EBA/GL/2024/01

16. januar 2024

Smernice o spremembi smernic EBA/GL/2021/02

na podlagi člena 17 in člena 18(4) Direktive (EU) 2015/849 o poenostavljenem in okrepljenem skrbnem preverjanju strank ter dejavnikih, ki bi jih kreditne in finančne institucije morale upoštevati pri oceni tveganja pranja denarja in financiranja terorizma, povezanega s posameznimi poslovnimi odnosi in občasnimi transakcijami (smernice o dejavnikih tveganja PD/FT)

1. Obveznosti glede skladnosti in poročanja

Vloga teh smernic

1. Dokument vsebuje smernice, izdane v skladu s členom 16 Uredbe (EU) št. 1093/2010[1]. V skladu s členom 16(3) Uredbe (EU) št. 1093/2010 si morajo pristojni organi in finančne institucije na vsak način prizadevati za upoštevanje smernic.

2. V smernicah je predstavljeno stališče organa EBA o ustreznih nadzorniških praksah v Evropskem sistemu finančnega nadzora in o tem, kako bi bilo treba zakonodajo Unije uporabljati na določenem področju. Pristojni organi iz člena 4(2) Uredbe (EU) št. 1093/2010, za katere smernice veljajo, bi jih morali upoštevali tako, da jih ustrezno vključijo v svoje prakse (npr. s spremembo svojega pravnega okvira ali nadzorniških postopkov), tudi če so smernice namenjene predvsem institucijam.

Dolžnost poročanja

3. Pristojni organi bi morali v skladu s členom 16(3) Uredbe (EU) št. 1093/2010 do 28.08.2024 organ EBA uradno obvestiti, ali ravnajo oziroma ali nameravajo ravnati v skladu s temi smernicami, ali pa mu sporočiti razloge za njihovo neupoštevanje. Če pristojni organi uradnega obvestila ne bodo poslali do tega roka, bo organ EBA štel, da smernic ne upoštevajo. Uradna obvestila je treba poslati na obrazcu, ki je na voljo na spletnem mestu organa EBA, z navedbo sklica „EBA/GL/2024/01“. Predložiti bi jih morale osebe, ki so pooblaščene za poročanje o skladnosti v imenu svojih pristojnih organov. Organu EBA je treba sporočiti tudi vsako spremembo stanja glede upoštevanja smernic.

4. Uradna obvestila bodo v skladu s členom 16(3) objavljena na spletnem mestu organa EBA.

[1] Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12).

2. Vsebina, področje uporabe in opredelitev pojmov

Naslovniki

5. Te smernice so naslovljene na kreditne in finančne institucije, kot so opredeljene v členu 3(1) in (2) Direktive (EU) 2015/849[2], ter pristojne organe, kot so opredeljeni v členu 4(2)(iii) Uredbe (EU) št. 1093/2010.

[2] Direktiva (EU) 2015/849 Evropskega parlamenta in Sveta z dne 20. maja 2015 o preprečevanju uporabe finančnega sistema za pranje denarja ali financiranje terorizma (UL L 141, 5.6.2015, str. 73-117).

3. Izvajanje

Začetek uporabe

6. Te smernice se začnejo uporabljati 30. decembra 2024.

4. Spremembe

(i) Sprememba naslova smernic

7. Naslov smernic se nadomesti z naslednjim:

„Smernice EBA/2021/02 na podlagi Direktive (EU) 2015/849 o poenostavljenem in okrepljenem skrbnem preverjanju strank ter dejavnikih, ki bi jih kreditne in finančne institucije morale upoštevati pri oceni tveganja pranja denarja in financiranja terorizma, povezanega s posameznimi poslovnimi odnosi in občasnimi transakcijami (smernice o dejavnikih tveganja PD/FT)“

(ii) Spremembe poglavja „Vsebina, področje uporabe in opredelitev pojmov“

8. V odstavku 12 se uvodni stavek nadomesti z naslednjim:

„Če ni navedeno drugače, imajo izrazi v teh smernicah enak pomen kot izrazi, ki se uporabljajo in so opredeljeni v Direktivi (EU) 2015/849 in Uredbi (EU) 2023/1113. Za namene teh smernic se uporabljajo tudi naslednje opredelitve pojmov:“

9. V odstavku 12 se črtata točki (f) in (m).

(iii) Spremembe smernice 1: Ocena tveganja: ključna načela za vsa podjetja

10. V smernici 1.7 se doda naslednja točka:

„d) Kadar podjetje uvaja nove produkte, storitve ali poslovne prakse ali jih bistveno spreminja, vključno z uvedbo nove tržne poti ali sprejetjem inovativne tehnologije kot del svojih sistemov in kontrolnega okvira za preprečevanje pranja denarja in financiranja terorizma (PPDFT), mora pred uvedbo teh produktov, storitev ali poslovnih praks oceniti izpostavljenost tveganju pranja denarja in financiranja terorizma (PD/FT). Kadar imajo ti produkti, storitve ali poslovne prakse pomemben vpliv na izpostavljenost podjetja tveganju PD/FT, bi moralo podjetje to oceno upoštevati v svoji oceni tveganja poslovanja podjetja, ki se izvaja v skladu s členom 8(2) Direktive (EU) 2015/849, ter v svojih politikah in postopkih.“

(iv) Spremembe smernice 2: Opredelitev dejavnikov tveganja PD/FT

11. V smernici 2.4 se točka b) nadomesti z naslednjim:

„b) Ali ima stranka ali dejanski lastnik povezave s sektorji, ki so povezani z višjim tveganjem PD/FT, na primer z nekaterimi podjetji, ki opravljajo denarne storitve, ponudniki storitev v zvezi s kriptosredstvi (CASP), kot so opisani v smernicah 9.20 in 9.21, igralnicami ali trgovci s plemenitimi kovinami?“

(v) Spremembe smernice 4: Ukrepi skrbnega preverjanja strank, ki bi jih morala izvajati vsa podjetja

12. V smernici 4.29 se uvodni stavek nadomesti z naslednjim:

„4.29 Da bi podjetja izpolnjevala svoje obveznosti iz člena 13(1) Direktive (EU) 2015/849, kadar se poslovni odnos začne, vzpostavi ali izvaja brezosebno ali se občasne transakcije opravijo brezosebno v skladu s Smernicami EBA (EBA/GL/2022/15) o uporabi rešitev za sklepanje poslovnega razmerja s stranko na daljavo v skladu s členom 13(1) Direktive (EU) 2015/849, bi morala:“

