih funkcija pružatelju usluga unutar grupe ili institucionalnog sustava zaštite, za potrebe praćenja i revizije ugovora o eksternalizaciji institucije trebaju osigurati (i za te ugovore o eksternalizaciji) uspješnu provedbu tih operativnih zadataka, uključujući putem primanja odgovarajućih izvješća.

23. Osim navedenog u stavku 22., institucije i institucije za platni promet unutar grupe kojima nisu odobrena izuzeća na temelju članka 109. Direktive 2013/36/EU i članka 7. Uredbe (EU) br. 575/2013, institucije koje su središnje tijelo ili su stalno povezane sa središnjim tijelom, a kojima nisu odobrena izuzeća na temelju članka 21. Direktive 2013/36/EU, ili institucije koje su članice institucionalnog sustava zaštite trebaju uzeti u obzir i sljedeće:

    a. ako je operativno praćenje eksternalizacije centralizirano (npr. u okviru standardiziranog sporazuma o praćenju ugovora o eksternalizaciji), institucije i institucije za platni promet trebaju osigurati, najmanje za eksternalizirane ključne ili važne funkcije, da svaka institucija ili institucija za platni promet može provoditi neovisno praćenje pružatelja usluga i odgovarajući nadzor, uključujući primanje izvješća od centralizirane funkcije za praćenje, koja se podnose barem jednom godišnje i na zahtjev, a koja najmanje sadržavaju sažetak procjene rizika i praćenja provedbe. Osim toga, institucije i institucije za platni promet trebaju od centralizirane funkcije za praćenje dobivati sažetak relevantnih revizijskih izvješća u pogledu eksternalizacije ključnih ili važnih funkcija te, na zahtjev, potpuno revizijsko izvješće;

    b. institucije i institucije za platni promet trebaju osigurati da njihovo upravljačko tijelo bude pravodobno obaviješteno o relevantnim planiranim promjenama u pogledu pružatelja usluga koji se centralizirano prate te o mogućem učinku tih promjena na ključne ili važne funkcije koje se pružaju, uključujući sažetak analize rizika, među ostalim pravnih rizika, usklađenost s regulatornim zahtjevima i učinak na razine usluga, kako bi se mogao procijeniti učinak tih promjena;

    c. ako se te institucije i institucije za platni promet unutar grupe, institucije povezane sa središnjim tijelom ili institucije koje su dio institucionalnog sustava zaštite oslanjaju na

[15] U skladu s člankom 113. stavkom 7. Uredbe o kapitalnim zahtjevima, institucionalni sustav zaštite ugovorno je ili zakonski određeno uređenje odgovornosti koje štiti institucije članice tog sustava, a posebno osigurava njihovu likvidnost i solventnost kako bi se izbjegao stečaj u slučaju da to postane neophodno.

centraliziranu procjenu eksternalizacije koja se provodi prije sklapanja ugovora o eksternalizaciji, kako je navedeno u odjeljku 12., svaka institucija i institucija za platni promet trebaju primiti sažetak procjene i osigurati da se u postupku donošenja odluke uzmu u obzir njezina specifična struktura i rizici;

d. ako je uspostavljen registar svih postojećih ugovora o eksternalizaciji, kako je navedeno u odjeljku 11., te ako se on vodi centralizirano unutar grupe ili institucionalnog sustava zaštite, nadležna tijela, sve institucije i institucije za platni promet trebaju moći dobiti svoj registar bez nepotrebnog odgađanja. Taj registar treba sadržavati sve ugovore o eksternalizaciji, uključujući i one sklopljene s pružateljima usluga unutar te grupe ili institucionalnog sustava zaštite;

e. ako se te institucije i institucije za platni promet oslanjaju na izlazni plan za ključne ili važne funkcije koji je uspostavljen na razini grupe, unutar institucionalnog sustava zaštite ili koji je uspostavilo središnje tijelo, sve institucije i institucije za platni promet trebaju primiti sažetak plana i uvjeriti se da se plan može uspješno provesti.

24. Ako su odobrena izuzeća u skladu s člankom 21. Direktive 2013/36/EU ili člankom 109. stavkom 1. Direktive 2013/36/EU u vezi s člankom 7. Uredbe (EU) br. 575/2013, odredbe ovih Smjernica trebaju primjenjivati matično društvo u državi članici na sebe i svoja društva kćeri ili središnje tijelo za cjelinu koju čine to središnje tijelo i njegovi povezani subjekti.

25. Institucije i institucije za platni promet koje su društva kćeri matičnog društva iz EU-a ili matičnog društva iz države članice kojima nisu odobrena izuzeća na temelju članka 21. Direktive 2013/36/EU ili članka 109. stavka 1. Direktive 2013/36/EU u vezi s člankom 7. Uredbe (EU) br. 575/2013 trebaju osigurati da svaka pojedinačno bude usklađena s ovim Smjernicama.

Glava II. – Procjena ugovora o eksternalizaciji

3 Eksternalizacija

26. Institucije i institucije za platni promet trebaju utvrditi odgovara li određeni ugovor sklopljen s trećom stranom definiciji eksternalizacije. U okviru te procjene treba uzeti u obzir izvršava li pružatelj usluga funkciju (ili neki njezin dio) koja mu se eksternalizira redovito ili kontinuirano i pripada li ta funkcija (ili neki njezin dio) funkcijama koje bi realno mogle obavljati institucije ili institucije za platni promet, čak i ako predmetna institucija ili institucija za platni promet u prošlosti nije sama obavljala tu funkciju.

27. Ako ugovor sklopljen s pružateljem usluga obuhvaća više funkcija, institucije i institucije za platni promet trebaju u svojoj procjeni razmotriti sve aspekte ugovora, na primjer ako se u okviru usluge koja se pruža osigurava računalna oprema za pohranu podataka i izrada sigurnosne kopije podataka, te aspekte treba razmotriti zajedno.

28. Institucije i institucije za platni promet u načelu ne trebaju sljedeće smatrati eksternalizacijom:

a. funkciju koju u skladu sa zakonom treba izvršavati pružatelj usluga, npr. zakonsku reviziju;

b. usluge pružanja informacija o tržištu (npr. podatci koje pružaju društva Bloomberg, Moody's, Standard & Poor's, Fitch);

c. globalne mrežne infrastrukture (npr. Visa, MasterCard);

d. sustave poravnanja i namire između klirinških kuća, središnjih drugih ugovornih strana te institucija za namiru i njihovih članova;

e. globalne infrastrukture za financijsku komunikaciju koje podliježu nadzoru relevantnih tijela;

f. usluge korespondentnog bankarstva; i

g. pribavljanje usluga koje inače ne obavlja institucija ili institucija za platni promet (npr. arhitektonski savjeti, pružanje pravnih mišljenja i zastupanje na sudu i pred upravnim tijelima, čišćenje, vrtlarstvo i održavanje objekata institucije ili institucije za platni promet, zdravstvene usluge, servisno održavanje službenih automobila, ugostiteljske usluge, automati za prodaju, uredski poslovi, putničke usluge, poštanske usluge, recepcionarske i tajničke usluge, telefonska centrala), dobara (npr. plastične kartice, čitači kartica, uredski pribor, osobna računala, namještaj) ili komunalnih usluga (npr. električna energija, plin, voda, telefonska linija).

4 Ključne ili važne funkcije

29. Institucije i institucije za platni promet uvijek trebaju funkciju smatrati ključnom ili važnom u sljedećim slučajevima[16]:

    a. ako bi pogreška ili nedostatak u njezinu izvršavanju značajno naštetio:

        i. njihovoj kontinuiranoj usklađenosti s uvjetima iz odobrenja za rad ili drugim obvezama u okviru Direktive 2013/36/EU, Uredbe (EU) br. 575/2013, Direktive 2014/65/EU, Direktive (EU) 2015/2366 i Direktive 2009/110/EZ te njihovim regulatornim obvezama;

        ii. njihovim financijskim rezultatima; ili

        iii. stabilnosti ili nastavku njihovih bankarskih i platnih usluga i aktivnosti;

[16] Vidjeti i članak 30. Delegirane uredbe Komisije (EU) 2017/565 od 25. travnja 2016. o dopuni Direktive 2014/65/EU Europskog parlamenta i Vijeća u vezi s organizacijskim zahtjevima i uvjetima poslovanja investicijskih društava te izrazima definiranima za potrebe te Direktive.

b. ako se eksternaliziraju operativni zadatci kontrolnih funkcija, osim ako procjena pokaže da nepružanje eksternalizirane funkcije ili neodgovarajuće pružanje eksternalizirane funkcije ne bi imalo negativan utjecaj na učinkovitost kontrolne funkcije;

c. ako namjeravaju eksternalizirati funkcije bankarskih aktivnosti ili platnih usluga u mjeri za koju bi bilo potrebno odobrenje za rad[17] nadležnog tijela, kako je navedeno u odjeljku 12.1.

30. U slučaju institucija, posebnu pozornost treba posvetiti procjeni ključnosti ili važnosti funkcija ako se eksternalizacija odnosi na funkcije koje su povezane s temeljnim linijama poslovanja i ključnim funkcijama kako su definirane u članku 2. stavku 1. točki (35) i članku 2. stavku 1. točki (36) Direktive 2014/59/EU[18] i koje su utvrdile institucije s pomoću kriterija iz članaka 6. i 7. Delegirane uredbe Komisije (EU) 2016/778[19]. Funkcije koje su potrebne za obavljanje djelatnosti u okviru temeljnih linija poslovanja ili ključnih funkcija trebaju se smatrati ključnim ili važnim funkcijama za potrebe ovih Smjernica, osim ako procjena institucije pokaže da nepružanje eksternalizirane funkcije ili neodgovarajuće pružanje eksternalizirane funkcije ne bi imalo negativan utjecaj na operativni kontinuitet temeljne linije poslovanja ili ključne funkcije.

31. Pri procjeni toga odnosi li se eksternalizacija na funkciju koja je ključna ili važna, institucije i institucije za platni promet uzimaju u obzir, zajedno s rezultatom procjene rizika koja je opisana u odjeljku 12.2., najmanje sljedeće čimbenike:

a. je li ugovor o eksternalizaciji izravno povezan s pružanjem bankarskih aktivnosti ili platnih usluga[20] za koje imaju odobrenje za rad;

b. mogući utjecaj bilo kakvog prekida eksternalizirane funkcije ili nemogućnosti pružatelja usluga da kontinuirano pruža uslugu na dogovorenoj razini usluge na:

i. njihovu kratkoročnu i dugoročnu financijsku otpornost i održivost, uključujući, ako je primjenjivo, njihovu imovinu, kapital, troškove, izvore financiranja, likvidnost, dobit i gubitak;

ii. kontinuitet njihova poslovanja i operativnu otpornost;

iii. njihov operativni rizik, uključujući rizik nesavjesnog ponašanja, rizik informacijsko-komunikacijske tehnologije (IKT) te pravni rizik;

---

[17] Vidjeti djelatnosti navedene u Prilogu I. Direktivi 2013/36/EU.

