Na podlagi petega odstavka 35. člena Zakona o preprečevanju pranja denarja in financiranja terorizma (Uradni list RS, št. Uradni list RS, št. 48/22 in 145/22) izdaja minister, pristojen za finance, v soglasju z ministrom, pristojnim za informacijsko družbo, naslednji

P R A V I L N I K
o tehničnih pogojih, ki jih morajo izpolnjevati varni daljinsko upravljani ali elektronski postopki ter sredstva za identifikacijo

1. člen
(vsebina pravilnika)

(1) S tem pravilnikom se določajo pogoji in zahteve, ki jih morajo izpolnjevati varni daljinsko upravljani ali elektronski postopki in sredstva za identifikacijo iz 35. člena Zakona o preprečevanju pranja denarja in financiranja terorizma (Uradni list RS, št. Uradni list RS, št. 48/22 in 145/22; v nadaljnjem besedilu: ZPPDFT-2), ter način njihove uporabe za namen ugotavljanja in preverjanja istovetnosti strank pri izvajanju pregleda stranke kot ukrepa za preprečevanje pranja denarja in financiranja terorizma s strani zavezancev iz 4. člena ZPPDFT-2.

(2) Določbe tega pravilnika se uporabljajo za vsakega posameznika, ki je v postopku ugotavljanja in preverjanja istovetnosti, ne glede na to, ali je posameznik sam stranka ali le zakoniti zastopnik oziroma pooblaščenec stranke.

2. člen
(izrazi)

Posamezni izrazi, uporabljeni v tem pravilniku, pomenijo:

1. »daljinsko upravljani ali elektronski postopki za identifikacijo« so postopki ugotavljanja in preverjanja istovetnosti strank brez osebne navzočnosti stranke z uporabo daljinsko upravljanih ali elektronskih sredstev iz 35. člena ZPPDFT-2;
2. »daljinsko upravljana ali elektronska sredstva za identifikacijo« so tehnična in strojna oprema, s pomočjo katere se izvajajo daljinsko upravljani ali elektronski postopki za identifikacijo;
3. »uradni osebni dokument« je uradni osebni dokument, opremljen s fotografijo, s katere je jasno prepoznavna slika obraza osebe, v katerem so navedeni podatki vsaj o njenem osebnem imenu in datumu rojstva;
4. »elektronska naprava« je elektronska naprava kot na primer pametni telefon, tablični, namizni ali prenosni računalnik, ki ima zmožnost zajemanja digitalnih barvnih fotografij in posnetkov z ustrezno kakovostjo in podpira naprednejše računalniške sposobnosti ter funkcije povezljivosti preko spletne povezave in omogoča komunikacijo stranke z uporabniškim vmesnikom;
5. »uporabniški vmesnik« je digitalno okolje, do katerega stranka dostopa z elektronsko napravo in omogoča stranki interakcijo, komunikacijo in izmenjavo podatkov v daljinsko upravljanem ali elektronskem postopku za identifikacijo;
6. »oddaljen zajem« je zajem fotografije, sekvenc fotografij ali posnetka obraza stranke ali uradnega osebnega dokumenta, ki ga stranka opravi z uporabo elektronske naprave.

3. člen
(tehnične zahteve daljinsko upravljanih ali elektronskih postopkov za identifikacijo)

(1) Daljinsko upravljani ali elektronski postopki za identifikacijo morajo imeti implementirane vsaj naslednje varnostne mehanizme, ki omogočajo ugotavljanje in preverjanje istovetnosti strank ter zaznavo morebitnih zlorab v postopku ugotavljanja in preverjanja istovetnosti strank:

a. preverjanje pristnosti fotografije uradnega osebnega dokumenta ter zaznavanje kakršnih koli digitalnih ali analognih manipulaciji pred ali med postopkom oddaljenega zajemanja posnetka;