13. Smernica 4.35 se nadomesti z naslednjim:

„4.35 Če je zunanji ponudnik podjetje s sedežem v državi, ki ni članica EU, bi moralo podjetje zagotoviti, da razume pravna in operativna tveganja ter z njimi povezane zahteve glede varstva podatkov in da ta tveganja učinkovito blaži. Podjetje bi moralo tudi zagotoviti, da ima po potrebi takojšen dostop do ustreznih podatkov in informacij o strankah, tudi v primeru odpovedi dogovora o zunanjem izvajanju.“

14. V smernici 4.60 se točka a) nadomesti z naslednjim:

„a) se razlikujejo od transakcij, ki jih podjetje običajno pričakuje na podlagi svojega poznavanja stranke, poslovnega odnosa ali kategorije, v katero sodi stranka, bodisi po znesku, pogostosti, kompleksnosti transakcij ali podobno, tudi kadar so transakcije večje ali pogostejše kot običajno, ali pri transakcijah z majhnimi zneski, ki so nenavadno pogoste, ali kadar se zaporedne transakcije izvajajo brez očitne ekonomske utemeljitve, kot so transakcije, ki so razdeljene, da bi zaobšli omejitve poročanja ali uskladili neobičajne transakcije z običajno pričakovanim ravnanjem in vzorci, podprtimi z informacijami, zbranimi med postopkom vključitve in stalnim spremljanjem poslovnega odnosa;“

15. V smernici 4.61 se točka a) nadomesti z naslednjim:

„a) sprejemanje utemeljenih in ustreznih ukrepov za razumevanje ozadja in namena teh transakcij, na primer z opredelitvijo vira in prejemnikov sredstev ali kriptosredstev ali s pridobitvijo več informacij o poslovanju stranke, da bi se ugotovilo, ali obstaja verjetnost, da bo stranka izvedla take transakcije; in“

16. V smernici 4.74 se točka b) nadomesti z naslednjim:

„b) ali bodo transakcije spremljala ročno ali z uporabo avtomatiziranega sistema za spremljanje transakcij. Podjetja, ki obdelujejo veliko število transakcij ali transakcije izvajajo pogosto, bi morala razmisliti o vzpostavitvi avtomatiziranega sistema za spremljanje transakcij;“

17. V smernici 4.74 se doda naslednja točka:

„d) ali je uporaba naprednih analitičnih orodij, kot so analitična orodja razpršene evidence ali blokovnih verig, potrebna glede na tveganje PD/FT, povezano s poslovanjem podjetja, in s posameznimi transakcijami strank podjetja.“

(vi) Spremembe smernice 6: Usposabljanje

18. V smernici 6.2 se točka c) nadomesti z naslednjim:

„(c) kako prepoznati sumljive ali neobičajne transakcije in dejavnosti, ob upoštevanju posebne narave njihovih produktov in storitev, ter kako v takih primerih ravnati;“

19. V smernici 6.2 se doda naslednja točka:

„d) kako uporabljati avtomatizirane sisteme, vključno z naprednimi analitičnimi orodji, za spremljanje transakcij in poslovnih odnosov ter kako razlagati rezultate teh sistemov in orodij.“

(vii) Spremembe smernice 8: Sektorske smernice za korespondenčne odnose

20. V smernici 8.6 se točka d) nadomesti z naslednjim:

„d) respondent veliko posluje s sektorji, ki so povezani z višjimi stopnjami tveganja PD/FT. Na primer izvaja:

i. Številna denarna nakazila;

ii. posle v imenu nekaterih subjektov, ki izvajajo denarna nakazila, ali menjalnic;

iii. posle v imenu CASP ali z njimi, ki niso CASP, ki jih ureja Uredba (EU) 2023/1114[3], za katere velja regulativna in nadzorna ureditev PPDFT, ki je manj stroga kot ureditev, predvidena v Direktivi (EU) 2015/849, ali za katere ne veljajo nobene obveznosti PPDFT;

iv. pomemben obseg poslovanja v imenu CASP, za katere je poslovni model osredotočen na zagotavljanje produktov in storitev, opisanih v smernici 21.3(d);

v. poslovanje z nerezidenti; ali

vi. poslovanje v valuti, ki ni valuta države, v kateri ima sedež.“

21. V smernici 8.6 se doda naslednja točka:

„h) račun IBAN, ki ga je zagotovil CASP, na katerem prejema sredstva v uradni valuti[4] od strank, je v imenu in lasti podjetja, ki ni podjetje CASP ali za katerega je kakor koli znano, da je povezano s CASP.“

22. V smernici 8.8 se doda naslednja točka:

„d) respondent ne more z zadostno stopnjo gotovosti preveriti, da njegove stranke nimajo sedeža v jurisdikcijah, navedenih v točki (a) smernice 8.8, vključno s preverjanjem naslovov internetnega protokola (IP) svojih strank ali drugimi sredstvi, v okoliščinah, ko to zahtevajo

[3] Uredba (EU) št. 2023/1114 o trgih kriptosredstev ter spremembi uredb (EU) št. 1093/2010 in (EU) št. 1095/2010 ter direktiv 2013/36/EU in (EU) 2019/1937

[4] Člen 3(8) Uredbe (EU) 2023/1114 opredeljuje uradno valuto kot uradno valuto države, ki jo izda centralna banka ali drug monetarni organ.

politike in postopki respondenta.“

23. V smernici 8.17 se točki a) in c) nadomestita z naslednjim:

„a) zberejo dovolj informacij o respondenčni instituciji in se tako v celoti seznanijo z naravo poslovanja respondenta, da ugotovijo, v kolikšnem obsegu je korespondent zaradi tega poslovanja izpostavljen višjemu tveganju pranja denarja. To bi moralo vključevati sprejetje ukrepov za razumevanje in oceno tveganja narave kroga respondentovih strank, po potrebi tako, da podjetja respondenta vprašajo o njegovih strankah, in vrsti dejavnosti, s katerimi bo respondent opravljal transakcije prek korespondenčnega računa, ali, če je to ustrezno, vrste kriptosredstev, s katerimi bo respondent CASP izvedel transakcije prek korespondenčnega računa;“