[18] Direktiva 2014/59/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o uspostavi okvira za oporavak i sanaciju kreditnih institucija i investicijskih društava te o izmjeni Direktive Vijeća 82/891/EEZ i direktiva 2001/24/EZ, 2002/47/EZ, 2004/25/EZ, 2005/56/EZ, 2007/36/EZ, 2011/35/EU, 2012/30/EU i 2013/36/EU te uredbi (EU) br. 1093/2010 i (EU) br. 648/2012 Europskog parlamenta i Vijeća (Direktiva o oporavku i sanaciji banaka) (SL L 173, 12. 6. 2014., str. 190.).

[19] Delegirana uredba Komisije (EU) 2016/778 od 2. veljače 2016. o dopuni Direktive 2014/59/EU Europskog parlamenta i Vijeća u pogledu okolnosti i uvjeta u kojima se plaćanje izvanrednih ex post doprinosa može djelomično ili u cijelosti odgoditi te o kriterijima za utvrđivanje aktivnosti, usluga i djelatnosti povezanih s ključnim funkcijama i za utvrđivanje linija poslovanja i pripadajućih usluga u pogledu temeljnih linija poslovanja (SL L 131, 20. 5. 2016., str. 41.).

[20] Vidjeti djelatnosti navedene u Prilogu I. Direktivi 2013/36/EU.

iv. njihov reputacijski rizik;

v. ako je primjenjivo, njihov plan oporavka i sanacije, mogućnost sanacije i operativni kontinuitet u situaciji rane intervencije, oporavka ili sanacije;

c. mogući utjecaj ugovora o eksternalizaciji na njihovu sposobnost:

i. utvrđivanja i praćenja svih rizika te upravljanja njima;

ii. ispunjavanja svih pravnih i regulatornih zahtjeva;

iii. provedbe odgovarajućih revizija u pogledu eksternalizirane funkcije;

d. mogući utjecaj na usluge koje pružaju svojim klijentima;

e. sve ugovore o eksternalizaciji, ukupnu izloženost institucije ili institucije za platni promet prema istom pružatelju usluga i mogući kumulativni učinak ugovora o eksternalizaciji u istom području poslovanja;

f. veličinu i složenost zahvaćenog područja poslovanja;

g. mogućnost prilagodbe predloženog ugovora o eksternalizaciji bez zamjene ili revidiranja temeljnog ugovora;

h. mogućnost prijenosa, ugovorno i u praksi, predloženog ugovora o eksternalizaciji na drugog pružatelja usluga ako je to potrebno ili poželjno, uključujući procijenjene rizike, prepreke za kontinuitet poslovanja, troškove i vremenski okvir u kojem to treba učiniti („zamjenjivost”);

i. mogućnost ponovne integracije eksternalizirane funkcije u instituciju ili instituciju za platni promet, ako je to potrebno ili poželjno;

j. zaštitu podataka i mogući utjecaj povrede povjerljivosti ili propusta u osiguravanju dostupnosti i integriteta podataka na instituciju ili instituciju za platni promet te njezine klijente, uključujući, ali ne isključivo, usklađenost s Uredbom (EU) 2016/679[21].

[21] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

Glava III. – Okvir upravljanja

5 Stabilni sustavi upravljanja i rizik treće strane

32. Kao dio ukupnog okvira unutarnje kontrole[22], uključujući i mehanizme unutarnje kontrole[23], institucije i institucije za platni promet trebaju uspostaviti sveobuhvatan okvir upravljanja rizicima za cijelu instituciju koji obuhvaća sve poslovne linije i interne jedinice. U tom okviru institucije i institucije za platni promet trebaju utvrditi sve svoje rizike i upravljati njima, uključujući rizike koji proizlaze iz ugovora s trećim stranama. Okvir upravljanja rizicima treba omogućiti institucijama i institucijama za platni promet da donose informirane odluke o preuzimanju rizika i osiguraju odgovarajuću provedbu mjera za upravljanje rizicima, uključujući kibernetičke rizike[24].

33. Institucije i institucije za platni promet trebaju, uzimajući u obzir načelo proporcionalnosti u skladu s odjeljkom 1., utvrditi, procijeniti i pratiti sve rizike koji proizlaze iz ugovora s trećim stranama kojima jesu ili bi mogle biti izložene, bez obzira na to je li ili nije riječ o ugovorima o eksternalizaciji, te upravljati tim rizicima. Rizike, posebno operativne rizike, koji proizlaze iz svih ugovora s trećim stranama, uključujući one iz stavaka 26. i 28., treba procijeniti u skladu s odjeljkom 12.2.

34. Institucije i institucije za platni promet trebaju osigurati svoju usklađenost sa svim zahtjevima iz Uredbe (EU) 2016/679, uključujući i njihove ugovore s trećim stranama i ugovore o eksternalizaciji.

6 Stabilni sustavi upravljanja i eksternalizacija

35. Eksternalizacija funkcija ne smije za posljedicu imati delegiranje odgovornosti upravljačkog tijela. Institucije i institucije za platni promet ostaju potpuno odgovorne i zadužene za osiguravanje usklađenosti sa svim svojim regulatornim obvezama, uključujući sposobnost nadziranja eksternalizacije ključnih ili važnih funkcija.

36. Upravljačko tijelo u svakom je trenutku potpuno odgovorno i zaduženo najmanje za:

    a. osiguravanje da institucija ili institucija za platni promet kontinuirano ispunjava uvjete koje mora ispunjavati da bi zadržala svoje odobrenje za rad, uključujući sve uvjete koje je odredilo nadležno tijelo;

    b. unutarnju organizaciju institucije ili institucije za platni promet;

---

[22] Institucije bi trebale proučiti glavu V. Smjernica EBA-e o internom upravljanju.

[23] Vidjeti i članak 11. Direktive 2015/2366 (PSD2).

[24] Vidjeti i Smjernice EBA-e o IKT-u i upravljanju sigurnosnim rizicima (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) i Temeljne elemente skupine G7 u pogledu upravljanja kibernetičkim rizicima trećih strana u financijskom sektoru (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

c. utvrđivanje i procjenu sukoba interesa te upravljanje njima;

d. utvrđivanje strategija i politika institucije ili institucije za platni promet (npr. poslovnog modela, sklonosti preuzimanju rizika, okvira upravljanja rizicima);

e. nadziranje svakodnevnog upravljanja institucijom ili institucijom za platni promet, uključujući upravljanje svim rizicima povezanima s eksternalizacijom; i

f. nadzornu ulogu upravljačkog tijela u svojstvu nadzorne funkcije, uključujući nadziranje i praćenje donošenja upravljačkih odluka.

37. Eksternalizacija ne smije smanjiti zahtjeve u pogledu primjerenosti članova upravljačkog tijela institucije, direktore i osobe odgovorne za upravljanje institucijom za platni promet te nositelje ključnih funkcija. Institucije i institucije za platni promet trebaju imati odgovarajuću podjelu nadležnosti i i dostatne ljudske resurse s potrebnim vještinama kako bi osigurale primjereno upravljanje i nadziranje ugovora o eksternalizaciji.

38. Institucije i institucije za platni promet trebaju:

a. jasno dodijeliti odgovornosti za dokumentiranje, upravljenje i kontrolu ugovora o eksternalizaciji;

b. odrediti dostatne resurse za osiguravanje usklađenosti sa svim pravnim i regulatornim zahtjevima, uključujući ove Smjernice, te za dokumentiranje i praćenje svih ugovora o eksternalizaciji;

c. uzimajući u obzir odjeljak 1. ovih Smjernica, uspostaviti funkciju odgovornu za eksternalizaciju ili odrediti člana višeg rukovodstva koji izravno odgovara upravljačkom tijelu (npr. nositelja ključne funkcije u okviru kontrolne funkcije) te je zadužen za upravljanje rizicima povezanima s ugovorima o eksternalizaciji i njihovo nadziranje unutar okvira unutarnje kontrole institucije, kao i za nadziranje dokumentacije povezane s eksternalizacijom. Male i manje složene institucije ili institucije za platni promet trebaju minimalno osigurati jasnu podjelu zadataka i odgovornosti za upravljanje ugovorima o eksternalizaciji i njihovu kontrolu te funkciju odgovornosti za eksternalizaciju mogu dodijeliti članu upravljačkog tijela institucije ili institucije za platni promet.

39. Institucije ili institucije za platni promet trebaju u svakom trenutku održavati dostatnu razinu poslovanja, a ne pretvoriti se u „prazne ljušture” ili fiktivne subjekte. U tu svrhu trebaju:

a. u svakom trenutku ispunjavati sve uvjete svojeg odobrenja za rad [25], uključujući upravljačko tijelo koje učinkovito izvršava svoje odgovornosti utvrđene u stavku 36. ovih Smjernica;

b. zadržati jasan i transparentan organizacijski okvir i strukturu koja im omogućuje osiguravanje usklađenosti s pravnim i regulatornim zahtjevima;

c. ako se eksternaliziraju operativni zadatci kontrolnih funkcija (na primjer u slučaju eksternalizacije unutar grupe ili eksternalizacije unutar institucionalnih sustava zaštite), izvršavati odgovarajući nadzor i moći upravljati rizicima koji proizlaze iz eksternalizacije ključnih ili važnih funkcija; i

d. raspolagati dostatnim resursima i kapacitetima za osiguravanje usklađenosti s točkama od (a) do (c).