b. preverjanje pristnosti zajetih fotografij obraza stranke z zmožnostjo zanesljivega zaznavanja, ali je zajeta fotografija stranke posneta živemu posamezniku, ki je prisoten v času oddaljenega zajema fotografij na elektronski napravi, vključno z mehanizmi za zaznavo kakršnihkoli digitalnih ali analognih zlorab oziroma manipulaciji digitalnih posnetkov pred ali med postopkom oddaljenega zajemanja posnetka obraza posameznika;

c. preverjanje biometričnih značilnosti obraza stranke iz zajetih fotografij oziroma posnetkov ter primerjava le-teh z biometričnimi lastnostmi fotografije vsebovane na uradnem osebnem dokumentu;
d. preverjanje ujemanja vnesenih podatkov s podatki iz uradnega osebnega dokumenta;
e. razpoznava in preverjanje obstoja optičnih zaščitnih znakov, vključno s holografskimi ali drugimi enakovrednimi zaščitnimi elementi na uradnem osebnem dokumentu (na primer varnostne nitke, variabilne barve in podobno);
f. preverjanje formalnih znakov uradnega osebnega dokumenta in njihovo ujemanje glede na vrsto uradnega osebnega dokumenta (grafična zasnova, velikost znakov, razmik med znaki, tipografija in podobno);
g. razpoznava identifikacijskih oznak uradnega osebnega dokumenta, preverjanje veljavnosti uradnega osebnega dokumenta in pravilnosti alfanumeričnih znakov njegove serijske številke;
h. preverjanje pravilnosti vizualnega izgleda fotografije uradnega osebnega dokumenta, nepoškodovanosti laminacije, ki obdaja uradni osebni dokument, ali drugih zaščitnih znakov, ki izkazujejo njegovo nepoškodovanost;
i. preverjanje logične doslednosti podatkov, ki izhajajo iz dokumenta (na primer pravilnost datuma izdaje in poteka veljavnosti, pravilnost rojstnega datuma, njihovo medsebojno ujemanje in podobno).

(2) Varnostni mehanizmi iz prejšnjega odstavka se lahko izvedejo s pomočjo avtomatiziranih sredstev ustrezne programske podpore.

(3) Daljinsko upravljana ali elektronska sredstva za identifikacijo morajo imeti implementirane najmanj naslednje varnostne mehanizme, ki preprečujejo nedovoljeno dostopanje in poseganje v informacijski sistem, na katerem so shranjeni ali evidentirani podatki strank, zajetih iz daljinsko upravljanih ali elektronskih postopkov za identifikacijo:
a. vzpostavitev varnostnih mehanizmov, ki zagotavljajo varen prenos podatkov s šifriranjem celotne komunikacijske poti (šifriranje med končnimi točkami), tako da prenosa ni mogoče prestreči. Za šifriranje je potrebno uporabiti šifrirne algoritme in postopek upravljanja s ključi, za katere niso znane varnostne pomanjkljivosti, in šifrirne ključe temu ustreznih dolžin;
b. vzpostavitev varnostnih mehanizmov za varovanje podatkov, pridobljenih med daljinsko upravljanim ali elektronskim postopkom za identifikacijo, ki zagotavljajo ustrezno zaščito pred nedovoljenim dostopom in zlorabo;
c. vzpostavitev učinkovitih varnostnih kontrol za onemogočanje nedovoljenih dostopov, razkritij, poškodovanj, spreminjanj ali brisanj podatkov, kar zajema tudi vzpostavitev ustreznega sistema evidentiranja dogodkov (revizijska sled).

4. člen
(način in postopek preverjanja)

(1) Zavezanec, ki izvaja ugotavljanje in preverjanje istovetnosti strank z daljinsko upravljanimi ali elektronskimi postopki, se mora prepričati:
a. o avtentičnosti in veljavnosti uradnega osebnega dokumenta fizične osebe,
b. o pristnosti in dejanskem obstoju stranke in
c. o ujemanju posredovanih osebnih podatkov stranke s podatki iz uradnega osebnega dokumenta ter ujemanju zajetih fotografij obraza stranke s fotografijo osebe na uradnem osebnem dokumentu.