„c) ocenijo kontrole na področju PPDFT v respondenčni instituciji. To pomeni, da bi moral korespondent izvesti kvalitativno oceno respondentovega okvira kontrol na področju PPDFT, ne pa le pridobiti izvoda respondentovih politik in postopkov na področju preprečevanja pranja denarja (PPD). Ta ocena bi morala vključevati vzpostavljena orodja za spremljanje transakcij, da se zagotovi, da so ustrezna za vrsto poslovanja, ki ga opravlja respondent. To oceno bi bilo treba ustrezno dokumentirati. Kadar je tveganje še posebej visoko in zlasti kadar je obseg korespondenčnih bančnih transakcij velik, bi moral korespondent v skladu s pristopom, ki temelji na tveganju, preučiti možnost neposrednega nadzora in/ali preskušanja vzorcev, da bi se prepričal, da se respondentove politike in postopki na področju PPD izvajajo učinkovito;

(viii) Spremembe smernice 9: Sektorska smernica za banke, ki poslujejo s prebivalstvom

24. Smernica 9.3 se nadomesti z naslednjim:

„9.3. Banke bi morale poleg dejavnikov tveganja in ukrepov, ki so določeni v naslovu I teh smernic, upoštevati tudi dejavnike tveganja in ukrepe, opredeljene v nadaljevanju. Banke, ki opravljajo storitve upravljanja premoženja, bi morale upoštevati tudi sektorsko smernico 12, tiste, ki opravljajo storitve odreditve plačil ali storitve zagotavljanja informacij o računih bi morale upoštevati tudi sektorsko smernico 18, banke, ki opravljajo storitve v zvezi s kriptosredstvi, pa bi morale upoštevati sektorsko smernico 21.“

25. Smernica 9.16 se nadomesti z naslednjim:

„9.16 Če stranka na banki odpre „fiduciarni/zbirni račun“ za upravljanje sredstev ali kriptosredstev, ki pripadajo njenim lastnim strankam, bi morala banka izvajati vse ukrepe skrbnega preverjanja strank, vključno z obravnavo teh strank kot dejanskih lastnikov sredstev na skupnem računu ter preverjanjem njihove identitete.

26. Smernica 9.17 se nadomesti z naslednjim:

„9.17 Če banka na podlagi ocene tveganja PD/FT, izvedene v skladu s temi smernicami, ugotovi, da je stopnja tveganja PD/FT, povezanega s poslovnim odnosom, visoka, mora po potrebi uporabiti ukrepe okrepljenega skrbnega preverjanja strank iz člena 18 Direktive (EU) 2015/849.“

27. V smernici 9.18 se uvodni stavek nadomesti z naslednjim:

„9.18. Vendar lahko banke, kolikor to dopušča nacionalna zakonodaja in kadar je tveganje, glede na individualno oceno tveganja PD/TF pri stranki, povezano s poslovnim odnosom, nizko, izvajajo ukrepe poenostavljenega skrbnega preverjanja strank, če:“

28. Naslov smernic 9.20 do 9.24 se nadomesti z naslednjim:

„Stranke, ki ponujajo storitve, povezane s kriptosredstvi“

29. Smernice 9.20 do 9.23 se črtajo.

30. Vstavita se naslednji smernici 9.20 in 9.21:

„9.20 Pri sklepanju poslovnega odnosa s stranko, ki je CASP, ki ni CASP, ki ga ureja Uredba (EU) 2023/1114[5], so lahko banke izpostavljene povečanemu tveganju PD/FT. Tveganje se lahko zmanjša v okoliščinah, ko je takšen ponudnik reguliran in nadzorovan na podlagi regulativnega okvira, podobnega tistemu iz Uredbe (EU) 2023/1114 ali Direktive (EU) 2015/849. Banke bi morale pri teh strankah opraviti oceno tveganja PD/FT, preden z njimi vzpostavijo poslovni odnos. Pri tem bi morale upoštevati tudi tveganje PD/FT, povezano s posebno vrsto kriptosredstev, ki jih ti ponudniki zagotavljajo ali opravljajo.“

„9.21 Da bi banke ublažile stopnjo tveganja PD/FT, povezanega s strankami iz smernice 9.20, bi morale v okviru ukrepov skrbnega preverjanja strank najmanj:

a) vzpostaviti dialog s stranko, da bi spoznale naravo poslovanja ter tveganja PD/FT, ki so mu izpostavljene;

b) poleg preverjanja identitete dejanskih lastnikov stranke izvajati preverjanje višjega vodstva, če to niso iste osebe, vključno z upoštevanjem morebitnih negativnih informacij;

c) se seznaniti, v kolikšni meri te stranke same uporabljajo ukrepe skrbnega preverjanja v zvezi z lastnimi strankami bodisi zaradi pravne obveznosti bodisi prostovoljno;

d) ugotoviti, ali je stranka registrirana oziroma je pridobila licenco v državi članici EU/EGP ali v državi, ki ni članica EU, in v primeru države, ki ni članica EU, sprejeti stališče o ustreznosti regulativne in nadzorne ureditve države, ki ni članica EU, na področju PPDFT v skladu s Smernico 2.11;

e) ugotoviti, ali se za storitve, ki jih zagotavlja stranka, zahteva registracije ali licenciranje stranke;

f) ugotoviti, ali stranka opravlja storitve, za katere ni registrirana ali nima licence kot kreditna ali finančna institucija;

[5] Uredba (EU) št. 2023/1114 o trgih kriptosredstev ter spremembi uredb (EU) št. 1093/2010 in (EU) št. 1095/2010 ter direktiv 2013/36/EU in (EU) 2019/1937.

g) kadar poslovanje stranke vključuje izdajanje kriptosredstev za zbiranje sredstev, kot so prve ponudbe kovancev, bi morale banke določiti, ali se takšno poslovanje izvaja v skladu z obstoječimi pravnimi zahtevami in, kadar je ustrezno, ali je regulirano za namene PPDFT v skladu z mednarodno dogovorjenimi standardi, kot so standardi, ki jih objavi Projektna skupina za finančno ukrepanje.“

(ix) Spremembe smernice 10: Sektorska smernica za izdajatelje elektronskega denarja

31. Smernica 10.2 se nadomesti z naslednjim:

„10.2. Podjetja, ki izdajajo e-denar, bi morala upoštevati naslednje dejavnike tveganja in ukrepe poleg tistih, ki so določeni v naslovu I teh smernic. Podjetja, ki so pooblaščena tudi za opravljanje poslovnih dejavnosti, kot so storitve odreditve plačil in storitve zagotavljanja informacij o računih, bi morala upoštevati tudi sektorsko smernico 18. V tem okviru je lahko ustrezna tudi sektorska smernica 11 za subjekte, ki izvajajo denarna nakazila. Podjetja, ki opravljajo storitve v zvezi s kriptosredstvi, bi morala upoštevati tudi sektorsko smernico 21.“

