EBA/GL/2022/15

22.11.2022.

Pamatnostādnes

par klientu attālinātas piesaistīšanas risinājumu izmantošanu saskaņā ar Direktīvas (ES) 2015/849 13. panta 1. punktu

1. Atbilstība un ziņošanas prasības

Šo pamatnostādņu statuss

1. Šajā dokumentā ir iekļautas pamatnostādnes, kas izdotas saskaņā ar Regulas (ES) Nr. 1093/2010[1] 16. pantu. Kompetentajām iestādēm un finanšu iestādēm saskaņā ar Regulas (ES) Nr. 1093/2010 16. panta 3. punktu jādara viss iespējamais, lai ievērotu šīs pamatnostādnes.

2. Pamatnostādnēs ir izklāstīts EBI skatījums uz uzraudzības pieeju Eiropas finanšu uzraudzības sistēmā vai par to, kā konkrētā jomā ir jāpiemēro Savienības tiesību akti. Kompetentajām iestādēm, kas minētas Regulas (ES) Nr. 1093/2010 4. panta 2. punktā un uz kurām šīs pamatnostādnes attiecas, tās jāiekļauj to praksē (piemēram, veicot grozījumus savā tiesiskajā regulējumā vai savos uzraudzības procesos), tostarp gadījumos, kad pamatnostādnes ir paredzētas galvenokārt iestādēm.

Ziņošanas prasības

3. Saskaņā ar Regulas (ES) Nr. 1093/2010 16. panta 3. punktu kompetentajām iestādēm līdz 30.05.2023 jāpaziņo EBI, vai tās ievēro vai plāno ievērot šīs pamatnostādnes, vai pretējā gadījumā ir jānorāda to neievērošanas iemesli. Ja attiecīgajā termiņā šāds paziņojums nebūs saņemts, EBI uzskatīs, ka kompetentās iestādes neievēro šīs pamatnostādnes. Paziņojumi jānosūta, iesniedzot EBI tīmekļa vietnē pieejamo veidlapu ar norādi "EBA/GL/2022/15". Personām, kas iesniedz paziņojumus, ir jābūt pilnvarotām pārstāvēto kompetento iestāžu vārdā ziņot par prasību izpildi. Par jebkurām izmaiņām atbilstības statusā arī ir jāziņo EBI.

4. Paziņojumi tiks publicēti EBI tīmekļa vietnē saskaņā ar 16. panta 3. punktu.

[1] Eiropas Parlamenta un Padomes 2010. gada 24. novembra Regula (ES) Nr. 1093/2010, ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK (OV L 331, 15.12.2010., 12. lpp.).

2. Priekšmets, piemērošanas joma un definīcijas

Priekšmets un piemērošanas joma

5. Šajās pamatnostādnēs ir izklāstītas darbības, kas kredītiestādēm un finanšu iestādēm jāveic, pieņemot vai pārskatot risinājumus, kurus tās piemēro, lai izpildītu pienākumus, kas Direktīvas (ES) 2015/849[2] 13. panta 1. punkta a), b) un c) apakšpunktā paredzēti attiecībā uz klientu attālinātu piesaistīšanu. Pamatnostādnēs ir izklāstītas arī darbības, kas saskaņā ar Direktīvas (ES) 2015/849 I nodaļas 4. iedaļu kredītiestādēm un finanšu iestādēm jāveic, iesaistot trešās personas, kā arī politikas nostādnes, kontroles pasākumi un procedūras, kas kredītiestādēm un finanšu iestādēm jāievieš saistībā ar klienta uzticamības pārbaudi (KUP), kā minēts Direktīvas (ES) 2015/849 8. panta 3. punktā un 4. punkta a) apakšpunktā, gadījumos, kad KUP pasākumus veic attālināti.

6. Kompetentajām iestādēm, novērtējot, vai darbības, ko finanšu iestādes un kredītiestādes veic, lai izpildītu pienākumus, kas saskaņā ar Direktīvu (ES) 2015/849 jāveic klientu attālinātas piesaistīšanas gadījumos, ir atbilstošas un efektīvas, jāņem vērā šīs pamatnostādnes.

Adresāti

7. Šīs pamatnostādnes attiecas uz Regulas (ES) Nr. 1093/2010 4. panta 2. apakšpunktā definētajām kompetentajām iestādēm. Šīs pamatnostādnes attiecas arī uz finanšu sektora dalībniekiem, kā definēts minētās regulas 4. panta 1.a punktā, kuri ir kredītiestādes un finanšu iestādes, kā definēts Direktīvas (ES) 2015/849 3. panta 1. un 2. punktā.

[2] Eiropas Parlamenta un Padomes 2015. gada 20. maija Direktīva (ES) 2015/849 par to, lai nepieļautu finanšu sistēmas izmantošanu nelikumīgi iegūtu līdzekļu legalizēšanai un teroristu finansēšanai

Definīcijas

8. Ja nav norādīts citādi, terminiem, kas lietoti un definēti Direktīvā (ES) 2015/849, ir tāda pati nozīme arī pamatnostādnēs. Papildus šajās pamatnostādnēs tiek piemērotas tālāk minētā definīcija.