(2) Zavezanec za namen ugotavljanja in preverjanja dejstev in okoliščin iz prejšnjega odstavka vzpostavi postopek interakcije stranke z uporabniškim vmesnikom, do katerega stranka dostopa z elektronsko napravo, pri čemer se postopek izvaja v realnem času brez prekinitev in vključuje vsaj naslednje elemente in funkcije:
a. vnos podatkov stranke v uporabniški vmesnik, in sicer vsaj podatkov o njenem osebnem imenu in datumu rojstva, o vrsti, datumu izdaje in datumu prenehanja osebnega dokumenta ter o nazivu izdajatelja uradnega osebnega dokumenta;
b. oddaljen zajem fotografij prednje in zadnje, oziroma katere koli druge strani uradnega osebnega dokumenta, ki vsebuje za preverjanje relevantne podatke, preko uporabniškega vmesnika ali nalaganje teh fotografij v uporabniškem vmesniku;
c. oddaljen zajem fotografije obraza stranke z elektronsko napravo preko uporabniškega vmesnika ali nalaganje fotografije obraza stranke v uporabniškem vmesniku.

(3) Fotografije uradnega osebnega dokumenta ter fotografije obraza stranke morajo biti posnete na način, ki omogoča razpoznavo vseh elementov, potrebnih za izvajanje varnostnih mehanizmov iz prvega odstavka 3. člena tega pravilnika.

(4) Zavezanec imenuje eno ali več oseb, ki za zavezanca spremljajo in nadzorujejo postopek ugotavljanja in preverjanja istovetnosti strank v skladu s tem pravilnikom. Pri tem takšna oseba oziroma osebe opravljajo preglede, s katerimi ob upoštevanju varnostnih mehanizmov iz prvega odstavka 3. člena tega pravilnika in zajetih podatkov iz drugega odstavka tega člena preverjajo, ali so dejstva ter okoliščine iz prvega odstavka tega člena ugotovljena in preverjena, ter dokumentirajo izvedbo teh pregledov.

5. člen
(obveznost prekinitve identifikacije)

(1) Postopek identifikacije z daljinsko upravljanimi ali elektronskimi postopki ter sredstvi je treba prekiniti oziroma identifikacijo zavrniti vedno, ko:

a. svetlobne ali tehnične zmogljivosti elektronske naprave pri stranki ne omogočajo oddaljenega zajema fotografij in prenosa podatkov v uporabniški vmesnik na način, ki bi bil primeren za ugotavljanje in preverjanje istovetnosti stranke v skladu s četrtim odstavkom prejšnjega člena;

b. je pri analiziranju zajetih podatkov na podlagi četrtega odstavka prejšnjega člena zaznano kakršno koli neujemanje, nedoslednost ali znak zlorabe, ki zavezancu onemogoča, da se zanesljivo prepriča o resničnosti dejstev in okoliščin iz prvega odstavka prejšnjega člena;

c. obstaja negotovost glede istovetnosti stranke;

d. obstaja verjetnost morebitnega vpliva tretjih oseb na izraženo voljo stranke in posledično veljavnost privolitve.

(2) Če nastopijo okoliščine iz 4. ali 5. točke prvega odstavka 22. člena ZPPDFT-2, zavezanec nadaljuje izvedbo identifikacije in po končani izvedbi prouči, ali so nastopile okoliščine, ki določajo obvezno sporočanje podatkov Uradu Republike Slovenije za preprečevanje pranja denarja po 76. členu ZPPDFT-2.

6. člen
(usposobljenost izvajalca)

(1) Oseba ali osebe iz četrtega odstavka 4. člena morajo biti ustrezno usposobljene in zanesljive.

(2) Ustrezna usposobljenost predpostavlja najmanj:

a. poznavanje predpisov s področja preprečevanja pranja denarja in financiranja terorizma ter varstva osebnih podatkov;

b. razumevanje tehničnih zahtev in delovanja naprav, s katerimi se izvede identifikacija z daljinsko upravljanimi ali elektronskimi postopki ter sredstvi;

c. poznavanje značilnosti uradnih osebnih dokumentov;

d. poznavanje praktične izvedbe identifikacije z daljinsko upravljanimi ali elektronskimi postopki ter sredstvi, vključno s preverjanjem zaščitnih znakov uradnega osebnega dokumenta oziroma uporabo ustrezne programske podpore za njihovo preverjanje, ugotavljanjem verodostojnosti podatkov ter zaznavo neujemanj, nedoslednosti ali znakov zlorabe v postopku izvedbe te identifikacije.