(x) Spremembe smernice 15: Sektorska smernica za investicijska podjetja

32. Smernica 15.1 se nadomesti z naslednjim:

„15.1. Investicijska podjetja, kot so opredeljena v členu 4(1)(1) Direktive 2014/65/EU, bi morala pri zagotavljanju ali izvajanju investicijskih storitev ali poslov, kot so opredeljeni v členu 4(1)(2) Direktive 2014/65/EU, upoštevati naslednje dejavnike tveganja in ukrepe poleg tistih iz naslova I teh smernic. V tem okviru sta lahko relevantni tudi sektorski smernici 12 in 21.“

(xi) Spremembe smernice 17: Sektorska smernica za regulirane platforme za množično financiranje

33. V smernici 17.4 se točka i) nadomesti z naslednjim:

„i). ponudnik storitev množičnega financiranja vlagateljem in lastnikom projektov omogoča, da uporabljajo kriptosredstva za poravnavo svojih plačilnih transakcij prek platforme za množično financiranje, kadar so takšne transakcije lahko izpostavljene povečanemu tveganju PD/FT zaradi dejavnikov, opisanih v smernici 21.3(d);“

34. V smernici 17.6 se točka b) nadomesti z naslednjim:

„b) vlagatelj ali lastnik projekta prenese kriptosredstva, kadar je takšna transakcija lahko izpostavljena povečanemu tveganju PD/FT zaradi dejavnikov, opisanih v smernici 21.3(d);“

35. Vstavi se naslednja smernica 21:

(xii) „Smernica 21: Sektorska smernica za ponudnike storitev v zvezi s kriptosredstvi (CASP)

21.1. CASP bi se morali zavedati, da so izpostavljeni tveganjem PD/FT zaradi posebnih značilnosti njihovega poslovnega modela in tehnologije, ki se uporablja v okviru njihovega poslovanja, kar jim omogoča takojšen prenos kriptosredstev po svetu in sklepanje poslovnih razmerij s strankami v različnih jurisdikcijah. Tveganje se še poveča, če obdelujejo ali omogočajo transakcije ali ponujajo produkte ali storitve, ki zagotavljajo višjo stopnjo anonimnosti.

21.2. CASP bi morali pri ponujanju storitev v zvezi s kriptosredstvi izpolnjevati določbe iz naslova I in sektorske določbe iz naslova II, kadar so te pomembne za ponudbo produkta CASP.

Dejavniki tveganja

Dejavniki tveganja v zvezi s produkti, storitvami in transakcijami

21.3. K **povečanju tveganja** lahko prispevajo naslednji dejavniki:

a) produkti ali storitve, ki jih zagotavlja CASP, zagotavljajo višjo stopnjo anonimnosti;

b) produkt dovoljuje plačila tretjih oseb, ki niso povezana s produktom ter niso vnaprej identificirana in preverjena, kadar takšna plačila nimajo očitnega ekonomskega razloga;

c) produkt ne postavlja vnaprejšnjih omejitev glede skupnega obsega ali vrednosti transakcij;

d) produkt omogoča transakcije med računom stranke in:

i. naslovi brez gostitelja;

ii. računi kriptosredstev ali naslovi razpršene evidence, ki jih upravlja CASP, kot je opredeljen v smernici 9.20, ali za katerega velja regulativna in nadzorna ureditev PPDFT, ki je manj stroga od ureditve, predvidene v Direktivi (EU) 2015/849;

iii. platformo za medsebojno izmenjavo kriptovalut ali drugo vrsto decentralizirane ali porazdeljene infrastrukture za kriptosredstva, ki je ne nadzoruje ali nanjo ne vpliva pravna ali fizična oseba (pogosto imenovana „decentralizirane finance“ (DeFi));

iv. platformami, katerih namen je prikriti transakcije in omogočiti anonimnost, kot so platforme mešalnik ali tambler (mixer or tumbler);

v. strojno opremo, ki se uporablja za zamenjavo kriptosredstev v uradne valute ali obratno (kot so kriptobankomati), ki vključuje uporabo gotovine ali elektronskega denarja, ki je izvzeta na podlagi člena 12 Direktive (EU) 2015/849 ali ki ne spada na področje regulativnega in

nadzornega sistema v EU;

e) produkti, ki vključujejo nove poslovne prakse, vključno z novimi tržnimi potmi, in uporabo tehnologij, pri katerih CASP zaradi pomanjkanja informacij ne more zanesljivo oceniti stopnje tveganja PD/FT v skladu s točko (d) smernice 1.7;

f) kadar CASP izvaja neučinkovit nadzor nad ugnezdeno storitvijo, ki jo zagotavlja drug CASP;

g) rezultati analize, izvedene z naprednimi analitičnimi orodji, kažejo na povečano stopnjo tveganja.

21.4. K **zmanjšanju tveganja** lahko prispevajo naslednji dejavniki:

a) produkti z zmanjšano funkcionalnostjo, kot je majhen obseg ali vrednost transakcij;

b) produkt omogoča transakcije med računom stranke in

i. računi kriptosredstev ali naslovi razpršene evidence na ime stranke, ki jih vodi CASP;

ii. računom kriptosredstva ali naslovom razpršene evidence na ime stranke, ki ga vodi CASP, ki ni CASP v skladu z Uredbo (EU) 2023/1114[6], temveč je reguliran zunaj EU na podlagi regulativnega okvira, ki je enako strog kot tisti, predviden v Uredbi (EU) 2023/1114, in za katerega velja regulativni in nadzorni okvir PD/FT, ki je enako strog kot tisti, predviden v Direktivi (EU) 2015/849;

iii. bančnim računom na ime stranke pri kreditni instituciji, za katero velja regulativni in nadzorni okvir za PPDFT iz Direktive (EU) 2015/849 ali drug zakonodajni okvir zunaj EU, ki je enako strog kot tisti iz Direktive (EU) 2015/849; ali

c) narava in obseg plačilnih kanalov ali sistemov, ki jih uporablja CASP, sta omejena na sisteme zaprtega trgovanja ali sisteme, katerih namen je olajšati mikroplačila ali plačila države subjektom in obratno;

d) produkt je na voljo le omejeni in določeni skupini strank, kot so zaposleni v podjetju, ki je izdalo kriptosredstvo.