40. Institucije i institucije za platni promet trebaju pri eksternalizaciji osigurati najmanje sljedeće:

a. da mogu donositi i provoditi odluke o svojim poslovnim aktivnostima i ključnim ili važnim funkcijama, uključujući o onima koje su eksternalizirane;

b. da nastave uredno obavljati svoje poslovanje i pružati bankarske i platne usluge;

c. da se rizici povezani s trenutačnim i planiranim ugovorima o eksternalizaciji, uključujući rizike povezane s IKT-om i financijskom tehnologijom (fintech), utvrde i procijene, da se njima upravlja te da se smanjuju na odgovarajući način;

d. da se sklope odgovarajući sporazumi o povjerljivosti podataka i drugih informacija;

e. da se održava odgovarajuća razmjena relevantnih informacija s pružateljima usluga;

f. kad je riječ o eksternalizaciji ključnih ili važnih funkcija, da su sposobne poduzeti najmanje jednu od sljedećih mjera u odgovarajućem roku:

   i. prijenos funkcije na druge pružatelje usluga;

   ii. ponovna integracija funkcije; ili

   iii. prestanak poslovnih aktivnosti koje ovise o toj funkciji.

---

[25] Vidjeti i regulatorne tehničke standarde u skladu s člankom 8. stavkom 2. Direktive 2013/36/EU o informacijama koje treba dostaviti za izdavanje odobrenja za rad kreditnim institucijama, kao i provedbene tehničke standarde u skladu s člankom 8. stavkom 3. Direktive 2013/36/EU za standardne obrasce, predloške i postupke za dostavljanje informacija potrebnih za izdavanje odobrenja za rad kreditnim institucijama (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

Za institucije za platni promet vidjeti Smjernice EBA-e u okviru Direktive (EU) 2015/2366 (PSD2) o informacijama koje treba dostaviti za izdavanje odobrenja institucijama za platni promet i institucijama za elektronički novac i za registraciju pružatelja usluga informiranja o računu (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

g. ako osobne podatke obrađuju pružatelji usluga u EU-u i/ili trećim zemljama, da se provode odgovarajuće mjere te da se podatci obrađuju u skladu s Uredbom (EU) 2016/679.

7 Politika eksternalizacije

41. Upravljačko tijelo institucije ili institucije za platni promet[26] koja je sklopila ili planira sklopiti ugovore o eksternalizaciji treba odobravati, redovito revidirati i ažurirati pisanu politiku eksternalizacije te osiguravati njezinu provedbu, prema potrebi, na pojedinačnoj, potkonsolidiranoj i konsolidiranoj osnovi. Kad je riječ o institucijama, politika eksternalizacije treba biti u skladu s odjeljkom 8. Smjernica EBA-e o internom upravljanju te posebno treba uzimati u obzir zahtjeve utvrđene u odjeljku 18. (novi proizvodi i značajne promjene) tih smjernica. Institucije za platni promet isto tako mogu uskladiti svoje politike s odjeljcima 8. i 18. Smjernica EBA-e o internom upravljanju.

42. Politika treba obuhvatiti glavne faze životnog ciklusa ugovora o eksternalizaciji te definirati načela, odgovornosti i postupke povezane s eksternalizacijom. Konkretno, politika treba obuhvatiti najmanje:

    a. odgovornosti upravljačkog tijela u skladu sa stavkom 36., uključujući njegovu uključenost, prema potrebi, u donošenje odluka o eksternalizaciji ključnih ili važnih funkcija;

    b. uključenost poslovnih linija, kontrolnih funkcija i drugih pojedinaca u pogledu eksternalizacije;

    c. planiranje ugovora o eksternalizaciji, uključujući:

        i. definiranje poslovnih zahtjeva u pogledu ugovora o eksternalizaciji;

        ii. kriterije, uključujući one navedene u odjeljku 4., i postupke za utvrđivanje ključnih ili važnih funkcija;

        iii. utvrđivanje i procjenu rizika te upravljanje njima, u skladu s odjeljkom 12.2.;

        iv. dubinsku analizu potencijalnih pružatelja usluga, uključujući mjere propisane odjeljkom 12.3.;

        v. postupke utvrđivanja i procjene potencijalnih sukoba interesa, upravljanja njima i njihova smanjenja, u skladu s odjeljkom 8.;

        vi. planiranje kontinuiteta poslovanja u skladu s odjeljkom 9.;

[26] Vidjeti i Smjernice EBA-e o sigurnosnim mjerama za operativne i sigurnosne rizike povezane s platnim uslugama na temelju Direktive PSD2, dostupne na poveznici: 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

vii. postupak odobravanja novih ugovora o eksternalizaciji;

d. provedbu i praćenje ugovora o eksternalizaciji te upravljanje njima, uključujući:

i. kontinuiranu procjenu rada pružatelja usluga u skladu s odjeljkom 14.;

ii. postupke primanja obavijesti o promjenama i odgovora na promjene ugovora o eksternalizaciji ili pružatelja usluga (npr. njegova financijskog stanja, organizacijske ili vlasničke strukture, podeksternalizacije);

iii. neovisnu provjeru i reviziju usklađenosti s pravnim i regulatornim zahtjevima i politikama;

iv. postupke obnavljanja ugovora;

e. dokumentiranje i vođenje evidencije, uzimajući u obzir zahtjeve iz odjeljka 11.;

f. izlazne strategije i postupke otkaza ugovora, uključujući zahtjev za dokumentirani izlazni plan za svaku ključnu ili važnu funkciju koja se eksternalizira ako se izlazak smatra mogućim nakon što se uzmu u obzir mogući prekidi u pružanju usluge ili neočekivan otkaz ugovora o eksternalizaciji.

43. U politici eksternalizacije treba razlikovati sljedeće:

a. eksternalizaciju ključnih ili važnih funkcija i druge ugovore o eksternalizaciji;

b. eksternalizaciju pružateljima usluga koji imaju odobrenje nadležnog tijela za rad i onima koji ga nemaju;

c. eksternalizaciju unutar grupe, eksternalizaciju unutar istog institucionalnog sustava zaštite (uključujući subjekte u punom pojedinačnom ili zajedničkom vlasništvu institucija unutar institucionalnog sustava zaštite) i eksternalizaciju subjektima izvan grupe; i

d. eksternalizaciju pružateljima usluga u nekoj državi članici i eksternalizaciju pružateljima usluga u trećim zemljama.

44. Institucije i institucije za platni promet trebaju osigurati da politika obuhvaća utvrđivanje sljedećih mogućih učinaka eksternalizacije ključnih ili važnih funkcija te da se oni uzmu u obzir u postupku donošenja odluka:

a. profil rizičnosti institucije;

b. mogućnost nadziranja pružatelja usluga i upravljanja rizicima;

c. mjere za održavanje kontinuiteta poslovanja; i

d. obavljanje njihovih poslovnih aktivnosti.

8 Sukobi interesa

45. Institucije, u skladu s glavom IV., odjeljkom 11. Smjernica EBA-e o internom upravljanju[27], i institucije za platni promet trebaju utvrditi i procijeniti sukobe interesa u pogledu svojih ugovora o eksternalizaciji te njima upravljati.

46. Ako iz eksternalizacije proizlaze materijalni sukobi interesa, uključujući između subjekata unutar iste grupe ili institucionalnog sustava zaštite, institucije i institucije za platni promet moraju poduzeti odgovarajuće mjere za upravljanje tim sukobima interesa.

47. Ako funkcije obavlja pružatelj usluga koji je dio grupe ili član institucionalnog sustava zaštite ili je u vlasništvu institucije, institucije za platni promet, grupe ili institucija koje su članice institucionalnog sustava zaštite, uvjete (uključujući financijske uvjete) za eksternalizirane usluge treba utvrđivati po tržišnim uvjetima. Međutim, pri određivanju cijena usluga mogu se uzeti u obzir sinergije koje proizlaze iz pružanja istih ili sličnih usluga za nekoliko institucija unutar grupe ili institucionalnog sustava zaštite, pod uvjetom da pružatelj usluga ostane samostalno održiv; unutar grupe to treba vrijediti bez obzira na propast bilo kojeg drugog subjekta grupe.

9 Planovi kontinuiteta poslovanja

48. Institucije, u skladu sa zahtjevima iz članka 85. stavka 2. Direktive 2013/36/EU i glave VI. Smjernica EBA-e o internom upravljanju[28], i institucije za platni promet trebaju uspostaviti, održavati i redovito testirati odgovarajuće planove kontinuiteta poslovanja u pogledu eksternaliziranih ključnih ili važnih funkcija. Institucije i institucije za platni promet unutar grupe ili institucionalnog sustava zaštite mogu se osloniti na centralizirano uspostavljene planove kontinuiteta poslovanja u pogledu svojih eksternaliziranih funkcija.

49. Planovi kontinuiteta poslovanja trebaju uzimati u obzir mogućnost pada kvalitete pružanja eksternalizirane ključne ili važne funkcije do neprihvatljive razine ili potpunog nepružanja. Ti planovi trebaju uzimati u obzir i mogući učinak stečaja ili propasti pružatelja usluga iz drugih razloga te, kad je to relevantno, političke rizike u državi pružatelja usluga.

[27] Institucije za platni promet također mogu uskladiti svoje politike s tim smjernicama.

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

10 Funkcija unutarnje revizije

50. Aktivnosti funkcije unutarnje revizije[29] trebaju obuhvaćati, u skladu s pristupom temeljenim na procjeni rizika, neovisnu provjeru eksternaliziranih aktivnosti. Planom i programom revizije[30] osobito treba obuhvatiti ugovore o eksternalizaciji ključnih ili važnih funkcija.

51. Kad je riječ o postupku eksternalizacije, funkcija unutarnje revizije treba utvrditi najmanje:

    a. da se okvir kojim institucija ili institucija za platni promet uređuje eksternalizaciju, uključujući politiku eksternalizacije, provodi pravilno i učinkovito te da je u skladu s primjenjivim zakonima i propisima, strategijom rizika i odlukama upravljačkog tijela;

    b. prikladnost, kvalitetu i djelotvornost procjene ključnosti ili važnosti funkcija;

    c. prikladnost, kvalitetu i djelotvornost procjene rizika s obzirom na ugovore o eksternalizaciji te da su rizici u skladu sa strategijom rizika institucije;

    d. odgovarajuću uključenost upravljačkih tijela; i

    e. odgovarajuće praćenje ugovora o eksternalizaciji te upravljanje njima.

11 Zahtjevi s obzirom na dokumentiranje

52. Kao dio okvira upravljanja rizicima, institucije i institucije za platni promet trebaju voditi ažuran registar informacija o svim ugovorima o eksternalizaciji na razini institucije te, prema potrebi, na potkonsolidiranoj i konsolidiranoj razini, kako je utvrđeno u odjeljku 2.; isto tako, trebaju na odgovarajući način dokumentirati sve postojeće ugovore o eksternalizaciji, razlikujući ugovore o eksternalizaciji ključnih ili važnih funkcija i druge ugovore o eksternalizaciji. Uzimajući u obzir nacionalno pravo, institucije tijekom odgovarajućeg razdoblja u registru trebaju čuvati dokumentaciju o završenim ugovorima o eksternalizaciji, kao i prateću dokumentaciju.