(3) Zavezanec ali oseba, ki jo zavezanec pooblasti, dokumentira izvedbo usposabljanja tako, da je možno ugotoviti ustreznost usposabljanja.

7. člen
(predhodno soglasje stranke)

(1) Na začetku postopka identifikacije stranke se stranko, ki je pristopila k takemu načinu pregleda, pozove, da poda izrecno soglasje k izvedbi celotnega postopka in hrambi podatkov v skladu z drugim odstavkom 8. člena tega pravilnika.

(2) Za veljavnost soglasja iz prejšnjega odstavka veljajo določbe o pogojih za veljavnost privolitve, kot jih opredeljuje 7. člen Splošne Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z

dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L št. 119 z dne 4. 5. 2016, str. 1), zadnjič popravljene s Popravkom (UL L št. 127 z dne 23. 5. 2018, str. 2; v nadaljnjem besedilu: Splošna uredba).

(3) Če stranka na začetku postopka ne poda soglasja iz prvega odstavka tega člena, se identifikacija stranke prekine in se stranko napoti na drug način ugotavljanja in preverjanja njene istovetnosti, ki je v skladu z ZPPDFT-2.

8. člen
(osebni podatki in hramba podatkov)

(1) Osebni podatki, dokumentacija in posnetki, ki se zbirajo in obdelajo z identifikacijo z daljinsko upravljanimi ali elektronskimi postopki ter sredstvi na podlagi tega pravilnika, vključno z zajetimi podatki iz drugega odstavka 4. člena tega pravilnika in pregledi iz četrtega odstavka 4. člena tega pravilnika, se zbirajo in obdelajo za namen preprečevanja in odkrivanja pranja denarja in financiranja terorizma ter zanje v celoti veljajo določbe 139., 140., 141. in 142. člena ZPPDFT-2, s katerimi je določena uporaba pridobljenih podatkov, dokumentacije in posnetkov ter obveščanje posameznika o obdelavi osebnih podatkov.

(2) Zavezanca glede hrambe podatkov iz prvega odstavka prejšnjega člena zavezuje določba 142. člena ZPPDFT-2 o hrambi podatkov pri zavezancu.

9. člen
(izvedba identifikacije po zunanjem izvajalcu)

(1) Če zavezanec izvedbo identifikacije z daljinsko upravljanimi ali elektronskimi postopki ter sredstvi naroči pri zunanjem izvajalcu, je odgovoren za to, da zunanji izvajalec izvede vse zaščitne ukrepe tako, da po obsegu in kakovosti ustrezajo določbam tega pravilnika. Končno odgovornost za izpolnjevanje določb tega pravilnika nosi zavezanec, za katerega identifikacijo izvede zunanji izvajalec.

(2) Zavezanec mora pri sklenitvi naročila , med trajanjem in pri odpovedi naročila pri zunanjem izvajalcu ravnati kot dober gospodar s potrebno skrbnostjo ter pisno določiti obveznosti, ki izhajajo iz naročila za izvedbo identifikacije z daljinsko upravljanimi ali elektronskimi postopki ter sredstvi pri zunanjem izvajalcu. Pri tem mora zavezanec za ustrezno ureditev pogodbene obdelave osebnih podatkov upoštevati tudi določbe o obdelavi osebnih podatkov s strani obdelovalcev, kot so opredeljene v 28. členu Splošne uredbe.

(3) Okoliščina, da za zavezanca identifikacijo z daljinsko upravljanimi ali elektronskimi postopki ter sredstvi izvede zunanji izvajalec, ne sme vplivati na kakovost izvedbe notranjih kontrol ali ovirati izvedbe nadzora s strani nadzornih organov.