Dejavniki tveganja v zvezi s strankami

21.5. K **povečanju tveganja** lahko prispevajo naslednji dejavniki:

a) v zvezi z **naravo stranke** zlasti:

i. neprofitna organizacija, ki je bila na podlagi zanesljivih in neodvisnih virov povezana z ekstremizmom, ekstremistično propagando ali naklonjenostjo terorizmu in terorističnimi dejavnostmi ali je bila vpletena v nepravilno

[6] Uredba (EU) št. 2023/1114 o trgih kriptosredstev ter spremembi uredb (EU) št. 1093/2010 in (EU) št. 1095/2010 ter direktiv 2013/36/EU in (EU) 2019/1937

ravnanje ali kriminalne dejavnosti, vključno s primeri, povezanimi s pranjem denarja, financiranjem terorizma ali korupcijo;

ii. podjetje, ki je navidezna banka, kot je opredeljena v členu 3(17) Direktive (EU) 2015/849, ali druga vrsta navideznega podjetja;

iii. podjetje, ki je bilo ustanovljeno nedavno in obdeluje veliko število transakcij;

iv. zakonito registrirano podjetje, ki obdeluje veliko število transakcij po obdobju nedejavnosti odkar je bilo ustanovljeno;

v. podjetje, ki je v poslovnem odnosu z drugim(-i) podjetjem(-i) v skupini, kot je opredeljeno v členu 3(15) Direktive (EU) 2015/849, ki zagotavlja produkte in storitve, povezane s kriptosredstvi;

vi. podjetje ali oseba, ki uporablja naslov IP, povezan s temnim omrežjem, ali programsko opremo, ki omogoča anonimno komunikacijo, vključno s šifrirano elektronsko pošto, anonimnimi ali začasnimi storitvami elektronske pošte in navidezno zasebno omrežje (VPN);

vii. ranljiva oseba, tj. oseba, ki verjetno ni tipična stranka CASP, ali oseba, ki izkazuje zelo malo znanja in razumevanja o kriptosredstvih ali povezanih tehnologijah, kar se lahko dokaže z rezultati preskusa ustreznosti/znanja ali z drugimi stiki s stranko, in ki se kljub temu odloči za pogoste transakcije ali transakcije visoke vrednosti, lahko poveča tveganje, da se stranka izkorišča kot denarna mula;

b) v zvezi z **vedenjem stranke** zlasti situacije, v katerih stranka:

i. poskuša odpreti več računov kriptosredstev pri CASP brez očitne ekonomske utemeljitve ali poslovnega namena;

ii. ali dejanski lastnik stranke brez upravičenega razloga ne more ali noče zagotoviti potrebnih informacij o skrbnem preverjanju strank, kadar to zahteva CASP, in sicer tako, da:

a) se namenoma izogiba neposrednemu stiku s CASP, bodisi osebno bodisi na daljavo;

b) poskuša prikriti dejanskega lastnika sredstev z vključevanjem zastopnikov ali sodelavcev, kot so ponudniki bodisi storitev zaupanja bodisi poslovnih storitev, v poslovne odnose ali transakcije;

c) molči ali poskuša zavajati preostale CASP glede vira sredstev ali vira kriptosredstev, ki se uporabljajo za pridobivanje kriptosredstev, ali namena transakcij;

iii. uporablja naslov IP ali mobilno napravo, ki je povezana z več strankami brez kakršnega koli očitnega ekonomskega razloga ali za katero je znano, da je povezana s potencialno nezakonitimi ali kriminalnimi dejavnostmi, ali pa se do računa kriptosredstev stranke dostopa z več naslovov IP brez kakršne koli očitne povezave s stranko;

iv. zagotavlja informacije, ki so nedosledne, tudi kadar naslov IP stranke ni skladen z drugimi informacijami o stranki, kot so informacije, ki so potrebne za spremljanje prenosa v skladu s členom 14(1) in (2) Uredbe (EU) 2023/1113, ali informacije o običajnem prebivališču, registraciji ali poslovnih dejavnostih (tako v času vstopa v poslovni odnos kot v času transakcije) stranke, informacije o virih sredstev ali viru kriptosredstev niso skladne z drugimi informacijami o skrbnem preverjanju strank ali splošnim profilom stranke;

v. uporablja naslov, lokacijo ali naslov IP, povezan z računi kriptosredstev, registriranimi za različne uporabnike, ki jih imajo pri enem ali več CASP;

vi. pogosto spreminja svoje osebne podatke ali plačilne instrumente brez očitnega razloga;

vii. pogosto prejema ali prenaša takšne zneske kriptosredstev z naslovov brez gostitelja, ki so tik pod pragom 1000 EUR, določenim v členu 14(5) in členu 16(2) Uredbe (EU) 2023/1113, kar zahteva preverjanje upravičenca ali originatorja;

viii. navaja, da je namen naložbe v začetno javno ponudbo žetonov ali v kriptosredstev ali produkt, ki ponuja nesorazmerno visok donos in ima sedež v jurisdikciji z visokim tveganjem ali pri katerem obstaja veliko indicev, povezanih z goljufijami, ali ki ni podprt z belo knjigo, ki se zahteva v skladu z Uredbo (EU) 2023/1114[7];

ix. izkazuje vedenje ali vzorce transakcij, ki niso v skladu s pričakovanji glede na vrsto stranke ali kategorijo tveganja, ki ji pripada, ali so nepričakovani glede na informacije, ki jih je stranka zagotovila CASP na začetku poslovnega odnosa ali med njim. Takšne okoliščine vključujejo situacije, ko stranka:

a) nepričakovano in brez očitnega razloga znatno poveča obseg ali vrednosti prenosa kriptosredstev ali kombiniranih prenosov po obdobju mirovanja;

b) izvaja transakcije z nenavadno visoko pogostostjo in obsegom kriptosredstev, kar ni v skladu z namenom in naravo poslovnega odnosa ter nima očitnega gospodarskega namena;

c) poveča limit transakcije v obsegu, ki ni sorazmeren s prijavljenim dohodkom stranke ali kako drugače presega pričakovani obseg dejavnosti;

x. izkazuje vedenje in vzorce, ki so nenavadni, ker vključujejo nepojasnjene prenose na naslove razpršene evidence ali račune kriptosredstev ali z njih v več jurisdikcijah brez očitnega poslovnega ali zakonitega namena;

xi. pri zamenjavi kriptosredstev v uradne valute in obratno stranka:

