



Laidiens: **30.12.2016., Nr. 255**

Oficiālās publikācijas Nr.: **2016/255.6**

Finanšu un kapitāla tirgus komisijas normatīvie noteikumi Nr. 219

Rīgā 2016. gada 28. decembrī

(Finanšu un kapitāla tirgus komisijas padomes
sēdes protokols Nr. 45 3. p.)

Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas riska pārvaldības informācijas tehnoloģiju nodrošinājuma normatīvie noteikumi

*Izdoti saskaņā ar
Noziedzīgi iegūtu līdzekļu legalizācijas un
terorisma finansēšanas novēršanas likuma
47. panta otrās daļas 5. punktu*

1. Vispārīgie jautājumi

1. "Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas riska pārvaldības informācijas tehnoloģiju nodrošinājuma normatīvie noteikumi" (turpmāk – noteikumi) nosaka noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas (turpmāk – NILLTF) riska pārvaldības informācijas tehnoloģiju (turpmāk – IT) nodrošinājuma minimālās prasības kredītiestādēm un dalībvalstu un trešo valstu kredītiestāžu filiālēm (turpmāk – kredītiestāde). Kredītiestādes ievēro šo noteikumu prasības individuāli un konsolidācijas grupas vai konsolidācijas apakšgrupas līmenī, nodrošinot konsolidācijas grupā vai apakšgrupā, kā arī ikvienā meitas sabiedrībā šo noteikumu prasībām atbilstošas NILLTF riska pārvaldības IT.

2. Noteikumos lietoti šādi termini:

2.1. IT sistēma – datu ievades, uzglabāšanas un apstrādes sistēma vai šādu sistēmu kopums, kas nodrošina noteikto NILLTF riska pārvaldības funkciju izpildi un paredz IT sistēmas lietotājiem pieeju tajā glabātajiem datiem un informācijai;

2.2. IT sistēmas parametrs – IT sistēmas ietvaros lietojamais mainīgais lielums, kuram katrā konkrētā gadījumā piešķir noteiktu vērtību;

2.3. IT sistēmas lietotājs – kredītiestādes darbinieks, kurš piešķirto pilnvaru robežās veic darbības IT sistēmā;

2.4. klienta riska profils – termins lietots Finanšu un kapitāla tirgus komisijas 2015. gada 23. decembra normatīvo noteikumu Nr. 234 "Klientu padziļinātās izpētes normatīvie noteikumi kredītiestādēm un licencētām maksājumu un elektroniskās naudas iestādēm" (turpmāk – noteikumi Nr. 234) izpratnē;

2.5. klienta riska skaitliskā novērtējuma (*scoring*) sistēma – termins lietots noteikumu Nr. 234 izpratnē;

2.6. NILLTF risks – termins lietots Finanšu un kapitāla tirgus komisijas 2016. gada 23. septembra normatīvo noteikumu Nr. 154 "Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas riska pārvaldīšanas normatīvie noteikumi" (turpmāk – noteikumi Nr. 154) izpratnē;

2.7. NILLTF riska ekspozīcija – termins lietots noteikumu Nr. 154 izpratnē;

2.8. riska faktori jeb risku paaugstinošie faktori – termins lietots noteikumu Nr. 234 izpratnē;

2.9. riska segmenti – termins lietots noteikumu Nr. 234 izpratnē;

2.10. "snaudošais" konts – konts, kas atbilst vismaz vienai no šādām pazīmēm:

2.10.1. pirmais kredīta darījums kontā tiek veikts ne agrāk kā sešus mēnešus pēc dienas, kad sāktas darījuma attiecības ar klientu, un mēneša kredīta apgrozījums ir sasniedzis 70 000 *euro* ekvivalentu;

2.10.2. pirmais izejošais maksājums no konta tiek veikts ne agrāk kā 12 mēnešus pēc konta atvēršanas dienas;

2.10.3. klienta darījumi kontā tiek atsākti pēc vismaz sešu mēnešu pārtraukuma, un pirmajā darījumu atsākšanas mēnesī debeta vai kredīta apgrozījums ir sasniedzis 70 000 *euro* ekvivalentu;

2.11. sankciju saraksti – personu, teritoriju, pakalpojumu vai citu objektu, pret kuriem starptautiskā organizācija vai valsts ir noteikusi sankcijas (ierobežojumus), kuras ir piemērojamas Latvijā vai kuras kredītiestāde ir noteikusi par saistošām, saraksti;

2.12. speciālie saraksti – kredītiestādes uzturētie iekšējie klientu un potenciālo klientu, to patieso labuma guvēju un pilnvaroto pārstāvju, par kuriem ir pieejama negatīva informācija saistībā ar iesaistišanos NILLTF, tajā skaitā personu, ar kurām Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likumā noteiktajā kārtībā nav uzsāktas vai ir izbeigtas darījuma attiecības, saraksti.

3. Noteikumu mērķis ir nodrošināt efektīvas, kredītiestādes saimnieciskās darbības apmēram un raksturam, kā arī kredītiestādes NILLTF riska ekspozīcijai atbilstošas IT sistēmas izmantošanu kredītiestādes NILLTF riska pārvaldībai.