Biometriskie dati	Personas dati saistībā ar fiziskas personas fiziskajām, psiholoģiskajām vai uzvedības pazīmēm, kas ļauj apstiprināt vai apstiprina šīs fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopijas dati, un kas iegūti un apstrādāti, izmantojot tehniskus līdzekļus.

3. Īstenošana

Piemērošanas datums

Šīs pamatnostādnes tiek piemērotas, sākot no 02.10.2023.

4. Pamatnostādnes par attālinātas klientu piesaistīšanas risinājumu izmantošanu saskaņā ar Direktīvas (ES) 2015/849 13. panta 1. punktu

4.1 Iekšējā politika un procedūras

4.1.1 Politika un procedūras saistībā ar klientu attālinātu piesaistīšanu

9. Kredītiestādēm un finanšu iestādēm ir jāievieš un jāievēro politika un procedūras, lai situācijās, kad klientu piesaistīšana notiek attālināti, izpildītu pienākumus, kas tām noteikti Direktīvas (ES) 2015/849 13. panta 1. punkta a) un c) apakšpunktā. Izstrādājot šīs politikas nostādnes un procedūras, jāņem vērā riska pakāpe un tajās jāiekļauj vismaz:

    a) vispārīgi aprakstīts risinājums, ko kredītiestādes un finanšu iestādes ir ieviesušas, lai klientu attālinātas piesaistīšanas procesā iegūtu, pārbaudītu un ierakstītu informāciju. Tajā ir jāiekļauj skaidrojums par risinājuma īpatnībām un darbību;

    b) situācijas, kurās var izmantot klientu attālinātas piesaistīšanas risinājumu, ņemot vērā riska faktorus, kas apzināti un novērtēti saskaņā ar Direktīvas (ES) 2015/849 8. panta 1. punktu un veicot uzņēmējdarbības riska novērtējumu, iekļaujot attālinātai piesaistīšanai atbilstošas klientu kategorijas, produktus un pakalpojumus;

    c) darbības, kuras ir pilnībā automatizētas, un darbības, kurās vajadzīga cilvēka iejaukšanās;

    d) kontroles pasākumi, kas ieviesti, lai nodrošinātu, ka pirmais darījums ar jaunu piesaistīto klientu tiek izpildīts tikai pēc tam, kad ir piemēroti visi sākotnējās klienta uzticamības pārbaudes (KUP) pasākumi;

    e) instruktāžas un regulāro apmācības programmu apraksts, lai nodrošinātu darbinieku informētību un jaunākās zināšanas par klientu attālinātas piesaistīšanas risinājumiem, ar to saistītajiem riskiem un klientu attālinātas piesaistīšanas politikas nostādnēm un procedūrām, kuru mērķis ir šādu risku mazināšana.

10. Ieviestajās politikas nostādnēs un procedūrās ir jānodrošina kredītiestāžu un finanšu iestāžu atbilstībai šo pamatnostādņu 4.2.–4.7. sadaļā minētajām prasībām.

4.1.2 Pārvaldība

11. Papildus noteikumiem, kas izklāstīti EBI Pamatnostādņu par atbilstības amatpersonām [3] 4.2.4. sadaļā, NILL/TFN atbilstības amatpersonai [4], pildot vispārējo pienākumu sagatavot politiku un procedūras, lai izpildītu KUP prasības, ir jānodrošina, ka attālinātas klientu piesaistīšanas politikas nostādnes un procedūras tiek ieviestas faktiski, tiek regulāri pārskatītas un vajadzības gadījumā grozītas.

12. Kredītiestādes un finanšu iestādes vadības struktūrai jāapstiprina attālinātas klientu piesaistīšanas politika un procedūras un jāpārrauga to pareiza īstenošana.

4.1.3 Attālinātas klientu piesaistīšanas risinājuma pirmsīstenošanas novērtējums

13. Apsverot, vai ir jāpieņem jauns attālinātas klientu piesaistīšanas risinājums, kredītiestādēm un finanšu iestādēm jāveic klientu attālinātas piesaistīšanas risinājuma pirmsīstenošanas novērtējums.

14. Kredītiestādēm un finanšu iestādēm savā politikā un procedūrās jānosaka pirmsīstenošanas novērtējuma piemērošanas joma, posmi un uzskaites prasības, iekļaujot vismaz:

    a) novērtējumu par risinājuma atbilstību attiecībā uz iegūstamo datu un dokumentu pilnīgumu un precizitāti, kā arī tajā izmantoto informācijas avotu ticamību un neatkarību;

    b) novērtējumu par klientu attālinātas piesaistīšanas risinājuma izmantošanu attiecībā uz tā uzņēmējdarbības riskiem, tostarp nelikumīgi iegūtu līdzekļu legalizēšanas / teroristu finansēšanas riskiem;

    c) iespējamos apzinātos risku mazināšanas pasākumus un korektīvos pasākumus attiecībā uz katru risku, kas identificēts, veicot b) apakšpunktā minēto novērtējumu;

    d) testus, ar kuriem novērtē krāpšanas riskus, tostarp krāpniecības riskus saistībā ar identitātes zaudēšanu un citus informācijas un komunikācijas tehnoloģijas (“IKT”) un drošības riskus saskaņā ar 43. noteikumu EBI pamatnostādnēs par IKT un drošības risku pārvaldību[5];

    e) klientu attālinātas piesaistīšanas politikā un procedūrās identificētajiem klientiem, produktiem un pakalpojumiem paredzētā risinājuma darbības pilnīgu testēšanu.