[7] Uredba (EU) št. 2023/1114 o trgih kriptosredstev ter spremembi uredb (EU) št. 1093/2010 in (EU) št. 1095/2010 ter direktiv 2013/36/EU in (EU) 2019/1937.

a) uporablja več bančnih ali plačilnih računov, kreditnih kartic ali predplačniških kartic za financiranje računa s kriptosredstvi;

b) uporablja bančni ali plačilni račun, kreditno kartico v imenu druge osebe, ki ni stranka, ne da bi imela očitne povezave s to osebo;

c) uporablja bančni ali plačilni račun, ki se nahaja v jurisdikciji, ki ni skladna z naslovom ali lokacijo, ki jo je stranka navedla;

d) uporablja več ponudnikov plačilnih storitev;

e) večkrat zahteva zamenjavo kriptosredstev v gotovino ali anonimni elektronski denar ali iz njiju;

f) uporablja protokole, ki povezujejo dve blokovni verigi, za zamenjavo kriptosredstev v druga kriptosredstva na različnih omrežjih, kot so Monero, Zcash ali podobna;

g) uporablja kriptobankomate na različnih lokacijah za ponavljajoče se prenose sredstev na bančni račun;

h) dvigne kriptosredstva od CASP na naslov brez gostitelja takoj po deponiranju kriptosredstev ali zamenjavi za različna kriptosredstva pri CASP;

xii. vlaga ali menjava kriptosredstva, ki si jih je izposodila prek platforme za medsebojno posojanje ali druge platforme za posojanje, ki ne spada na področje uporabe Uredbe (EU) 2023/1114 ali katerega koli drugega ustreznega regulativnega okvira v EU ali zunaj nje in ki je predvsem decentralizirana ali porazdeljena aplikacija brez pravne ali fizične osebe, ki ima nad njo nadzor ali vpliv nanjo;

xiii. neposredno ali posredno prejema ali pošilja kriptosredstva, ki so povezana s temnim omrežjem ali so rezultat nezakonitih dejavnosti;

xiv. vlaga ali zamenjuje kriptosredstva, ki sama zagotavljajo višjo stopnjo anonimnosti, ali pa stranka prejme kriptosredstva, ki so bila predmet dejavnosti za povečanje anonimnosti, zlasti postopkov, ki prikrivajo transakcijo v razpršeni evidenci ali vsebujejo druge značilnosti, podobne tistim iz točke a) smernice 21.5;

xv. večkrat prejema kriptosredstva z ali pošilja kriptosredstva na:

a) račun kriptosredstev prek CASP, ki ne spada na področje uporabe Uredbe (EU) 2023/1114 ali katerega koli drugega ustreznega regulativnega okvira v EU ali zunaj nje; ali za katerega velja regulativni in nadzorni okvir na področju PPDFT, ki je manj zanesljiv kot okvir, določen v Direktivi (EU) 2015/849;

b) več naslovov brez gostitelja ali več računov kriptosredstev, ki jih vodijo isti ali različni CASP, brez očitne ekonomske utemeljitve;

c) novo ustvarjen ali prej neaktiven račun kriptosredstev ali naslov razpršene evidence, ki ga ima tretja oseba;

d) naslove brez gostitelja na decentraliziranih platformah, ki vključujejo uporabo mešalnikov, tamblerjev in drugih tehnologij za povečanje zasebnosti, ki lahko prikrijejo finančno zgodovino, povezano z naslovom razpršene evidence, in vir sredstev za transakcijo, s čimer se zmanjša sposobnost CASP, da pozna svoje stranke ter izvaja učinkovite sisteme in kontrole PPDFT;

e) račun kriptosredstev kmalu po tem, ko je CASP sklenil poslovno razmerje, čemur sledi dvig ali prenos s takšnega računa v kratkem času brez očitne ekonomske utemeljitve;

f) račun kriptosredstev pogosto pod določenim pragom ali, v primeru prenosov na naslov brez gostitelja pod pragom 1 000 EUR, kot je opredeljeno v členu 14(5) in členu 16(2) Uredbe (EU) 2023/1113;

g) račun kriptosredstev z razdelitvijo transakcij na več transakcij, ki se pošljejo na več naslovov razpršene evidence z uporabo tehnik drobljenja;

xvi. izkorišča tehnološke napake ali okvare v svojo korist;

xvii. pojasnjuje, da so bila kriptosredstva, prenesena na CASP, pridobljena z nagradami za rudarjenje ali zamrznitev, vendar se zdi, da te nagrade niso sorazmerne s kriptosredstvi, ustvarjenimi s temi dejavnostmi.

21.6. K **zmanjšanju tveganja** lahko prispevajo naslednji dejavniki, kadar:

a) je stranka pri prejšnjih transakcijah s kriptosredstvi izpolnjevala zahteve po informacijah, določene v Uredbi (EU) 2023/1113 in podrobneje opredeljene v oddelku 4 Smernic organa EBA o pravilih glede prenosov [8], ter zagotovila informacije, ki omogočajo identifikacijo stranke ali možnost njenega preverjanja v primeru dvoma ali suma;

b) prejšnje transakcije kriptosredstev ne vzbujajo suma ali zaskrbljenosti, zahtevani produkt ali storitev pa je skladen s profilom tveganosti stranke;

c) stranka zahteva zamenjavo v uradno valuto ali iz nje in vir ali prejemnik sredstev je lasten bančni račun stranke pri kreditni instituciji v jurisdikciji, ki jo CASP ocenjuje kot nizko tveganje;

d) stranka zahteva zamenjavo, vir ali prejemnik kriptosredstev pa je njen lasten račun kriptosredstev ali naslov razpršene evidence, ki ga gosti CASP, ki ga ureja Uredba (EU) 2023/1114, ali CASP, ki ni CASP, ki ga ureja Uredba (EU) 2023/1114, ki je reguliran in nadzorovan zunaj EU v skladu z regulativnim okvirom, ki je tako strog

[8] Smernice o preprečevanju zlorabe sredstev in nekaterih prenosov kriptosredstev za namene pranja denarja in financiranja terorizma v skladu z Uredbo (EU) 2023/1113, [.... prosimo, vstavite številko teh smernic po sprejetju“, trenutno v posvetovanju (EBA/CP/2023/35)] (smernice o pravilih glede prenosov).

kot tisti iz Uredbe (EU) 2023/1114 in za katerega veljajo tako stroge zahteve glede PPDFT, kot so tiste iz Direktive (EU) 2015/849, ki ga je CASP uvrstil na beli seznam ali drugače določil kot nizko tveganje;

e) stranka zahteva zamenjavo, pri čemer se vir ali prejemnik kriptosredstev nanaša na plačila nizke vrednosti za blago in storitve na račun kriptosredstev ali z njega ali na naslov razpršene evidence, o katerem ni na voljo negativnih informacij;

f) prenosi stranke med dvema CASP ali CASP in CASP, ki ni CASP, ki ga ureja Uredba (EU) 2023/1114, za katerega veljajo predpisi in nadzor v EU ali za katerega drugače velja enako strog regulativni okvir, kot je predviden v Uredbi (EU) 2023/1114, in za katerega veljajo enako stroge zahteve glede PPDFT, kot so predvidene v Direktivi (EU) 2015/849.