53. Uzimajući u obzir glavu I. ovih Smjernica te pod uvjetima iz stavka 23. točke (d), za institucije i institucije za platni promet unutar određene grupe, institucije koje su trajno povezane sa središnjim tijelom ili institucije koje su članice istog institucionalnog sustava zaštite može se voditi centralizirani registar.

54. Registar treba sadržavati najmanje sljedeće informacije za sve postojeće ugovore o eksternalizaciji:

---

[29] Kad je riječ o odgovornostima funkcije unutarnje revizije, institucije bi trebale proučiti odjeljak 22. Smjernica EBA-e o internom upravljanju (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-), a institucije za platni promet trebale bi proučiti smjernicu br. 5 Smjernica EBA-e o izdavanju odobrenja institucijama za platni promet (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

[30] Vidjeti i Smjernice EBA-e o postupku nadzorne provjere i ocjene: 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

a. referentni broj svakog ugovora o eksternalizaciji;

b. datum početka i, prema potrebi, datum sljedećeg produženja ugovora, datum završetka i/ili otkazne rokove za pružatelja usluga i za instituciju ili instituciju za platni promet;

c. kratak opis eksternalizirane funkcije, uključujući podatke koji se eksternaliziraju i informaciju o tome je li došlo do prijenosa osobnih podataka ili nije (npr. popunjavanjem odgovarajućeg polja s „da" ili „ne") te je li njihova obrada eksternalizirana nekom pružatelju usluga;

d. kategoriju koju dodjeljuje institucija ili institucija za platni promet, a koja odražava prirodu funkcije kako je opisana u točki (c) (npr. informacijska tehnologija (IT), kontrolna funkcija), što bi trebalo olakšati identifikaciju različitih vrsta ugovora;

e. naziv pružatelja usluga, broj iz registra poslovnih subjekata, identifikator pravnog subjekta (ako je dostupan), registriranu adresu i druge relevantne podatke za kontakt te naziv matičnog društva (ako postoji);

f. zemlju ili zemlje u kojoj će usluga biti pružena, uključujući lokaciju (tj. zemlju ili regiju) podataka;

g. smatra li se ili ne (da/ne) eksternalizirana funkcija ključnom ili važnom, uključujući, prema potrebi, kratak sažetak razloga zbog kojih se eksternalizirana funkcija smatra ključnom ili važnom;

h. u slučaju eksternalizacije pružatelju usluga računarstva u oblaku, model usluge u oblaku i model uporabe oblaka, tj. javni/privatni/hibridni/zajednički, kao i konkretna priroda podataka koji se čuvaju i lokacije (tj. zemlje ili regije) na kojima će se pohranjivati ti podatci;

i. datum zadnje procjene ključnosti ili važnosti eksternalizirane funkcije.

55. U slučaju eksternalizacije ključnih ili važnih funkcija, registar treba sadržavati najmanje sljedeće dodatne informacije:

a. institucije, institucije za platni promet i druga društva obuhvaćena bonitetnom konsolidacijom ili institucionalnim sustavom zaštite, ako postoji, koji se služe eksternalizacijom;

b. je li ili nije pružatelj usluga ili podizvođač usluga dio grupe ili član institucionalnog sustava zaštite ili u vlasništvu institucija ili institucija za platni promet unutar grupe ili u vlasništvu članova institucionalnog sustava zaštite;

c. datum posljednje procjene rizika i kratak sažetak njezinih glavnih rezultata;

d. informacije o pojedincu ili tijelu nadležnom za odlučivanje (npr. upravljačko tijelo) u instituciji ili instituciji za platni promet koje je odobrilo ugovor o eksternalizaciji;

e. mjerodavno pravo za ugovor o eksternalizaciji;

f. datum posljednje i sljedeće planirane revizije, prema potrebi;

g. prema potrebi, imena svih podizvođača kojima se podeksternaliziraju značajni dijelovi ključne ili važne funkcije, uključujući zemlju u kojoj su registrirani podizvođači, u kojoj će se pružati usluga i, ako je primjenjivo, lokaciju (tj. zemlju ili regiju) na kojoj će se pohranjivati podatci;

h. rezultat procjene zamjenjivosti pružatelja usluga (jednostavno, teško, nemoguće), mogućnost ponovne integracije ključne ili važne funkcije u instituciju ili instituciju za platni promet ili učinak prekida obavljanja ključne ili važne funkcije;

i. utvrđivanje alternativnih pružatelja usluga u skladu s točkom (h);

j. podržava li eksternalizirana ključna ili važna funkcija poslovne aktivnosti koje su vremenski kritične;

k. procjenu godišnjeg proračunskog troška.

56. Institucije i institucije za platni promet trebaju, na zahtjev, nadležnom tijelu dostaviti ili potpuni registar svih postojećih ugovora o eksternalizaciji[31] ili konkretne dijelove registra, kao što su informacije o svim ugovorima o eksternalizaciji obuhvaćenima nekom od kategorija iz stavka 54. točke (d) ovih Smjernica (npr. svi ugovori o eksternalizaciji koji se odnose na IT). Institucije i institucije za platni promet trebaju te informacije pružati u elektroničkom formatu koji se može obrađivati (npr. format koji se obično upotrebljava u bazama podataka, vrijednosti odvojene zarezom).

57. Institucije i institucije za platni promet trebaju, na zahtjev, nadležnom tijelu dostaviti sve informacije potrebne da bi se nadležnom tijelu omogućio djelotvoran nadzor nad institucijom ili institucijom za platni promet, uključujući, prema potrebi, presliku ugovora o eksternalizaciji.

58. Ne dovodeći u pitanje članak 19. stavak 6. Direktive (EU) 2015/2366, institucije i institucije za platni promet trebaju na odgovarajući način i pravodobno obavijestiti nadležna tijela ili započeti supervizorski dijalog s nadležnim tijelima o planiranim eksternalizacijama ključnih ili važnih funkcija i/ili kad eksternalizirana funkcija postane ključna ili važna te im dostaviti najmanje informacije navedene u stavku 54.

[31] Vidjeti i Smjernice EBA-e o postupku nadzorne provjere i ocjene, dostupne na poveznici: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

59. Institucije i institucije za platni promet[32] trebaju pravodobno obavijestiti nadležna tijela o značajnim promjenama i/ili ozbiljnim događajima u pogledu svojih ugovora o eksternalizaciji koji bi mogli materijalno utjecati na nastavak obavljanja poslovnih djelatnosti institucije ili institucije za platni promet.

60. Institucije i institucije za platni promet trebaju na odgovarajući način dokumentirati procjene izvršene u skladu s glavom IV. i rezultate svojeg kontinuiranog praćenja (npr. rad pružatelja usluga, usklađenost s ugovorenim razinama usluge, druge ugovorne i regulatorne zahtjeve, ažuriranja procjene rizika).

Glava IV. – Postupak eksternalizacije

12 Analiza prije eksternalizacije

61. Prije ugovaranja bilo kakve eksternalizacije, institucije i institucije za platni promet trebaju:

    a. procijeniti odnosi li se ugovor o eksternalizaciji na neku ključnu ili važnu funkciju, kako je utvrđeno u glavi II.;

    b. procijeniti jesu li ispunjeni supervizorski uvjeti za eksternalizaciju utvrđeni u odjeljku 12.1.;

    c. utvrditi i procijeniti sve relevantne rizike koji proizlaze iz ugovora o eksternalizaciji u skladu s odjeljkom 12.2.;

    d. provesti odgovarajuću dubinsku analizu potencijalnih pružatelja usluga u skladu s odjeljkom 12.3.;

    e. utvrditi i procijeniti, u skladu s odjeljkom 8., sukobe interesa koji bi mogli proizići iz eksternalizacije.

12.1 Supervizorski uvjeti za eksternalizaciju

62. Institucije i institucije za platni promet trebaju osigurati da se funkcije bankarskih aktivnosti[33] ili platnih usluga, ako je za obavljanje tih funkcija potrebno odobrenje ili registracija koje dodjeljuje nadležno tijelo u državi članici u kojoj te institucije imaju odobrenje za rad, eksternaliziraju pružatelju usluga u istoj ili drugoj državi samo ako je ispunjen jedan od sljedećih uvjeta:

[32] Vidjeti i Smjernice EBA-e o izvješćivanju o značajnim incidentima u skladu s Drugom direktivom o platnim uslugama, dostupne na poveznici: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

[33] Vidjeti članak 9. Direktive o kapitalnim zahtjevima, kojim se predviđa zabrana osobama ili društvima koja nisu kreditne institucije da obavljaju poslove primanja depozita ili ostalih povratnih sredstava od javnosti.

a. pružatelj usluga ima odobrenje nadležnog tijela ili ga je ono registriralo za obavljanje predmetnih bankarskih aktivnosti ili pružanje platnih usluga; ili

b. pružatelju usluga na neki je drugi način dopušteno obavljati predmetne bankarske aktivnosti ili pružati platne usluge u skladu s relevantnim nacionalnim pravnim okvirom.

63. Institucije i institucije za platni promet trebaju osigurati da se funkcije bankarskih aktivnosti ili platnih usluga, ako je za obavljanje tih funkcija potrebno odobrenje ili registracija koje dodjeljuje nadležno tijelo u državi članici u kojoj imaju odobrenje za rad, eksternaliziraju pružatelju usluga u nekoj trećoj zemlji samo ako su ispunjeni sljedeći uvjeti:

a. pružatelj usluga ima odobrenje ili je registriran za obavljanje predmetne bankarske aktivnosti ili pružanje platne usluge u trećoj zemlji te ga nadzire relevantno nadležno tijelo u toj trećoj zemlji (koje se naziva „nadzorno tijelo”);

b. sklopljen je odgovarajući sporazum o suradnji, na primjer u obliku memoranduma o razumijevanju ili ugovora o kolegiju, između nadležnih tijela odgovornih za nadzor institucije i nadzornih tijela odgovornih za nadzor pružatelja usluga; i

c. ugovorom o suradnji navedenim u točki (b) treba osigurati da nadležna tijela mogu najmanje:

i. na zahtjev dobiti sve informacije potrebne za izvršavanje svojih nadzornih zadataka u skladu s Direktivom 2013/36/EU, Uredbom (EU) br. 575/2013, Direktivom (EU) 2015/2366 i Direktivom 2009/110/EZ;

ii. dobiti odgovarajući pristup svim podatcima, dokumentima, prostorima ili osoblju u trećoj zemlji relevantnima za izvršavanje nadzornih ovlasti;

iii. što je prije moguće primiti informacije od nadzornog tijela u trećoj zemlji za potrebe istraživanja navodnih povreda zahtjeva iz Direktive 2013/36/EU, Uredbe (EU) br. 575/2013, Direktive (EU) 2015/2366 i Direktive 2009/110/EZ; i

iv. surađivati s relevantnim nadzornim tijelima u trećoj zemlji u pogledu postupanja u slučaju povrede primjenjivih regulatornih zahtjeva i nacionalnog prava u državi članici. Ta suradnja treba uključivati, među ostalim, zaprimanje informacija o mogućim kršenjima primjenjivih regulatornih zahtjeva od nadzornih tijela u trećoj zemlji što je prije moguće.