15. Kredītiestādēm un finanšu iestādēm jāuzskata, ka 14. punkta a), d) un e) apakšpunktā minētie kritēriji ir izpildīti, ja risinājumā izmanto vienu no šādiem elementiem:

[3] Pamatnostādnes par politiku un procedūrām saistībā ar atbilstības pārvaldību un NILL/TFN atbilstības amatpersonas lomu un uzdevumiem saskaņā ar Direktīvas (ES) 2015/849 8. pantu un VI nodaļu.

[4] Saskaņā ar proporcionalitātes kritēriju, kas noteikts Pamatnostādņu par atbilstības amatpersonām 4.2.2. iedaļā.

[5] EBA/GL/2019/04

a) elektroniskās identifikācijas shēmas, kas paziņotas saskaņā ar Regulas (EK) Nr. 910/2014 9. pantu un kas atbilst uzticamības līmeņiem "būtisks" vai "augsts", kā definēts minētās regulas 8. pantā;

b) attiecīgus kvalificētus uzticamības pakalpojumus, kas atbilst prasībām, kuras noteiktas Regulā (EK) Nr. 910/2014, jo īpaši tās III nodaļas 3. iedaļā un 24. panta 1. punkta 2. daļas b) apakšpunktā.

16. Kredītiestādēm un finanšu iestādēm jāspēj savai kompetentajai iestādei pierādīt, kādus novērtējumus tās veikušas pirms klientu attālinātas piesaistīšanas risinājuma ieviešanas, sava novērtējuma rezultātus un to, kā tas ir piemērots, ņemot vērā NIIL/TF riskus, kas risinājuma darbības jomā identificēti attiecībā uz klientu, pakalpojumu, ģeogrāfiju un produktu veidiem.

17. Kredītiestādēm un finanšu iestādēm klientu attālinātas piesaistīšanas risinājums jāsāk izmantot tikai pēc tam, kad tās ir pārliecinājušās, ka to var iekļaut plašākā iestādes iekšējas kontroles sistēmā, tādējādi nodrošinot iestādei iespēju pienācīgi pārvaldīt NIIL/TF riskus, kas varētu rasties, izmantojot klientu attālinātas piesaistīšanas risinājumu.

4.1.4 Klientu attālinātas piesaistīšanas risinājuma pastāvīga uzraudzība

18. Kredītiestādēm un finanšu iestādēm pastāvīgi jāuzrauga klientu attālinātas piesaistīšanas risinājums, lai nodrošinātu, ka tas darbojas atbilstoši kredītiestāžu un finanšu iestāžu vēlmēm. Kredītiestādēm un finanšu iestādēm ir jāpapildina pamatnostādņu 9. punktā minētās politikas nostādnes un procedūras, iekļaujot tajās vismaz:

a) darbības, ko tās veiks, lai pastāvīgi nodrošinātu kvalitāti, pilnīgumu, precizitāti un atbilstību datiem, kas iegūti attālinātas klientu piesaistīšanas procesā, kam jābūt saderīgam ar NIIL/TF riskiem, kuriem kredītiestāde un finanšu iestāde ir pakļauta;

b) regulāras pārskatīšanas tvērumu un biežumu; un

c) apstākļus, saistībā ar kuriem jāveic *ad hoc* pārskatīšana, iekļaujot vismaz šādus elementus:

a. kredītiestāžu un finanšu iestāžu NIIL/TF risku ekspozīcijas izmaiņas;

b. risinājuma darbības nepilnības, kas atklātas, veicot uzraudzības, revīzijas vai pārraudzības darbības;

c. ievērojamu krāpšanas mēģinājumu pieaugumu;

d. normatīvo aktu un tiesiskā regulējuma izmaiņas.

19. Kredītiestādēm un finanšu iestādēm savās procedūrās un procesos ir jānosaka novēršanas pasākumi gadījumiem, kad risks ir īstenojies vai ir atklātas kļūdas, kas ietekmē vispārējā

klientu attālinātas piesaistīšanas risinājuma efektivitāti un lietderību. Šajos pasākumos jāiekļauj vismaz:

a) visu attiecīgu darījumu attiecību pārskatīšana, lai novērtētu, vai kredītiestādes un finanšu iestādes ir veikušas pietiekamu sākotnējo klienta uzticamības pārbaudi, lai izpildītu prasības, kas noteiktas Direktīvas (ES) 2015/849 13. panta 1. punkta a), b) un c) apakšpunktā. Kredītiestādēm un finanšu iestādēm jānosaka prioritāte tām darījumu attiecībām, kas ietver visaugstāko NIIL/TF risku;

b) ņemot vērā minētajā pārskatīšanā iegūto informāciju – novērtējums par to, vai:

   a. attiecīgajām darījumu attiecībām jāpiemēro papildu izpētes pasākumi;

   b. attiecīgajām darījumu attiecībām jāpiemēro ierobežojumi, piemēram, darījumu apjoma ierobežojumi, ja tas ir atļauts valsts tiesību aktos, līdz brīdim, kad ir notikusi pārskatīšana;

   c. attiecīgās darījumu attiecības ir jāizbeidz;

   d. par attiecīgajām darījumu attiecībām jāziņo *FIU*;

   e. ir jāmaina attiecīgo darījumu attiecību riska kategorija.