Dejavniki tveganja, povezani z državami, ali geografski dejavniki tveganja

21.7. K **povečanju tveganja** lahko prispevajo naslednji dejavniki:

a) sredstva stranke, ki se zamenjajo za kriptosredstva, izvirajo iz osebnih ali poslovnih odnosov, ki vključujejo jurisdikcije, povezane z višjim tveganjem PD/FT;

b) izvorni ali prejemniški račun kriptosredstev ali naslov razpršene evidence je povezan z jurisdikcijo, povezano z večjim tveganjem PD/FT, ali jurisdikcijami/regijami, za katere je znano, da zagotavljajo financiranje ali podporo terorističnim dejavnostim ali da v njih delujejo skupine, ki izvajajo teroristična kazniva dejanja, ter jurisdikcijami, za katere veljajo finančne sankcije, embargo ali ukrepi, povezani s terorizmom, financiranjem terorizma ali širjenjem orožja;

c) stranka ali njen dejanski lastnik je rezident, ima sedež, posluje ali ima osebne ali poslovne odnose, ki vključujejo jurisdikcijo, povezano s povečanim tveganjem PD/FT;

d) poslovni odnos se vzpostavi prek CASP ali kriptobankomata, ki se nahaja v regiji ali jurisdikciji, ki je povezana z visoko stopnjo tveganja PD/FT;

e) stranka je prek odnosov s tretjimi osebami neposredno ali posredno vključena v dejavnosti rudarjenja kriptosredstev, ki potekajo v jurisdikciji z visokim tveganjem, ki jo je Evropska komisija določila v skladu s členom 9 Direktive (EU) 2015/849, ali v jurisdikciji, za katero veljajo omejevalni ukrepi ali ciljno usmerjene finančne sankcije.

21.8. K **zmanjšanju tveganja** lahko prispeva naslednji dejavnik:

a) če prenos prihaja z računa kriptosredstev ali naslova razpršene evidence, ki ga gosti CASP ali CASP, ki ni CASP, ki ga ureja Uredba (EU) 2023/1114, temveč v jurisdikciji, povezani z nizko stopnjo tveganja PD/FT, ali se prenese na ta račun ali naslov razpršene evidence.

Dejavniki tveganja, povezani z distribucijskimi potmi

21.9. K **povečanju tveganja** lahko prispevajo naslednji dejavniki:

a) poslovni odnos se vzpostavi z uporabo rešitev za sklepanje poslovnega razmerja s stranko na daljavo, ki niso v skladu s smernicami organa EBA za sklepanje poslovnega razmerja s stranko na daljavo[9];

b) pri instrumentu financiranja ni nobenih omejitev, na primer v primeru gotovine, čekov ali plačil s produkti elektronskega denarja, za katere velja izjema iz člena 12 Direktive (EU) 2015/849;

c) poslovno razmerje med CASP in stranko se vzpostavi prek ponudnika posredniških storitev v zvezi s kriptosredstvi, opredeljenega v smernici 9.20 zgoraj;

d) identifikacijo in preverjanje stranke izvaja CASP, ki se nahaja v jurisdikciji z visokim tveganjem, na podlagi dogovora o zunanjem izvajanju v skladu s členom 29 Direktive (EU) 2015/849;

e) nove distribucijske poti ali nova tehnologija, ki se uporablja za distribucijo kriptosredstev, ki še niso bili v celoti preizkušeni ali predstavljajo povečano stopnjo tveganja PD/FT;

f) poslovno razmerje se vzpostavi prek kriptobankomatov, kar povečuje tveganje zaradi uporabe gotovine.

21.10. K **zmanjšanju tveganja** lahko prispeva naslednji dejavnik:

a) kadar se CASP zanaša na ukrepe skrbnega preverjanja strank, ki jih izvaja tretja oseba v skladu s členom 26 Direktive (EU) 2015/849 in kadar ima ta tretja oseba sedež ali naslov v EU.

Ukrepi

21.11. CASP bi morali zagotoviti, da so sistemi, ki jih uporabljajo za ugotavljanje in odpravljanje tveganj PD/FT, skladni z merili iz naslova I teh smernic. Zaradi svojih poslovnih modelov bi morali zlasti zagotoviti, da imajo na voljo ustrezna in učinkovita orodja za spremljanje, vključno z orodji za spremljanje transakcij in orodji za napredno analitiko. Obseg takih orodij je določen glede na naravo in obseg dejavnosti CASP, vključno z vrsto kriptosredstev, ki so na voljo za trgovanje ali izmenjavo. CASP bi morali zagotoviti tudi, da so ustrezni zaposleni deležni specializiranega usposabljanja, da bi dobro razumeli kriptosredstva in tveganja PD/FT, ki jim je CASP lahko izpostavljen.

[9] Smernice EBA za uporabo rešitev za sklepanje poslovnega razmerja s stranko na daljavo v skladu s členom 13(1) Direktive (EU) 2015/849 (EBA/GL/2022/15).