12.2 Procjena rizika koji proizlaze iz ugovora o eksternalizaciji

64. Institucije i institucije za platni promet trebaju, prije ugovaranja eksternalizacije, procijeniti moguć učinak ugovora o eksternalizaciji na svoj operativni rizik, uzeti u obzir rezultate te

procjene pri donošenju odluke o eksternalizaciji funkcije određenom pružatelju usluga i poduzeti odgovarajuće korake kako bi se izbjegli nepotrebni dodatni operativni rizici.

65. Ta procjena treba uključivati, prema potrebi, scenarije mogućih događaja poveznih s rizikom, uključujući događaje s velikim gubicima povezane s operativnim rizikom. U okviru analize scenarija, institucije i institucije za platni promet trebaju procijeniti moguć utjecaj neuspjelih ili neadekvatnih usluga, uključujući rizike koji proizlaze iz neuspjelih ili neadekvatnih procesa, sustava, ljudi ili iz vanjskih događaja. Institucije i institucije za platni promet trebaju, uzimajući u obzir načelo proporcionalnosti iz odjeljka 1., dokumentirati izvršene analize i njihove rezultate te procijeniti u kojoj mjeri bi eksternalizacija povećala ili smanjila operativni rizik. Uzimajući u obzir glavu I., male i jednostavne institucije i institucije za platni promet mogu primijeniti pristup kvalitativne procjene rizika, dok velike ili složene institucije trebaju primjenjivati sofisticiraniji pristup koji uključuje upotrebu unutarnjih i vanjskih podataka o gubicima, ako su dostupni, za potrebe analize scenarija.

66. U okviru procjene rizika, institucije i institucije za platni promet trebaju uzeti u obzir i očekivane koristi i troškove predloženog ugovora o eksternalizaciji, uključujući ponderiranje rizika koji se mogu smanjiti ili kojima se može bolje upravljati u odnosu na rizike koji mogu proizići iz predloženog ugovora o eksternalizaciji, uzimajući u obzir najmanje:

    a. koncentracijske rizike koji, među ostalim, proizlaze iz:

        i. eksternalizacije dominantnom pružatelju usluga kojeg nije jednostavno zamijeniti; i

        ii. većeg broja ugovora o eksternalizaciji sklopljenih s istim pružateljem usluga ili usko povezanim pružateljima usluga;

    b. ukupne rizike koji proizlaze iz eksternalizacije nekoliko funkcija unutar institucije ili institucije za platni promet i, u slučaju grupa institucija ili institucionalnih sustava zaštite, ukupne rizike na konsolidiranoj razini ili na razini institucionalnog sustava zaštite;

    c. u slučaju značajnih institucija, rizik „step-in”, odnosno rizik koji može proizići iz potrebe pružanja financijske potpore pružatelju usluga suočenom s poteškoćama ili iz potrebe preuzimanja njegovih poslovnih djelatnosti; i

    d. mjere koje provode institucija ili institucija za platni promet i pružatelj usluga s ciljem upravljanja rizicima i njihova smanjivanja.

67. Ako ugovor o eksternalizaciji uključuje mogućnost da pružatelj usluga podeksternalizira ključne ili važne funkcije drugim pružateljima usluga, institucije i institucije za platni promet trebaju uzeti u obzir sljedeće:

a. rizike povezane s podeksternalizacijom, uključujući dodatne rizike koji mogu nastati ako je lokacija podizvođača u trećoj zemlji ili zemlji različitoj od one u kojoj je pružatelj usluga;

b. rizik od toga da dugi i složeni lanci podeksternalizacije smanjuju sposobnost institucija ili institucija za platni promet da nadziru eksternalizirane ključne ili važne funkcije kao i sposobnost nadležnih tijela da ih učinkovito nadziru.

68. Pri izvršavanju procjene rizika prije eksternalizacije i tijekom praćenja rada pružatelja usluga, institucije i institucije za platni promet trebaju najmanje:

a. utvrditi i razvrstati relevantne funkcije i povezane podatke i sustave s obzirom na njihovu osjetljivost i potrebne zaštitne mjere;

b. provesti podrobnu, na procjeni rizika utemeljenu, analizu funkcija i povezanih podataka i sustava za koje se razmatra eksternalizacija ili koji su eksternalizirani te razmotriti moguće rizike, prije svega operativne rizike, uključujući pravni, reputacijski, rizik IKT-a i rizik usklađenosti, kao i ograničenja u pogledu nadzora povezana sa zemljama u kojima se pružaju ili bi se mogle pružati eksternalizirane usluge i u kojima se pohranjuju ili će se vjerojatno pohranjivati podatci;

c. razmotriti utjecaj lokacije pružatelja usluga (u EU-u ili izvan njega);

d. razmotriti političku stabilnost i sigurnosno stanje predmetnih država, uključujući:

i. zakone koji su na snazi, uključujući zakone o zaštiti podataka;

ii. odredbe o provođenju zakona koje su na snazi; i

iii. odredbe stečajnog zakona koje bi se primjenjivale u slučaju propasti pružatelja usluga te sva ograničenja do kojih bi došlo s obzirom na hitan oporavak podataka institucije ili institucije za platni promet;

e. definirati i donijeti odluku o primjerenoj razini zaštite povjerljivosti podataka, kontinuitetu eksternaliziranih aktivnosti te integritetu i sljedivosti podataka i sustava u kontekstu planirane eksternalizacije. Institucije i institucije za platni promet trebaju razmotriti i konkretne mjere, gdje je to potrebno, za podatke u prijenosu, podatke u memoriji i pohranjene podatke, kao što je upotreba tehnologija enkripcije, zajedno s odgovarajućom arhitekturom upravljanja ključevima;

f. uzeti u obzir činjenicu je li pružatelj usluga društvo kći ili matično društvo institucije, je li uključen u računovodstvenu konsolidaciju ili je član ili u vlasništvu institucija koje su članice nekog institucionalnog sustava zaštite i, ako je tako, u kojoj ga mjeri ta institucija kontrolira ili može utjecati na njegove radnje, u skladu s odjeljkom 2.

12.3 Dubinska analiza

69. Prije sklapanja ugovora o eksternalizaciji i razmatranja operativnih rizika povezanih s funkcijom koju treba eksternalizirati, institucije i institucije za platni promet trebaju u okviru svojih postupaka odabira i procjene osigurati primjerenost pružatelja usluga.

70. Kad je riječ o ključnim ili važnim funkcijama, institucije i institucije za platni promet trebaju osigurati da pružatelj usluga ima poslovni ugled, odgovarajuće i dostatne sposobnosti, stručnost, kapacitete, resurse (npr. ljudske, IT, financijske), organizacijsku strukturu i, prema potrebi, potrebna regulatorna odobrenja ili registracije za obavljanje ključne ili važne funkcije na pouzdan i profesionalan način kako bi ispunio svoje obveze za trajanja predloženog ugovora.

71. Dodatni čimbenici koje treba razmotriti pri provedbi dubinske analize potencijalnog pružatelja usluga uključuju, među ostalim:

    a. njegov poslovni model, prirodu, veličinu, složenost, financijsko stanje, vlasničku strukturu i strukturu grupe;

    b. dugoročne odnose s pružateljima usluga koji su već procijenjeni i pružaju usluge instituciji ili instituciji za platni promet;

    c. činjenicu je li pružatelj usluga matično društvo ili društvo kći institucije ili institucije za platni promet, je li uključen u računovodstvenu konsolidaciju institucije ili je član ili u vlasništvu institucija koje su članovi istog institucionalnog sustava zaštite kojem pripada institucija;

    d. činjenicu je li pružatelj usluga pod nadzorom nadležnih tijela.

72. Ako eksternalizacija uključuje obradu osobnih ili povjerljivih podataka, institucije i institucije za platni promet trebaju se uvjeriti da pružatelj usluga provodi odgovarajuće tehničke i organizacijske mjere potrebne za zaštitu podataka.

73. Institucije i institucije za platni promet trebaju poduzeti odgovarajuće korake kako bi osigurale da pružatelji usluga postupaju u skladu s njihovim vrijednostima i kodeksom ponašanja. Konkretno, kad je riječ o pružateljima usluga u trećim zemljama i, ako je primjenjivo, njihovim podizvođačima, institucije i institucije za platni promet trebaju se uvjeriti da pružatelj usluga posluje na etički i društveno odgovoran način te da poštuje međunarodne standarde ljudskih prava (npr. Europsku konvenciju o ljudskim pravima) i zaštite okoliša i osigurava primjerene radne uvjete, uključujući zabranu rada djece.

13 Ugovorna faza

74. Prava i obveze institucije, institucije za platni promet i pružatelja usluga treba jasno odrediti i navesti u pisanom ugovoru.