20. Kredītiestādēm un finanšu iestādēm jāapsver, kā visefektīvāk iespējams uzraudzīt klientu attālināto piesaistīšanas risinājumu pastāvīgu atbilstību un ticamību. Tām jāapsver iespēja, ka tiek izmantots viens vai vairāki šādi līdzekļi:

   i. kvalitātes nodrošināšanas testēšana;

   ii. automatizēti svarīgi brīdinājumi un paziņojumi;

   iii. regulāri automatizēti kvalitātes ziņojumi;

   iv. izlases pārbaudes;

   v. manuāla pārskatīšana.

21. Šī sadaļa attiecas arī uz gadījumiem, kad izmanto pilnīgi automatizētus klientu attālinātas piesaistīšanas risinājumus, kas lielā mērā ir atkarīgi no automatizētiem algoritmiem bez cilvēka iejaukšanās vai ar niecīgu cilvēka iejaukšanos.

22. Kredītiestādēm un finanšu iestādēm jāspēj savai kompetentajai iestādei pierādīt, kādu pārskatīšanu tās ir veikušas un kādi riska mazināšanas pasākumi ir veikti, lai novērstu visas nepilnības, kas apzinātas visā klientu attālinātas piesaistīšanas risinājumu izmantošanas darbības laikā.

4.2 Informācijas iegūšana;

4.2.1 Klienta identifikācija

23. Papildus darbībām, kas izklāstītas 9. punktā, kredītiestādēm un finanšu iestādēm savās politikas nostādnēs un procedūrās jānosaka informācija, kas ir nepieciešama, lai identificētu klientu, identifikācijas dokumentu veidi, dati vai informācija, ko iestāde izmantos, lai pārbaudītu klienta identitāti, un veids, kā šī informācija tiks pārbaudīta.

24. Kredītiestādēm un finanšu iestādēm jānodrošina, ka:

    a) informācija, kas iegūta, izmantojot klientu attālinātas piesaistīšanas risinājumu, ir aktuāla un atbilst piemērojamiem sākotnējās klienta izpētes juridiskajiem un normatīvajos aktos noteiktajiem standartiem;

    b) visi attēli, videomateriāli, skaņas ieraksti un dati tiek ierakstīti lasāmā formātā un pietiekamā kvalitātē, lai klients ir nepārprotami identificējams;

    c) konstatējot tehniskas nepilnības vai neparedzētus savienojuma pārtraukumus, klienta identifikācijas process netiek turpināts.

25. Kredītiestādēm vai finanšu iestādēm jāuzskata, ka 24. punktā minētie kritēriji ir izpildīti, ja risinājumā izmanto vienu no šādiem elementiem:

    a) elektroniskās identifikācijas shēmas, par kurām paziņo saskaņā ar Regulas (EK) Nr. 910/2014 9. pantu un kas atbilst uzticamības līmeņiem “būtisks” vai “augsts”, kā definēts minētās regulas 8. pantā;

    b) attiecīgus kvalitatīvus uzticamus pakalpojumus, kas atbilst prasībām, kuras noteiktas Regulā (EK) Nr. 910/2014, jo īpaši tās III nodaļas 3. iedaļā un 24. panta 1. punkta 2. daļas b) apakšpunktā.

26. Dokumenti un informācija, kas iegūti attālinātas identifikācijas procesā un kas jāuzglabā atbilstoši Direktīvas (ES) 2015/849 40. panta 1. punkta a) apakšpunktam, kredītiestādei un finanšu iestādei jāapzīmogo ar laika zīmogu un jāuzglabā drošībā. Uzglabāto failu, tostarp attēlu, videomateriālu, skaņas ierakstu un datu, ierakstu saturam jābūt pieejamam lasāmā formātā un jānodrošina iespēja veikt *ex post* pārbaudes.

4.2.2 Fizisku personu identifikācija

27. Atbilstoši pamatnostādņu 4.1.1. sadaļas 9. punktam kredītiestādēm un finanšu iestādēm savās politikas nostādnēs jānosaka informācija, kas jāiegūst, lai attālināti identificētu klientus saskaņā ar Direktīvas (ES) 2015/849 13. panta 1. punkta a) un c) apakšpunktu. Kredītiestādēm un finanšu iestādēm arī jānosaka, kādu informāciju:

    a) manuāli ievada klients;

b) automātiski iegūst no klienta iesniegtajiem dokumentiem;

c) iegūst, izmantojot citus iekšējus vai ārējus informācijas avotus.

28. Kredītiestādēm un finanšu iestādēm jāievieš un jāuztur pienācīgi mehānismi, kas nodrošina, ka informācija, ko tās iegūst automātiski saskaņā ar 27. punktu, ir ticama. Tās piemēro kontroles pasākumus, lai novērstu saistītos riskus, tostarp riskus, kas saistīti ar datu automātisku iegūšanu, piemēram, klienta ierīces atrašanās vietas slēpšanu, interneta protokola (IP) adreses viltošanu vai tādus pakalpojumus kā virtuālie privātie tīkli (*VPN*).