Okrepljeno skrbno preverjanje strank

21.12. Kadar se tveganje, povezano s poslovnim odnosom ali občasno transakcijo, poveča, morajo CASP uporabiti okrepljene ukrepe skrbnega preverjanja strank v skladu s členom 18 Direktive (EU) 2015/849 in kot je določeno v naslovu I teh smernic. Poleg tega bi morali CASP po potrebi izvajati ustrezne okrepljene ukrepe skrbnega preverjanja strank, ki so navedeni spodaj, odvisno od izpostavljenosti poslovnega odnosa tveganju:

a) preveriti identiteto stranke in dejanskega lastnika na podlagi več zanesljivih in neodvisnih virov;

b) identificirati in preveriti identiteto večinskih delničarjev, ki ne ustrezajo opredelitvi dejanskih lastnikov v skladu s členom 3 Direktive (EU) 2015/849, ali katerih koli fizičnih oseb, pooblaščenih za upravljanje računa kriptosredstva ali naslova razpršene evidence v imenu stranke ali dajati navodila za prenos ali zamenjavo kriptosredstev ali drugih storitev v zvezi s temi kriptosredstvi;

c) pridobiti več informacij o stranki ter naravi in namenu poslovnega odnosa za oblikovanje popolnejšega profila stranke, na primer z iskanjem po javnih virih, iskanjem negativnega medijskega poročanja ali naročilom poročila z obveščevalnimi podatki, ki ga pripravi tretja oseba. Primeri informacij, ki jih CASP lahko zahtevajo glede na izpostavljenost tveganju poslovnega razmerja, vključujejo informacije o:

   i. naravi poslovanja ali zaposlitvi stranke;

   ii. viru premoženja in sredstvih stranke, ki se zamenjajo za kriptosredstva, da bi se ustrezno prepričali o njihovi legitimnosti;

   iii. viru kriptosredstev stranke, ki se zamenjajo za uradne valute, vključno s tem, kdaj in kje so bila kupljena;

   iv. namenu transakcije, vključno s prejemniki prenosa kriptosredstev, kadar je to primerno;

   v. morebitnih povezavah, ki bi jih stranka lahko imela z drugimi jurisdikcijami (sedeži, operativne zmogljivosti, podružnice itd.) ali posamezniki, za katere je znano, da pomembno vplivajo na dejavnosti stranke;

   vi. zahtevati ali pridobiti podatke o transakcijah stranke s kriptosredstvi in, če je stranka CASP, njeno zgodovino trgovanja znotraj sistema;

d) pridobiti dokazila o viru sredstev, viru premoženja ali viru kriptosredstev v zvezi s tistimi transakcijami, ki predstavljajo večje tveganje;

e) povečati pogostost spremljanja transakcij s kriptosredstvi. Pri vseh transakcijah bi bilo treba spremljati nepričakovano vedenje, vzorce in kazalnike sumljive dejavnosti, pri tem pa upoštevati tudi stranke, s katerimi stranka posluje;

f) pogosteje pregledovati in po potrebi posodabljati informacije, podatke in dokumentacijo, zlasti v primeru sprožilnega dogodka;

g) če je tveganje, povezano z odnosom, še posebej visoko, bi morali CASP poslovni odnos pregledati pogosteje;

h) pogosteje ali bolj poglobljeno oceniti dejavnosti, ki se izvajajo prek računov kriptosredstev stranke, z uporabo orodij za preiskovanje kriptosredstev;

i) kadar ima stranka več naslovov razpršene evidence ali omrežij blokovnih verig, bi moral CASP te naslove povezati s stranko;

j) povečati pogostost spremljanja naslovov IP stranke in preverjanja teh naslovov glede na naslove IP, ki jih uporabljajo druge stranke;

k) pridobiti potrditev o ravni znanja in razumevanja stranke v zvezi s kriptosredstvi, da se doseže raven zagotovila, da se stranka ne uporablja kot denarna mula;

l) kadar vzorec dvigov ali odkupov ni v skladu s profilom stranke ali naravo in namenom poslovnega odnosa, bi moral CASP dodati dodatne ukrepe za zagotovitev, da dvig ali odkup zahteva stranka in ne tretja oseba. To je zlasti pomembno za visoko tvegane ali starejše ali ranljivejše odjemalce;

m) pridobiti potrditev, da je naslov brez gostitelja, iz katerega se prejme prenos, pod nadzorom ali lastništvom stranke CASP.

21.13. CASP bi morali za transakcije uporabljati napredna analitična orodja na podlagi občutljivosti na tveganje kot dodatek k standardnim orodjem za spremljanje transakcij. CASP bi morali uporabljati napredna analitična orodja za ocenjevanje tveganja, povezanega s transakcijami, zlasti transakcijami, ki vključujejo naslove brez gostitelja, saj jim omogočajo sledenje preteklih transakcij in odkrivanje morebitnih povezav s kriminalnimi dejavnostmi, osebami ali subjekti.

21.14. V zvezi s poslovnimi odnosi ali transakcijami, ki vključujejo države z visokim tveganjem, ki niso članice EU, bi morali upoštevati smernice iz naslova I teh smernic.

Poenostavljeno skrbno preverjanje strank

21.15. V razmerah z nizkim tveganjem, ki so bile kot take opredeljene na podlagi ocene tveganja PD/FT, ki jo je CASP izvedel v skladu s temi smernicami, in v obsegu, ki ga dovoljuje nacionalna zakonodaja, lahko CASP uporabijo ukrepe poenostavljenega skrbnega preverjanj, ki lahko vključujejo:

a) za stranke, za katere velja zakonska ureditev licenciranja in regulativna ureditev v EU ali državi, ki ni članica EU, preverjanje njihove identitete na podlagi dokazil, ki potrjujejo, da za stranko velja ta ureditev, na primer z iskanjem v javnem registru regulatorja;

b) posodabljanje informacij, podatkov ali dokumentacije o skrbnem preverjanju strank samo, če obstajajo posebni sprožilni dogodki, na primer kadar stranka zahteva nov produkt ali produkt z višjim tveganjem ali v primeru sprememb v ravnanju stranke ali profilu transakcij, ki kažejo, da tveganje, povezano z odnosom,

ni več nizko, pri čemer se upoštevajo obdobja posodobitve, določena v nacionalni zakonodaji;

c) zmanjšanje pogostosti spremljanja transakcij za produkte, ki vključujejo ponavljajoče se transakcije.

Vodenje evidenc

21.16. Kadar so informacije o strankah in transakcijah na voljo v razpršeni evidenci, se CASP za vodenje evidenc ne bi smeli zanašati na razpršeno evidenco, temveč bi morali sprejeti ukrepe za izpolnjevanje svojih odgovornosti glede vodenja evidenc v skladu z Direktivo (EU) 2015/849 ter smernicami 5.1 in 5.2, opisanimi zgoraj. CASP bi morali vzpostaviti postopke, ki jim omogočajo, da naslov razpršene evidence povežejo z zasebnim ključem, ki ga nadzira fizična ali pravna oseba.