75. U ugovoru o eksternalizaciji ključnih ili važnih funkcija treba navesti najmanje sljedeće:

    a. jasan opis eksternalizirane funkcije koja će se pružati;

    b. datum početka i datum završetka ugovora, ako je primjenjivo, te otkazne rokove za pružatelja usluga i za instituciju ili instituciju za platni promet;

    c. mjerodavno pravo za ugovor;

    d. financijske obveze ugovornih strana;

    e. je li dopuštena podeksternalizacija ključne ili važne funkcije ili nekih njezinih značajnih dijelova i, ako jest, uvjete iz odjeljka 13.1. koji se odnose na takvu podeksternalizaciju;

    f. lokacije (npr. regije ili zemlje) na kojima će se pružati predmetna ključna ili važna funkcija i/ili na kojima će se čuvati i obrađivati relevantni podatci, uključujući lokaciju na kojoj će se možda pohranjivati, kao i uvjete koje je potrebno ispuniti, uključujući zahtjev za obavješćivanje institucije ili institucije za platni promet u slučaju da pružatelj usluga predloži promjenu lokacije (lokacija);

    g. prema potrebi, odredbe u pogledu pristupačnosti, dostupnosti, integriteta, privatnosti i sigurnosti relevantnih podataka, kako je navedeno u odjeljku 13.2.;

    h. pravo institucije ili institucije za platni promet na kontinuirano praćenje rada pružatelja usluga;

    i. dogovorene razine usluge, što treba uključivati precizne kvantitativne i kvalitativne ciljeve uspješnosti za eksternaliziranu funkciju kako bi se omogućilo pravodobno praćenje te time i poduzimanje odgovarajućih korektivnih mjera ako se ne postigne dogovorena razina usluge;

    j. obveze pružatelja usluga u pogledu izvješćivanja institucije ili institucije za platni promet, uključujući obvezu pružatelja usluga u pogledu obavješćivanja o svakom događaju koji bi mogao materijalno utjecati na sposobnost pružatelja usluga da učinkovito izvršava ključnu ili važnu funkciju u skladu s dogovorenim razinama usluge i u skladu s primjenjivim zakonima i regulatornim zahtjevima te, prema potrebi, obveze podnošenja izvješća funkcije unutarnje revizije pružatelja usluga;

    k. treba li pružatelj usluga poduzeti obvezne mjere osiguranja od određenih rizika te, prema potrebi, razinu pokrića osiguranja koja se traži;

l. zahtjeve u pogledu uvođenja i testiranja poslovnih planova postupanja u kriznim situacijama;

m. odredbe kojima se osigurava da se podatcima u vlasništvu institucije ili institucije za platni promet može pristupiti u slučaju stečaja, sanacije ili prestanka poslovnih djelatnosti pružatelja usluga;

n. obvezu pružatelja usluga da surađuje s nadležnim tijelima i sanacijskim tijelima institucije ili institucije za platni promet, uključujući druge osobe koje ona imenuju;

o. kad je riječ o institucijama, jasno upućivanje na ovlasti nacionalnog sanacijskog tijela, posebno na članke 68. i 71. Direktive 2014/59/EU (Direktiva o oporavku i sanaciji kreditnih institucija i investicijskih društava) te konkretno na opis „bitnih obveza" iz ugovora u smislu članka 68. te direktive;

p. neograničeno pravo institucija, institucija za platni promet i nadležnih tijela na inspekciju i pravo na reviziju pružatelja usluga posebno u pogledu eksternalizirane ključne ili važne funkcije, kako je navedeno u odjeljku 13.3.;

q. prava otkaza ugovora, kako je navedeno u odjeljku 13.4.

13.1 Podeksternalizacija ključnih ili važnih funkcija

76. U ugovoru o eksternalizaciji treba odrediti je li dopuštena podeksternalizacija ključnih ili važnih funkcija ili njihovih značajnih dijelova.

77. Ako je dopuštena podeksternalizacija ključnih ili važnih funkcija, institucije i institucije za platni promet trebaju utvrditi je li dio funkcije koji se namjerava podeksternalizirati sâm po sebi ključan ili važan (odnosno značajan dio ključne ili važne funkcije) te, ako jest, upisati ga u registar.

78. Ako je podeksternalizacija ključnih ili važnih funkcija dopuštena, u pisanom ugovoru treba:

a. navesti sve vrste aktivnosti koje su isključene iz podeksternalizacije;

b. navesti uvjete koje je potrebno ispuniti u slučaju podeksternalizacije;

c. navesti da je pružatelj usluga obvezan nadzirati usluge koje je podugovorio kako bi osigurao da se kontinuirano ispunjavaju sve ugovorne obveze između pružatelja usluga i institucije ili institucije za platni promet;

d. zahtijevati od pružatelja usluga da prije podeksternalizacije podataka pribavi posebno ili opće pisano odobrenje od institucije ili institucije za platni promet[34];

[34] Vidjeti članak 28. Uredbe (EU) br. 2016/679.

e. uključiti obvezu pružatelja usluga da obavijesti instituciju ili instituciju za platni promet o svakoj planiranoj podeksternalizaciji, ili njezinim materijalno značajnim promjenama, posebno ako one mogu utjecati na sposobnost pružatelja usluga da ispuni svoje obveze iz ugovora o eksternalizaciji. To uključuje planirane bitne izmjene podizvođača i rok za slanje obavijesti; konkretno, rok za slanje obavijesti koji je potrebno utvrditi treba omogućiti instituciji ili instituciji za platni promet koja eksternalizira određenu funkciju da barem provede procjenu rizika predloženih promjena te da podnese prigovor na njih prije no što planirana podeksternalizacija, ili njezine značajne promjene, stupe na snagu;

f. osigurati, prema potrebi, da institucija ili institucija za platni promet ima pravo prigovora na planiranu podeksternalizaciju, ili njezine materijalno značajne promjene, ili da se zahtijeva izričito odobrenje;

g. osigurati da institucija ili institucija za platni promet ima ugovorno pravo otkaza ugovora u slučaju neopravdane podeksternalizacije, na primjer ako ta podeksternalizacija značajno povećava rizike za instituciju ili instituciju za platni promet ili ako pružatelj usluga izvrši podeksternalizaciju bez obavješćivanja institucije ili institucije za platni promet.

79. Institucije i institucije za platni promet trebaju se složiti s podeksternalizacijom samo ako se podizvođač obveže da će:

    a. poštovati sve primjenjive zakone, regulatorne zahtjeve i ugovorne obveze; i

    b. dati instituciji, instituciji za platni promet i nadležnom tijelu ista ugovorna prava pristupa i prava na reviziju koja im daje pružatelj usluga.

80. Institucije i institucije za platni promet trebaju osigurati da pružatelj usluga na odgovarajući način nadzire podizvođača usluga, u skladu s politikom koju definira institucija ili institucija za platni promet. Ako bi predložena podeksternalizacija mogla značajno negativno utjecati na ugovor o eksternalizaciji ključne ili važne funkcije ili bi dovela do materijalno značajnog povećanja rizika, uključujući ako se ne bi ispunili uvjeti iz stavka 79., institucija ili institucija za platni promet trebaju ostvariti svoje pravo prigovora na podeksternalizaciju, ako je takvo pravo ugovoreno, i/ili pravo na otkaz ugovora.

13.2 Sigurnost podataka i sustava

81. Institucije i institucije za platni promet trebaju osigurati da pružatelji usluga, kad je to relevantno, poštuju odgovarajuće standarde IT sigurnosti.

82. Prema potrebi (npr. kad je riječ o eksternalizaciji računarstva u oblaku ili drugoj eksternalizaciji u području IKT-a), institucije i institucije za platni promet trebaju u ugovoru o eksternalizaciji definirati zahtjeve u pogledu sigurnosti podataka i sustava te kontinuirano pratiti usklađenost s tim zahtjevima.

83. U slučaju eksternalizacije pružateljima usluga računarstva u oblaku i drugih ugovora o eksternalizaciji koji uključuju rukovanje osobnim ili povjerljivim podatcima te njihov prijenos, institucije i institucije za platni promet trebaju primjenjivati pristup temeljen na procjeni rizika s obzirom na lokaciju ili lokacije (tj. zemlju ili regiju) za pohranjivanje i obradu podataka te pitanja sigurnosti informacija.

84. Ne dovodeći u pitanje zahtjeve iz Uredbe (EU) 2016/679, institucije i institucije za platni promet trebaju pri eksternalizaciji (posebno u treće zemlje) uzeti u obzir razlike među nacionalnim propisima o zaštiti podataka. Institucije i institucije za platni promet trebaju osigurati da ugovor o eksternalizaciji uključuje obvezu pružatelja usluga da čuva povjerljive, osobne ili na drugi način osjetljive informacije te da poštuje sve pravne zahtjeve koji se odnose na zaštitu podataka, a primjenjuju se na instituciju ili instituciju za platni promet (npr. zaštita osobnih podataka i poštovanje bankovnih tajni ili sličnih pravnih obveza u pogledu povjerljivosti koje se odnose na informacije o klijentima, gdje je to primjenjivo).

13.3 Pravo pristupa, informiranja i pravo na reviziju

85. Institucije i institucije za platni promet trebaju u pisanom ugovoru o eksternalizaciji osigurati da njihova funkcija unutarnje revizije može obavljati reviziju eksternalizirane funkcije primjenom pristupa temeljenog na procjeni rizika.

86. Bez obzira na ključnost ili važnost eksternalizirane funkcije, u pisanim ugovorima o eksternalizaciji između institucija i pružatelja usluga treba se pozvati na ovlasti za prikupljanje informacija i istražne ovlasti nadležnih tijela i sanacijskih tijela u skladu s člankom 63. stavkom 1. točkom (a) Direktive 2014/59/EU i člankom 65. stavkom 3. Direktive 2013/36/EU kad je riječ o pružateljima usluga u državama članicama; trebaju se zajamčiti ta prava i kad je riječ o pružateljima usluga u trećim zemljama.

87. Kad je riječ o eksternalizaciji ključnih ili važnih funkcija, institucije i institucije za platni promet trebaju u pisanom ugovoru o eksternalizaciji osigurati da pružatelj usluga njima i njihovim nadležnim tijelima, uključujući sanacijska tijela, te svakoj drugoj osobi koju imenuju one ili njihova nadležna tijela odobri sljedeće:

    a. neograničen pristup svim relevantnim poslovnim prostorima (npr. glavnim uredima i operativnim/podatkovnim centrima), uključujući pristup cijelom nizu relevantnih uređaja, sustava, mreža, informacija i podataka koji se upotrebljavaju za pružanje eksternalizirane funkcije, kao i svim povezanim financijskim informacijama, osoblju i vanjskim revizorima pružatelja usluga („prava pristupa i informiranja”); i

    b. neograničena prava inspekcije i revizije u vezi s eksternalizacijom („pravo na reviziju”) kako bi im se omogućilo da prate eksternalizaciju i osiguravaju usklađenost sa svim primjenjivim regulatornim i ugovornim zahtjevima.