4. Kredītiestāde atbilstoši NILLTF riska ekspozīcijai nodrošina nepieciešamos IT risinājumus efektīvai NILLTF riska pārvaldībai, veicot savlaicīgu, precīzu un pilnīgu NILLTF riska identifikāciju, to raksturojošās informācijas apstrādi un rezultātu izvērtēšanu, kā arī vadības atskaišu sagatavošanu.

5. Kredītiestāde regulāri, bet ne retāk kā reizi 18 mēnešos, pamatojoties uz aktuālo kredītiestādes NILLTF riska ekspozīciju, NILLTF riska kontroles funkcijas efektivitātes vērtējumu un ievērojot šo noteikumu 17. punktā minētā audita rezultātus, izvērtē IT sistēmas efektivitāti un atbilstību kredītiestādes aktuālajai NILLTF riska ekspozīcijai. Kredītiestāde nodrošina, ka, palielinoties kredītiestādes NILLTF riska ekspozīcijai, tiek savlaicīgi nodrošināta IT sistēmas atbilstība aktuālajai situācijai.

6. Kredītiestādes valde vai filiāles vadītājs, kas rīkojas piešķirto pilnvaru ietvaros, pieņem lēmumu par IT sistēmas ieviešanu kredītiestādē, kā arī nepieciešamības gadījumā apstiprina būtiskas izmaiņas IT sistēmā. Valdes loceklis, kurš ir atbildīgs par NILLTF novēršanu kredītiestādē, vai filiāles vadītājs regulāri informē kredītiestādes valdi par IT sistēmas darbības efektivitāti.

7. Kredītiestādes padomei, valdei, tās komitejām, struktūrvienību vadītājiem un atbildīgajiem darbiniekiem regulāri vai pēc pieprasījuma ir pieejama pilnīga, precīza, savlaicīga un pietiekama IT sistēmas nodrošinātā informācija, kas nepieciešama to amata pienākumu izpildei un lēmumu pieņemšanai.

2. NILLTF riska pārvaldības IT sistēmas prasības

2.1. IT sistēmas ieviešanas un pilnveidošanas prasības

8. Kredītiestāde, ieviešot IT sistēmu, nodrošina izstrādes un ieviešanas procesa, tajā skaitā izmantojamās informācijas un datu, drošumu atbilstoši normatīvo aktu informācijas sistēmu drošības jomā prasībām.

9. Kredītiestāde izvērtē tai pieejamos personāla, tehnoloģiskos un citus resursus, kas nepieciešami efektīvai NILLTF riska pārvaldībai, un pieņem lēmumu par IT sistēmas ieviešanu vienā no šādiem veidiem:

9.1. kredītiestāde iegādājas un ievieš specializētu IT sistēmu;

9.2. kredītiestāde izstrādā IT sistēmu, izmantojot kredītiestādes vai tās grupas uzņēmuma iekšējos resursus;

9.3. kredītiestāde izstrādā IT sistēmu, izmantojot ārpalpojumu.

10. Kredītiestāde, ieviešot IT sistēmu, nodrošina šādu prasību izpildi:

10.1. kredītiestāde pārlicinās, ka šo noteikumu 9.3. punktā minētajam ārpalpojuma sniedzējam ir dokumentāri pierādāma pieredze un zināšanas NILLTF riska pārvaldības IT sistēmu izstrādē un ieviešanā;

10.2. IT sistēmas parametri atbilst normatīvo aktu NILLTF novēršanas jomā prasībām, kredītiestādes NILLTF riska ekspozīcijai un saimnieciskās darbības modelim, kā arī labākajai starptautiskajai praksei NILLTF riska pārvaldības IT nodrošinājuma jomā;

10.3. IT sistēmas funkcijas aptver visus kredītiestādei raksturīgos NILLTF riska segmentus, t.sk. kredītiestādes sniegtos pakalpojumus un klientu kontus, kā arī visus darījumus, kuri tiek veikti klienta interesēs vai pēc klienta rīkojuma.

2.2. IT sistēmas funkcionālās prasības

11. IT sistēmas ietvaros tiek nodrošināta izmantojamās informācijas un datu integritāte, aktualitāte un precizitāte.

12. IT sistēmas ietvaros tiek automatizēti sagatavoti brīdinājuma ziņojumi. IT sistēmas sagatavotie brīdinājuma ziņojumi ir pieejami atbilstoši pilnvarotiem IT sistēmas lietotājiem izvērtēšanai un lēmuma pieņemšanai.

13. IT sistēmas ietvaros tiek nodrošināta IT sistēmas lietotāju pieejas un pilnvarojuma sistēmas uzturēšana klienta riska profila novērtēšanai, darījumu uzraudzībai un ar tiem saistīto risku izvērtēšanai, skaidri nosakot IT sistēmas lietotājiem atļautās darbības atbilstoši kredītiestādes darbinieku veicamajām funkcijām un pilnvarojuma līmeņiem, tajā skaitā nodrošinot ierobežojumus attiecībā uz darbinieku tiesībām veikt klienta riska profila un klientam noteikto ierobežojumu informācijas izmaiņas.