4.2.3 Juridisku personu identifikācija

29. Ja kredītiestādes un finanšu iestādes attālināti piesaista klientus, kuri ir juridiskas personas, tās savās politikas nostādnēs un procedūrās atbilstoši 4.1.1. sadaļas 9. punktam nosaka juridisko personu kategorijas, kuras tās piesaistīs attālināti, ņemot vērā NIIL/TF risku saistībā ar katru kategoriju un cilvēka iejaukšanās pakāpi, kas nepieciešama apstiprinātu identifikācijas informācijas apstiprināšanai.

30. Kredītiestādēm un finanšu iestādēm jānodrošina, ka klientu attālinātas piesaistīšanas risinājumam ir funkcijas, kas nodrošina iespēju iegūt:

a) visus būtiskos datus un dokumentāciju, lai identificētu un pārbaudītu juridisku personu;

b) visus būtiskos datus un dokumentāciju, lai pārliecinātos, ka fiziskai personai, kura rīkojas juridiskās personas vārdā, ir likumīgas tiesības šādi rīkoties;

c) informāciju par patiesajiem labuma guvējiem saskaņā ar EBI riska faktoru pamatnostādņu[6] 4.12. noteikumu.

31. Attiecībā uz fizisku personu, kura rīkojas juridiskas personas vārdā, kredītiestādes un finanšu iestādes piemēro identifikācijas procesu, kas aprakstīts 4.2.2.sadaļā.

4.2.4 Darījumu attiecību būtība un mērķis

32. Kad kredītiestādes un finanšu iestādes novērtē un attiecīgā gadījumā iegūst informāciju par darījumu attiecību mērķi un paredzamo būtību saskaņā ar Direktīvas (ES) 2015/849 13. panta 1. punkta c) apakšpunktu, kā sīkāk izklāstīts EBI riska faktoru pamatnostādņu 4.38. iedaļā, tās atbilstoši šīm pamatnostādnēm ir pabeigušas attiecīgās darbības līdz attālinātas klientu piesaistīšanas procesa beigām.

[6] EBA/GL/2021/02

4.3 Dokumentu autentiskums un integritāte

33. Ja kredītiestādes un finanšu iestādes pieņem dokumenta oriģināla kopiju un nepārbauda dokumenta oriģinālu, tām jāpārliecinās, vai kopija ir ticama. Kredītiestādēm un finanšu iestādēm jānosaka vismaz:

    a) vai dokumenta kopijā ir aizsardzības elementi, kas iekļauti dokumenta oriģinālā, un vai dokumenta kopijā esošie specifiski elementi ir derīgi un vai atbilst dokumenta oriģinālā esošajiem elementiem, pievēršot īpašu uzmanību , dokumenta veidam, rakstzīmju lielumam un uzbūvei, salīdzinot tās ar informāciju oficiālajās datubāzēs, piemēram, *PRADO*[7];

    b) vai personas dati ir pārveidoti vai citādi laboti vai – attiecīgā gadījumā – ir aizstāts dokumentā iestrādātais klienta attēls;

    c) vai ir saglabāta dokumenta oriģināla unikālā identifikācijas numura ģenerēšanai izmantotā algoritma integritāte, ja oficiālais dokuments ietver mašīnlasāmu zonu (*MRZ*);

    d) vai iesniegtajai kopijai ir pietiekama kvalitāte un skaidrība, lai nodrošinātu, ka attiecīgā informācija ir nepārprotama;

    e) ka iesniegtā kopija nav izveidota, izmantojot identifikācijas dokumenta oriģināla fotokopiju vai skenēto kopiju.

34. Ja kredītiestādes un finanšu iestādes izmanto rīkus (funkcijas), ar kuru palīdzību var automātiski nolasīt informāciju no dokumentiem, piemēram, izmanto optiskas rakstzīmju pazīšanas (*OCR*) algoritmus vai mašīnlasāmās zonas (*MRZ*) verifikāciju, tad tām jāveic darbības, kas ir nepieciešamas, lai nodrošinātu, ka šie rīki precīzi un konsekventi nolasa informāciju.

35. Situācijās, kad ierīce, ko klients izmanto, lai pierādītu identitāti, ļauj iegūt attiecīgos datus, piemēram, gadījumos, kad dati ir ierakstīti personas elektroniskās identifikācijas kartes čipā un kredītiestādes un finanšu iestādes ar tehniskiem līdzekļiem var piekļūt šiem datiem, kredītiestādēm un finanšu iestādēm jāapsver iespēja izmantot šo informāciju, lai pārbaudītu tās atbilstību informācijai, kas iegūta no citiem avotiem, piemēram, no iesniegtajiem datiem vai citiem dokumentiem, ko iesniedzis klients.

36. Ja pārbaudes procesā ir pieejams oficiālais dokuments, lai pārbaudītu tā autentiskumu, kredītiestādēm un finanšu iestādēm ir jāpārbauda tajā iestrādātie aizsardzības elementi, ja tādi ir, piemēram, hologrammas.