88. Za eksternalizaciju funkcija koje nisu ključne ili važne, institucije i institucije za platni promet trebaju osigurati pravo pristupa i pravo na reviziju navedena u stavku 87. točkama (a) i (b) te

odjeljku 13.3., uz primjenu pristupa temeljenog na procjeni rizika, uzimajući u obzir prirodu eksternalizirane funkcije i s njom povezane operativne i reputacijske rizike, prilagodljivost, moguć utjecaj na kontinuirano obavljanje aktivnosti i ugovorno razdoblje. Institucije i institucije za platni promet trebaju uzeti u obzir činjenicu da određene funkcije mogu s vremenom postati ključne ili važne.

89. Institucije i institucije za platni promet trebaju osigurati da se ugovorom o eksternalizaciji ili nekim drugim ugovorom ne sprječava ni ne ugrožava njihovo uspješno ostvarivanje prava pristupa i prava na reviziju ili pravo pristupa i pravo na reviziju nadležnih tijela ili trećih strana koje one imenuju za ostvarenje tih prava.

90. Institucije i institucije za platni promet trebaju ostvarivati svoja prava pristupa i prava na reviziju, na temelju pristupa temeljenog na procjeni rizika utvrđivati učestalost revizije i područja u kojima treba provesti reviziju te poštovati relevantne i općeprihvaćene nacionalne i međunarodne revizijske standarde[35].

91. Ne dovodeći u pitanje njihovu krajnju odgovornost u pogledu ugovora o eksternalizaciji, institucije i institucije za platni promet mogu primjenjivati:

    a. skupne revizije organizirane zajedno s drugim klijentima istog pružatelja usluga koje provode one same i ti klijenti ili treća strana koju su oni imenovali, kako bi se racionalnije iskoristili resursi za reviziju te kako bi se klijentima i pružatelju usluga smanjilo organizacijsko opterećenje;

    b. certifikate trećih strana i revizorska izvješća trećih strana ili izvješća unutarnje revizije koja je pružatelj usluga stavio na raspolaganje.

92. Kad je riječ o eksternalizaciji ključnih ili važnih funkcija, institucije i institucije za platni promet trebaju procijeniti jesu li certifikati i izvješća trećih strana navedeni u stavku 91. točki (b) prikladni i dostatni za ispunjavanje regulatornih obveza te se ne trebaju dugoročno oslanjati samo na ta izvješća.

93. Institucije i institucije za platni promet trebaju se služiti metodom iz stavka 91. točke (b) samo u sljedećim slučajevima:

    a. ako su zadovoljne planom revizije za eksternaliziranu funkciju;

    b. ako osiguraju da obuhvat certifikacije ili revizorskog izvješća uključuje sustave (tj. postupke, aplikacije, infrastrukturu, podatkovne centre itd.) i kontrole koje je nstitucija ili institucija za platni promet utvrdila kao ključne, kao i usklađenost s relevantnim regulatornih zahtjevima;

[35] Kad je riječ o institucijama, vidjeti odjeljak 22. Smjernica EBA-e o internom upravljanju: https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889

c. ako detaljno i kontinuirano pregledavaju sadržaj certifikacije ili revizorskih izvješća te provjeravaju da izvješća i certifikati nisu zastarjeli;

d. ako osiguravaju da su ključni sustavi i kontrole obuhvaćeni budućim verzijama certifikata ili revizijskog izvješća;

e. ako su zadovoljne osposobljenošću društva/osoba koji obavljaju reviziju ili certifikaciju (npr. u pogledu rotacije društva za reviziju ili certifikaciju, kvalifikacija, stručnosti, ponovnog izvođenja / provjere dokaza u temeljnom revizijskom dosjeu);

f. ako su se uvjerile da se certifikati izdaju i revizije provode u skladu s općepriznatim relevantnim profesionalnim standardima te uključuju testiranje operativne učinkovitosti postojećih ključnih kontrola;

g. ako imaju ugovorno pravo zatražiti proširenje obuhvata certifikacije ili revizorskih izvješća na druge relevantne sustave i kontrole; broj i učestalost takvih zahtjeva za izmjenu obuhvata trebaju biti razumni i opravdani sa stajališta upravljanja rizicima; i

h. ako zadržavaju ugovorno pravo provođenja, prema vlastitoj odluci, pojedinačnih revizija eksternalizacije ključnih ili važnih funkcija.

94. U skladu sa Smjernicama EBA-e o procjeni rizika IKT-a u okviru postupka nadzorne provjere i ocjene (SREP), institucije trebaju, kad je to relevantno, osigurati da mogu izvršiti sigurnosna penetracijska testiranja radi procjene učinkovitosti implementiranih kibernetičkih i internih sigurnosnih mjera i postupaka u području IKT-a[36]. Uzimajući u obzir glavu I., institucije za platni promet trebaju raspolagati i mehanizmima unutarnje kontrole za IKT, uključujući sigurnosne kontrole IKT-a i mjere za smanjenje rizika.

95. Prije planiranog izravnog posjeta lokaciji, institucije, institucije za platni promet, nadležna tijela i revizori ili treće strane koji djeluju u ime institucije, institucije za platni promet ili nadležnih tijela trebaju pružatelju usluga na vrijeme najaviti svoj posjet, osim u slučajevima kada to nije moguće zbog hitne ili krizne situacije ili bi dovelo do situacije u kojoj revizija više ne bi bila djelotvorna.

96. Pri obavljanju revizija u okruženjima s više klijenata treba poduzeti mjere kojima se izbjegavaju ili smanjuju rizici za okruženje nekog drugog klijenta (npr. utjecaj na razinu usluge, dostupnost podataka, povjerljivost).

97. Ako eksternalizacija podrazumijeva visoku razinu tehničke složenosti, na primjer u slučaju eksternalizacije računarstva u oblaku, institucija ili institucija za platni promet trebaju provjeriti ima li subjekt koji provodi reviziju, bez obzira na to radi li se o njezinim unutarnjim revizorima, skupini revizora ili vanjskim revizorima koji djeluju u njezino ime, odgovarajuće i relevantne

[36] Vidjeti i Smjernice EBA-e o procjeni rizika IKT-a: 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

vještine i znanja za djelotvorno izvršavanje relevantnih revizija i/ili procjena. Isto se odnosi na svo osoblje institucije ili institucije za platni promet koje pregledava certifikate trećih strana ili revizije koje su proveli pružatelji usluga.

13.4 Pravo na otkaz

98. Ugovorom o eksternalizaciji treba se izričito omogućiti instituciji ili instituciji za platni promet da otkaže ugovor, u skladu s primjenjivim pravom, uključujući u sljedećim situacijama:

    a. ako pružatelj eksternaliziranih funkcija krši primjenjivo pravo, propise ili ugovorne odredbe;

    b. ako se utvrde prepreke koje bi mogle izmijeniti način obavljanja eksternalizirane funkcije;

    c. ako postoje materijalno značajne promjene koje utječu na eksternalizaciju ili pružatelja usluga (npr. podeksternalizacija ili promjena podizvođača);

    d. ako postoje slabosti u pogledu upravljanja povjerljivim, osobnim ili na drugi način osjetljivim podatcima ili informacijama ili u pogledu njihove sigurnosti; i

    e. ako nadležno tijelo institucije ili institucije za platni promet izda takvu uputu, na primjer ako nadležno tijelo zbog eksternalizacije više nije u mogućnosti učinkovito nadzirati instituciju ili instituciju za platni promet.

99. Ugovorom o eksternalizaciji treba omogućiti prijenos eksternalizirane funkcije na drugog pružatelja usluga ili njezinu ponovnu integraciju u instituciju ili instituciju za platni promet. Zato pisanim ugovorom o eksternalizaciji treba:

    a. jasno utvrditi obveze postojećeg pružatelja usluga u slučaju prijenosa eksternalizirane funkcije na drugog pružatelja usluga ili njezine ponovne integracije u instituciju ili instituciju za platni promet, uključujući obveze u pogledu postupanja s podatcima;

    b. utvrditi prikladno prijelazno razdoblje tijekom kojeg bi pružatelj usluga nakon otkaza ugovora o eksternalizaciji nastavio pružati eksternaliziranu funkciju kako bi se smanjio rizik prekida; i

    c. uključiti obvezu pružatelja usluga da pruži podršku instituciji ili instituciji za platni promet u pravilnom prijenosu funkcije u slučaju otkaza ugovora o eksternalizaciji.

14 Nadzor eksternaliziranih funkcija

100. Institucije i institucije za platni promet trebaju kontinuirano pratiti rad pružatelja usluga kad je riječ o svim ugovorima o eksternalizaciji primjenjujući pristup temeljen na procjeni rizika, pri čemu naglasak treba biti na eksternalizaciji ključnih ili važnih funkcija, uključujući osiguravanje dostupnosti, integriteta i sigurnosti podataka i informacija. Ako su se rizik, priroda

ili veličina eksternalizirane funkcije materijalno značajno promijenili, institucije i institucije za platni promet trebaju ponovno procijeniti ključnost ili važnost te funkcije u skladu s odjeljkom 4.

101. Institucije i institucije za platni promet trebaju postupati s pažnjom dobrog stručnjaka pri praćenju ugovora o eksternalizaciji i upravljanju njima.

102. Institucije trebaju redovito ažurirati svoje procjene rizika u skladu s odjeljkom 12.2. i redovito izvješćivati upravljačko tijelo o rizicima utvrđenima u pogledu eksternalizacije ključnih ili važnih funkcija.

103. Institucije i institucije za platni promet trebaju pratiti svoje unutarnje koncentracijske rizike uzrokovane eksternalizacijom i upravljati njima, uzimajući u obzir odjeljak 12.2. ovih Smjernica.

104. Institucije i institucije za platni promet trebaju kontinuirano osiguravati da eksternalizacije, pri čemu bi naglasak trebao biti na eksternaliziranim ključnim ili važnim funkcijama, zadovoljavaju odgovarajuće standarde u pogledu rada i kvalitete u skladu s njihovim politikama, i to na način da:

a. osiguravaju da im pružatelji usluga dostavljaju odgovarajuća izvješća;

b. ocjenjuju rad pružatelja usluga primjenjujući alate kao što su ključni pokazatelji uspješnosti, ključni pokazatelji kontrole, izvješća o isporuci usluge, samocertificiranje i neovisne provjere; i

c. pregledavaju sve druge relevantne informacije primljene od pružatelja usluge, uključujući izvješća o mjerama za osiguravanje kontinuiteta poslovanja i njihovu testiranju.