14. IT sistēmas lietotājiem atbilstoši pilnvarojuma līmenim ir iespēja veikt visas nepieciešamās darbības IT sistēmas ietvaros, lai efektīvi pārvaldītu NILLTF risku, tajā skaitā:

14.1. iespēja noteikt papildu parametrus darījumu uzraudzībai, aizdomīgu un neparastu darījumu pazīmju identifikācijai un brīdinājumiem par izmaiņām klientu riska profilā (piemēram, robežvērtības, darījumu skaits u.tml.) vai veikt citas līdzīgas darbības;

14.2. iespēja centralizēti iegūt sistematizētu informāciju par risku paaugstinošajiem faktoriem;

14.3. iespēja klasificēt klientus pēc riska skaitliskā novērtējuma un klienta riska tipa;

14.4. iespēja apstrādāt IT sistēmas sagatavotos brīdinājuma ziņojumus, izmantojot kredītiestādes rīcībā esošo klientu un darījumu informāciju, kas var ietekmēt NILLTF risku;

14.5. iespēja noteikt papildu prasības obligāto informācijas lauku (turpmāk – obligātie lauki) aizpildīšanai.

15. IT sistēmas lietotāju veikto darbību, tajā skaitā saistībā ar saņemto brīdinājuma ziņojumu apstrādi, auditācijas pieraksti tiek glabāti sešus gadus pēc attiecīgās darbības veikšanas.

16. IT sistēmas ietvaros tiek nodrošinātas vismaz šādas NILLTF riska pārvaldības funkcijas:

16.1. kredītiestādes klientu informācijas apstrāde, nodrošinot:

16.1.1. automatizētu kontroli pār klienta, tā patiesā labuma guvēja, pilnvarotā pārstāvja un citas klienta identifikācijai un saimnieciskās un personiskās darbības pārzināšanai nepieciešamās informācijas obligāto lauku aizpildīšanu;

16.1.2. automatizētu ievadītās informācijas par klientu, tā patieso labuma guvēju un pilnvaroto pārstāvi pārbaudi attiecībā pret speciālajiem sarakstiem;

16.1.3. automatizētu aizliegumu klienta konta atvēršanai pirms obligāto lauku aizpildīšanas;

16.1.4. ievadītās informācijas pareizības pārbaudi (piemēram, dzimšanas gada skaitļa vērtības kontrole, rezidences valsts esamības kontrole u.tml.);

16.1.5. ievadītās informācijas automatizētu pārbaudi, nodrošinot brīdinājuma ziņojumu sagatavošanu sakritības gadījumā, attiecībā pret:

16.1.5.1. kredītiestādes speciālajiem sarakstiem vai sankciju sarakstiem, tostarp gadījumā, ja sadarbības laikā klientam mainās patiesais labuma guvējs vai pilnvarotais pārstāvis,

16.1.5.2. kredītiestādes informācijas sistēmā glabāto sadarbības ar klientu vēstures informāciju;

16.1.6. klienta identifikācijas un izpētes procesā iegūtās informācijas glabāšanu elektroniskā formā un pieejamību klienta izpētei sadarbības laikā;

16.1.7. automatizētu brīdinājuma ziņojumu sagatavošanu par klienta un tā pilnvarotās personas identifikācijas dokumentu vai pilnvaras derīguma termiņa beigām un atbilstošu ierobežojumu piemērošanu attiecībā uz klienta darījumiem pēc minēto dokumentu derīguma termiņa beigām;

16.2. klienta riska klasifikācija un riska skaitliskā novērtējuma (*scoring*) sistēmas uzturēšana un lietošana, nodrošinot:

16.2.1. automatizētu klienta riska faktoru novērtējumu, riska tipa noteikšanu un atbilstoša skaitliskā novērtējuma piešķiršanu;

16.2.2. automatizētu klienta riska profilam piemērojamo robežvērtību sistēmas uzturēšanu un lietošanu klienta darbības uzraudzībai (piemēram, klienta tips, rezidence, plānotais vai esošais darījumu apmērs, politiski nozīmīgas personas, tās ģimenes loceklis vai ar politiski nozīmīgu personu cieši saistītas personas statuss, plānoto vai izmantojamo pakalpojumu veids, normatīvajos aktos klientu padziļinātās izpētes un pastiprinātās uzraudzības jomā noteiktie kritēriji u.tml.);

16.2.3. automatizētu tādu klientu identificēšanu, kuriem jāveic padziļinātā izpēte gadījumos, kad klients veido saistīto klientu grupu ar klientu, kura riska skaitliskais novērtējums sasniedz kredītiestādes noteikto robežlīmeni, pēc kura sasniegšanas klientam tiek piemēroti padziļinātās izpētes pasākumi pirms sadarbības uzsākšanas un sadarbības laikā;