37. Kredītiestādēm un finanšu iestādēm savās politikas nostādnēs un procedūrās jānosaka, kā tās pielāgos savus dokumentu iesniegšanas pieprasījumus finansiālās integrācijas vajadzībām. Ja

[7] https://www.consilium.europa.eu/prado/en/prado-start-page.html

finanšu integrācijas dēļ tiek akceptēti mazāk aizsargāti vai netradicionāli dokumentu veidi, kredītiestādēm un finanšu iestādēm papildus pasākumiem, kas izklāstīti EBI riska faktoru pamatnostādņu 4.10. iedaļā, jāveic kontroles pasākumi vai jānodrošina pastiprināta cilvēku iejaukšanās, lai pārliecinātos, ka viņi izprot NIIL/TF riskus saistībā ar darījumu attiecībām.

4.4 Klienta identitātes atbilstības noteikšana pārbaudes procesā

38. Klientu attālinātas piesaistīšanas risinājumu, ko ievieš kredītiestādes un finanšu iestādes, pārbaudes procesā ir jānodrošina iespēja noteikt vismaz:

    a) vai fiziskās personas redzamā informācija atbilst personas iesniegtajiem dokumentiem;

    b) vai klients kā juridiska persona ir reģistrēts publiskā reģistrā;

    c) vai fiziska persona – juridiskās personas pārstāve ir tiesīga rīkoties klienta – juridiskās personas vārdā.

39. Ja klientu attālinātas piesaistīšanas risinājums ietver biometrisko datu izmantošanu, lai pārbaudītu klienta identitāti, kredītiestādēm un finanšu iestādēm ir jānodrošina, ka biometriskie dati ir pietiekami unikāli, lai tos nepārprotami varētu attiecināt uz konkrētu fizisko personu. Kredītiestādēm un finanšu iestādēm jāizmanto stingri un droši algoritmi, lai pārbaudītu iesniegtajā personas apliecinošajā dokumentā norādīto biometrisko datu atbilstību klientam. Situācijās, kad risinājums nenodrošina pietiekamu uzticamības līmeni, jāpiemēro papildu kontroles pasākumi.

40. Situācijās, kad iesniegtie pierādījumi nav pietiekami kvalitatīvi, tādējādi radot bažas vai neskaidrību tādā mērā, kas ietekmē attālinātas pārbaudes izpildi, konkrētais klienta attālinātas piesaistīšanas process ir jāpārtrauc un jāveic atkārtoti vai klients jāidentificē klātienē.

41. Ja kredītiestādes un finanšu iestādes izmanto attālinātas piesaistīšanas risinājumus, kur klients nesadarbojas ar darbinieku, lai veiktu identifikācijas procesu, tad ir:

    a) jānodrošina, ka visi fotoattēli vai videomateriāli tiek uzņemti pietiekami spilgta apgaismojuma apstākļos un ka nepieciešamie parametri tiek ierakstīti pietiekami skaidri, lai ļautu pienācīgi pārbaudīt klienta identitāti;

    b) jānodrošina, ka visi fotoattēli vai videomateriāli tiek uzņemti klienta identifikācijas procesā;

    c) jāveic dzīvīguma noteikšanas pārbaudes, kas var ietvert procedūras, kurās klientam jāveic īpaša darbība, lai pārliecinātos, ka viņš/viņa piedalās komunikācijas procesā, vai kuru pamatā var būt saņemto datu analīze un klientam nav jāveic īpašas darbības;

d) jāizmanto droši algoritmi, lai pārbaudītu, vai uzņemtie fotoattēli vai videomateriāli atbilst attēliem, kas izgūti no oficiālajiem dokumentiem, kuri ir klienta rīcībā.

42. Ja kredītiestādes un finanšu iestādes izmanto klientu attālinātas piesaistīšanas risinājumus, kur klients sadarbojas ar darbinieku, lai veiktu pārbaudes procesu, tad ir:

a) jānodrošina, ka attēlu un skaņas ierakstu kvalitāte ir pietiekama, lai varētu pienācīgi pārbaudīt klienta identitāti, un ka tiek izmantotas drošas tehniskas sistēmas;

b) jāparedz tāda darbinieka piedalīšanās, kuram ir pietiekamas zināšanas par NILL/TFN regulējumu un attālinātas pārbaudes drošības aspektiem un kurš ir pietiekami apmācīts, lai paredzētu un novērstu tīšu vai apzinātu maldināšanas paņēmienu izmantošanu attālinātā pārbaudē, atklātu šādus gadījumus un attiecīgi reaģētu;

c) jāizstrādā klientu intervēšanas rokasgrāmata, kurā ir definēti nākamie attālinātas pārbaudes procesa posmi un darbības, kas jāveic darbiniekam. Intervēšanas rokasgrāmatā jāiekļauj norādījumi par psiholoģisku faktoru vai citu pazīmju novērošanu un identificēšanu, kas varētu raksturot aizdomīgu uzvedību attālinātas identifikācijas laikā.