105. Institucije trebaju poduzeti odgovarajuće mjere ako utvrde nedostatke u pružanju eksternalizirane funkcije. Konkretno, institucije i institucije za platni promet trebaju reagirati na sve naznake da pružatelji usluga možda ne obavljaju eksternaliziranu ključnu ili važnu funkciju efikasno ili u skladu s primjenjivim zakonima i regulatornim zahtjevima. Ako se utvrde nedostatci, institucije i institucije za platni promet trebaju poduzeti odgovarajuće korektivne mjere. Prema potrebi, te mjere mogu uključivati otkaz ugovora o eksternalizaciji s trenutačnim učinkom.

15 Izlazne strategije

106. Institucije i institucije za platni promet trebaju imati dokumentiranu izlaznu strategiju za eksternalizaciju ključnih ili važnih funkcija, koja je u skladu s njihovom politikom eksternalizacije i planovima kontinuiteta poslovanja[37], uzimajući u obzir najmanje sljedeće mogućnosti:

a. otkaza ugovora o eksternalizaciji;

b. propasti pružatelja usluge;

c. pogoršanja kvalitete eksternalizirane funkcije i stvarnih ili mogućih poremećaja poslovanja uzrokovanih neodgovarajućim ili neuspješnim obavljanjem eksternalizirane funkcije;

d. materijalno značajnih rizika za prikladno i kontinuirano obavljanje funkcije.

107. Institucije i institucije za platni promet trebaju osigurati da mogu otkazati ugovor o eksternalizaciji bez nepotrebnih prekida poslovnih aktivnosti, bez ograničavanja svoje usklađenosti s regulatornim zahtjevima i bez štetnih posljedica za kontinuitet i kvalitetu vlastitog pružanja usluga klijentima. Kako bi to postigle, trebaju:

a. izraditi i provoditi izlazne planove koji su sveobuhvatni, dokumentirani i, prema potrebi, dovoljno testirani (npr. provedbom analize mogućih troškova, učinaka, resursa i vremenskih aspekata prijenosa eksternalizirane funkcije na drugog pružatelja usluge); i

b. utvrditi alternativna rješenja i izraditi prijelazne planove kako bi se instituciji ili instituciji za platni promet omogućilo oduzimanje eksternalizirane funkcije i podataka pružatelju usluge i prijenos drugim pružateljima ili vraćanje u instituciju ili instituciju za platni promet, ili poduzimanje drugih mjera kojima se osigurava kontinuirano obavljanje ključne ili važne funkcije ili poslovne aktivnosti na kontroliran i dobro testiran način, uzimajući u obzir probleme do kojih može doći zbog lokacije podataka te poduzimanja odgovarajućih mjera za osiguravanje kontinuiteta poslovanja tijekom prijelazne faze.

108. Pri izradi izlaznih strategija institucije i institucije za platni promet trebaju:

a. definirati ciljeve izlazne strategije;

b. provesti analizu učinka na poslovanje proporcionalnu riziku eksternaliziranih procesa, usluga ili aktivnosti kako bi se utvrdilo koji su ljudski i financijski resursi potrebni za provedbu izlaznog plana i koliko će vremena za to trebati;

[37] U skladu sa zahtjevima iz članka 85. stavka 2. Direktive 2013/36/EU i glave VI. Smjernica EBA-e o internom upravljanju, institucije i institucije za platni promet trebaju uspostaviti odgovarajuće planove kontinuiteta poslovanja u pogledu eksternaliziranih ključnih ili važnih funkcija.

c. dodijeliti uloge, odgovornosti i dostatne resurse za upravljanje izlaznim planovima i prijenosom aktivnosti;

d. definirati kriterije uspješnosti za prijenos eksternaliziranih funkcija i podataka; i

e. definirati pokazatelje koji će se primijeniti za praćenje ugovora o eksternalizaciji (kako je navedeno u odjeljku 14.), uključujući pokazatelje neprihvatljivih razina usluge koji trebaju potaknuti izlaz.

Glava V. – Smjernice za eksternalizaciju namijenjene nadležnim tijelima

109. Pri utvrđivanju odgovarajućih metoda praćenja usklađenosti institucija i institucija za platni promet s uvjetima inicijalnog odobrenja za rad, nadležna tijela trebaju utvrditi predstavljaju li ugovori o eksternalizaciji materijalno značajnu promjenu uvjeta i obveza iz inicijalnog odobrenja za rad koje je dodijeljeno institucijama i institucijama za platni promet.

110. Nadležna tijela trebaju se uvjeriti da mogu uspješno nadzirati institucije i institucije za platni promet te da su institucije ili institucije za platni promet u svojim ugovorima o eksternalizaciji osigurale da pružatelji usluga moraju nadležnim tijelima i instituciji odobriti pravo na reviziju i pravo pristupa, u skladu s odjeljkom 13.3.

111. Analiza rizika eksternalizacije institucije treba se provoditi barem u okviru postupka nadzorne provjere i ocjene (SREP) ili, kad je riječ o institucijama za platni promet, u okviru drugih nadzornih postupaka, uključujući ad hoc zahtjeve, ili tijekom izravnih nadzora.

112. Osim informacija koje se bilježe u registru, kako je navedeno u odjeljku 11., nadležna tijela mogu od institucija i institucija za platni promet zatražiti i dodatne informacije, posebno kad je riječ o eksternalizaciji ključnih ili važnih funkcija, na primjer:

a. detaljnu analizu rizika;

b. informaciju o tome ima li pružatelj usluga plan kontinuiteta poslovanja koji je primjeren uslugama koje će se pružati instituciji ili instituciji za platni promet koja je zatražila eksternalizaciju;

c. izlaznu strategiju koja se primjenjuje ako bilo koja strana otkaže ugovor o eksternalizaciji ili ako dođe do prekida pružanja usluga; i

d. resurse i mjere uspostavljene za primjereno praćenje eksternaliziranih aktivnosti.

113. Osim informacija koje se zahtijevaju u skladu s odjeljkom 11., nadležna tijela mogu od institucija i institucija za platni promet zatražiti i da dostave detaljne informacije o bilo kojem ugovoru o eksternalizaciji, čak i ako se predmetna funkcija ne smatra ključnom ili važnom.

114. Nadležna tijela trebaju procijeniti sljedeće, u skladu s pristupom temeljenom na procjeni rizika:

a. prate li institucije i institucije za platni promet na odgovarajući način ugovore o eksternalizaciji, posebno one koji se odnose na ključne ili važne funkcije, te upravljaju li njima na odgovarajući način;

b. raspolažu li institucije i institucije za platni promet dostatnim resursima za praćenje ugovora o eksternalizaciji i upravljanje njima;

c. utvrđuju li institucije i institucije za platni promet sve relevantne rizike i upravljaju li njima; i

d. utvrđuju li i procjenjuju institucije i institucije za platni promet na odgovarajući način sukobe interesa u pogledu ugovora o eksternalizaciji, na primjer u slučaju eksternalizacije unutar grupe ili istog institucionalnog sustava zaštite, te upravljaju li njima na odgovarajući način.

115. Nadležna tijela trebaju osigurati da institucije i institucije za platni promet na području EU-a/EGP-a ne djeluju kao „prazne ljušture", među ostalim u situacijama u kojima institucije upotrebljavaju naizmjenične transakcije (back-to-back transakcije) ili transakcije unutar grupe za prijenos dijela tržišnog rizika ili kreditnog rizika na subjekt izvan EU-a/EGP-a, te trebaju osigurati da te institucije raspolažu odgovarajućim mehanizmima upravljanja i mehanizmima za upravljanje rizicima potrebnima za utvrđivanje rizika i upravljanje njima.

116. U okviru svoje procjene, nadležna tijela trebala bi uzeti u obzir sve rizike, a posebno[38]:

a. operativne rizike[39] koji proizlaze iz ugovora o eksternalizaciji;

b. reputacijske rizike;

c. rizik „step-in" zbog kojeg će institucija možda morati spašavati pružatelja usluge, u slučaju značajnih institucija;

d. koncentracijske rizike unutar institucije, uključujući na konsolidiranoj osnovi, uzrokovane većim brojem ugovora o eksternalizaciji s istim pružateljem usluga ili usko povezanim pružateljima usluga ili većim brojem ugovora o eksternalizaciji unutar istog poslovnog područja;

e. koncentracijske rizike na razini sektora, na primjer ako više institucija ili institucija za platni promet koristi istog pružatelja usluga ili malu skupinu pružatelja usluga;

---

[38] Za institucije na koje se primjenjuje Direktiva 2013/36/EU vidjeti i Smjernice EBA-e o SREP-u: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Vidjeti i Smjernice EBA-e o riziku IKT-a: 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

f. mjeru u kojoj institucija ili institucija za platni promet koja zahtijeva eksternalizaciju kontrolira pružatelja usluga ili može utjecati na njegovo djelovanje, smanjenje rizika do kojeg može doći zbog veće razine kontrole, te je li pružatelj usluge uključen u konsolidirani nadzor grupe;

g. sukobe interesa između institucije i pružatelja usluga.

117. Ako se utvrde koncentracijski rizici, nadležna tijela trebaju pratiti kretanje tih rizika i ocijeniti njihov moguć utjecaj na druge institucije i institucije za platni promet te na stabilnost financijskog tržišta; nadležna tijela trebaju obavijestiti sanacijsko tijelo, kad je to potrebno, o novim potencijalno ključnim funkcijama[40] utvrđenima tijekom te procjene.

118. Ako se utvrde razlozi za zabrinutost iz kojih se može zaključiti da određena institucija ili institucija za platni promet više ne raspolaže pouzdanim sustavima upravljanja ili nije usklađena s regulatornim zahtjevima, nadležna tijela trebaju poduzeti odgovarajuće mjere koje mogu uključivati ograničavanje obujma eksternaliziranih funkcija ili zahtjev za izlazak iz jednog ugovora o eksternalizaciji ili više njih. Konkretno, uzimajući u obzir potrebu da institucija ili institucija za platni promet kontinuirano posluje, može se zatražiti raskid ugovora ako se nadzor i ispunjenje regulatornih zahtjeva ne mogu osigurati drugim mjerama.

119. Nadležna tijela trebaju se uvjeriti da mogu uspješno provoditi nadzor, posebno kad institucije i institucije za platni promet eksternaliziraju ključne ili važne funkcije izvan EU-a/EGP-a.

[40] Kako je definirano u članku 2. stavku 1. točki (35) Direktive o oporavku i sanaciji banaka.