43. Ja iespējams, kredītiestādēm un finanšu iestādēm jāizmanto tādi klientu attālinātas piesaistīšanas risinājumi, kas ietver nejaušību to darbību secībā, kuras klientam jāveic pārbaudes nolūkā, lai aizsargātos pret tādiem riskiem kā sintētisko identitāšu vai piespiešanas izmantošana. Ja iespējams, kredītiestādēm un finanšu iestādēm arī izlases veidā jānorīko darbinieki, kuri atbild par attālinātās pārbaudes procesu, lai nepieļautu klienta un atbildīgā darbinieka slepenu vienošanos.

44. Papildus minētajam atbilstoši NIIL/TF riskiem, kas saistīti ar darījumu attiecībām, kredītiestādēm un finanšu iestādēm jāizmanto viens vai vairāki tālāk minētie kontroles pasākumi vai līdzīgi pasākumi, lai uzlabotu pārbaudes procesa ticamību. Minētajos kontroles pasākumos cita starpā var iekļaut šādas darbības:

a) pirmais maksājums tiek veikts uz kontu, kas vienpersoniski vai kopīgi atvērts uz klienta vārda regulētā EEZ kredītiestādē vai finanšu iestādē vai trešā valstī, kuras NILL/TFN prasības atbilst Direktīvā (ES) 2015/849 noteiktajām;

b) klientam nosūta nejaušināti ģenerētu pieejas kodu, ar ko klients apstiprina klātbūtni attālinātās pārbaudes procesā. Pieejas kodam jābūt vienreiz lietojamam un ar ierobežotu darbības laiku;

c) iegūst biometriskos datus, lai salīdzinātu tos ar datiem, kas iegūti no citiem neatkarīgiem un ticamiem avotiem;

d) saziņa ar klientu pa tālruni;

e) tieši pasta sūtījumi (gan elektroniski, gan pa pastu) klientam.

45. Kredītiestādēm un finanšu iestādēm jāuzskata, ka no 38. punkta līdz 43. punktam minētie kritēriji ir izpildīti, ja risinājumā izmanto vienu no šādiem elementiem:

    a) elektroniskās identifikācijas shēmas, kas paziņotas saskaņā ar Regulas (EK) Nr. 910/2014 9. pantu un kas atbilst uzticamības līmeņiem "būtisks" vai "augsts", kā definēts minētās regulas 8. pantā;

    b) attiecīgus kvalitatīvus un uzticamus pakalpojumus, kas atbilst prasībām, kuras noteiktas Regulā (EK) Nr. 910/2014, jo īpaši tās III nodaļas 3. iedaļā un 24. panta 1. punkta 2. daļas b) apakšpunktā.

4.5 Paļaušanās uz trešām personām un ārpakalpojumi

46. Papildus darbībām, kas izklāstītas 9. punktā, kredītiestādēm un finanšu iestādēm savās politikas nostādnēs un procedūrās jānosaka, kuras klientu attālinātas piesaistīšanas funkcijas un darbības veiks vai izpildīs kredītiestāde un finanšu iestāde, trešās personas vai citi ārpakalpojumu sniedzēji.

4.5.1 Paļaušanās uz trešo personu sniegtajiem pakalpojumiem saskaņā ar Direktīvas (ES) 2015/849 II nodaļas 4. iedaļu

47. Papildus EBI riska faktoru pamatnostādnēm[8], jo īpaši minēto pamatnostādņu 2.20. līdz 2.21. iedaļai, 4.32. un 4.37. iedaļai, tiem jāpiemēro šādi kritēriji:

    a) jāveic darbības, kas nepieciešamas, lai pārliecinātos, ka trešo personu klientu attālinātas piesaistīšanas procesos un procedūrās ir noteikta klientu izpēte un ka informācija un dati, ko tās šajā kontekstā iegūst, ir pietiekami un atbilst prasībām, kas izklāstītas šajās pamatnostādnēs;

    b) jānodrošina klienta un kredītiestādes un finanšu iestādes uzsākto darījumu attiecību nepārtrauktība, lai nodrošinātu aizsardzību pret notikumiem, kas varētu atklāt nepilnības trešās puses veiktajā klienta attālinātās piesaistīšanas procesā.

4.5.2 Ārpakalpojumu izmantošana klienta uzticamības pārbaudes veikšanai

48. Ja kredītiestādes un finanšu iestādes visu klientu attālināto piesaistīšanas procesu vai tā daļas uztic ārpakalpojumu sniedzējam, kā minēts Direktīvas (ES) 2015/849 29. pantā, kredītiestādēm un finanšu iestādēm papildus EBI riska faktoru pamatnostādņu 2.20. līdz 2.21. iedaļai, 4.32. un 4.37. iedaļai, kā arī attiecīgā gadījumā papildus EBI pamatnostādnēm par ārpakalpojumu izmantošanu[9] pirms darījumu attiecībām ar ārpakalpojumu sniedzēju un darījumu attiecību laikā ir jāveic šādi pasākumi, ņemot vērā uz risku balstītu pieeju:

[8] EBA/GL/2021/02

[9] EBI pamatnostādnes par ārpakalpojumu izmantošanu.docx (europa.eu)

a) jānodrošina, ka ārpakalpojumu sniedzējs faktiski īsteno un ievēro kredītiestādes un finanšu iestādes attālinātās klientu piesaistīšanas politikas nostādnes un procedūras saskaņā ar ārpakalpojumu līgumu. Minēto politiku un procedūru ievērošana jānodrošina ar regulāru ziņošanu, pastāvīgu uzraudzību, apmeklējumiem uz vietas vai izlases pārbaudēm;

b) jāveic novērtējumi, lai nodrošinātu, ka ārpakalpojuma sniedzēja rīcībā ir pietiekami līdzekļi un tas spēj veikt attālinātas klientu piesaistīšanas procesu. Novērtējumos cita starpā var iekļaut ārpakalpojumu sniedzēja darbinieku apmācības, tehniskās gatavības un datu pārvaldības novērtējumu;

c) jānodrošina, ka ārpakalpojumu sniedzējs informē kredītiestādes un finanšu iestādes par visiem ierosinātajiem klientu attālinātas piesaistīšanas procesa grozījumiem vai visām izmaiņām, kas veiktas ārpakalpojumu sniedzēja nodrošinātajam risinājumam.

49. Ja ārpakalpojumu sniedzējs klientu attālinātas piesaistīšanas procesā glabā klientu datus, tostarp fotoattēlus, videomateriālus un dokumentus, kredītiestādēm un finanšu iestādēm jānodrošina, ka:

a) tiek vākti tikai nepieciešamie klientu dati un ka tie tiek glabāti skaidri noteiktā uzglabāšanas periodā;

b) piekļuve datiem ir stingri ierobežota un reģistrēta;

c) ir ieviesti pienācīgi drošības pasākumi, lai nodrošinātu uzglabāto datu aizsardzību.

4.6 IKT un drošības risku pārvaldība

50. Kredītiestādēm un finanšu iestādēm jāidentificē un jāpārvalda savi IKT un drošības riski, kas saistīti ar klientu attālinātās piesaistīšanas procesa izmantošanu, tostarp gadījumos, kad kredītiestādes un finanšu iestādes paļaujas uz trešām personām vai izmanto ārpakalpojumus, tostarp arī grupas struktūru pakalpojumus.

51. Papildus prasībām, kas noteiktas EBI pamatnostādnēs par IKT un drošības risku pārvaldību[10], attiecīgā gadījumā kredītiestādēm un finanšu iestādēm sadarbībai ar klientiem attālinātās klientu piesaistīšanas procesā jāizmanto droši saziņas kanāli. Attālinātās klientu piesaistīšanas risinājumā jāizmanto droši protokoli un šifrēšanas algoritmi atbilstoši nozares labākajai praksei, lai attiecīgi garantētu iesniegto datu konfidencialitāti, autentiskumu un integritāti.

52. Kredītiestādēm un finanšu iestādēm jānodrošina drošs piekļuves punkts attālinātas klientu piesaistīšanas procesa sākšanai, pamatojoties uz kvalificētiem elektronisko zīmogu sertifikātiem, kā minēts Regula (ES) Nr. 910/2014, 3. panta 30. punktā, vai kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem, kā minēts šīs regulas 3. panta 39. punktā. Klients

[10] EBA/GL/2019/04

jāinformē arī par piemērojamiem drošības pasākumiem, kas jāveic, lai garantētu drošu sistēmas izmantošanu.

53. Ja klientu attālinātas piesaistīšanas procesa izpildei izmanto universālu ierīci, attiecīgā gadījumā ir jāizmanto droša vide programmatūras koda izpildei klienta pusē. Jāievieš papildu drošības pasākumi, lai garantētu programmatūras koda un iegūto datu drošību un uzticamību, ņemot vērā drošības risku novērtējumu, kā izklāstīts EBI pamatnostādnēs par IKT un drošības risku pārvaldību.

4.7 Šo pamatnostādņu ievērošana gadījumos, kad kredītiestādes un finanšu iestādes izmanto uzticamības pakalpojumus un valsts identifikācijas procesus, kā minēts Direktīvas (ES) 2015/849 13. panta 1. punkta a) apakšpunktā

54. Lai izpildītu šajās pamatnostādnēs noteikto, kredītiestādes un finanšu iestādes var izmantot attiecīgus uzticamus pakalpojumus un elektroniskus identifikācijas procesus, ko regulē, ir atzinušas, apstiprinājušas vai pieņēmušas attiecīgās valsts iestādes, kā minēts Direktīvas (ES) 2015/849 13. panta 1. punkta a) apakšpunktā. Izmantojot šādus risinājumus, kredītiestādēm un finanšu iestādēm jānovērtē, cik lielā mērā attiecīgais risinājums atbilst šīm pamatnostādnēm, un jāpiemēro pasākumi, kas vajadzīgi, lai mazinātu visus attiecīgos riskus, kas izriet no šo risinājumu izmantošanas. Tām jo īpaši jāņem vērā, vai ir novērsti šādi riski:

    a) riski, kas saistīti ar autentifikāciju, un to politikas nostādnēs un procedūrās noteiktie īpašie riska mazināšanas pasākumi, jo īpaši attiecībā uz "līdzinieku" krāpniecības riskiem;

    b) risks, ka klienta identitāte nav viņa īstā identitāte;

    c) zaudētu, nozagtu, apturētu, atsauktu vai nederīgu identitātes pierādījumu risks, kā arī attiecīgā gadījumā rīki viltotas identitātes izmantošanas atklāšanai.