(4) Zunanji izvajalec zavezanca redno obvešča o vseh spremembah, ki vplivajo na izvajanje identifikacije stranke.

(5) Zavezanec in zunanji izvajalec s sporazumom dogovorita način prenosa podatkov v primeru, da zunanji izvajalec preneha z izvajanjem identifikacije stranke.

10. člen
(odgovornost)

Zavezanec, ki izvaja daljinsko upravljan ali elektronski postopek za identifikacijo, je odgovoren za škodo, ki je namenoma ali iz malomarnosti povzročena fizični ali pravni osebi zaradi neizpolnjevanja obveznosti po tem pravilniku.

KONČNA DOLOČBA

11. člen
(začetek veljavnosti)

Ta pravilnik začne veljati 15. dan po objavi v Uradnem listu Republike Slovenije.

Št.
Ljubljana, dne …

Minister za finance

Obrazložitev:

Podlaga za sprejem pravilnika je peti odstavek 35. člena ZPPDFT-2, ki določa, da minister za finance v soglasju z ministrom, pristojnim za informacijsko družbo, podrobneje določi zahteve in pogoje, ki jih morajo izpolnjevati identifikacijska sredstva in postopki ugotavljanja in preverjanja istovetnosti strank iz tega člena. Zakon o preprečevanju pranja denarja in financiranja terorizma je omogočal 3 načine identifikacije strank, in sicer z osebno navzočnostjo, na podlagi videoelektronske identifikacije ter na podlagi sredstva za elektronsko identifikacijo.

ZPPDFT-2 je na tem področju uvedel dve novosti, in sicer možnost, da se opravi pregled brez osebne navzočnosti stranke, v primeru da je ugotovljeno neznatno tveganje za pranje denarja in financiranje terorizma (32. člen ZPPDFT -2). Druga novost je, da se pod določenimi pogoji omogočijo tudi drugi varni daljinsko upravljani ali elektronski postopki oziroma sredstva za identifikacijo, s čimer se omogoča uporaba novih tehnologij pri identifikaciji strank zavezancev. V Pravilniku so podrobneje določene zahteve in pogoji, ki jih morajo izpolnjevati identifikacijska sredstva in postopki ugotavljanja in preverjanja istovetnosti strank iz tega člena. Ker gre za nove tehnologije, sta bistveni lastnosti, ki ju pravilnik zasleduje, varnost in zanesljivost, zato da je v najvišji možni meri mogoče izključiti možnost zlorabe teh postopkov in sredstev.

Pravilnik podrobneje ureja tehnične zahteve daljinsko upravljanih ali elektronskih postopkov za identifikacijo in sicer določa minimalne varnostne mehanizme, z namenom, da se onemogoči zlorabe glede identifikacije strank ter da se zgotovi varstvo osebnih podatkov strank. Gre za minimalen nabor mehanizmov, ki morajo biti zagotovljeni. Zaradi tveganj zlorab, so pogoji za opravljanje take identifikacije določeni dokaj strogo.

Pravilnik nadalje določa, da se mora zavezanec prepričati o avtentičnosti in veljavnosti uradnega osebnega dokumenta stranke, o pristnosti in dejanskem obstoju stranke ter o ujemanju podatkov. Pravilnik zahteva izvajanje tega mehanizma v sklopu postopka za identifikacijo, torej tudi po vnosu podatkov oziroma zajemu iz drugega odstavka 4. člena pravilnika, vendar pred samim zaključkom identifikacije.

Točka c. prvega odstavka 4. člena pravilnika zajema preverjanje biometričnih značilnosti iz zajetih posnetkov, medtem ko točka d. zajema preverjanje ujemanja (drugih) podatkov, ki so vneseni prek uporabniškega vmesnika.

Zavezanci lahko izvajajo določbe tega pravilnika s pomočjo več avtomatiziranih sredstev.

Nadalje so določene zahteve za usposobljenost izvajalcev ter našteti primeri, v katerih je potrebno postopek identifikacije prekiniti oziroma zavrniti. V nekaterih primerih namreč lahko algoritem identifikacijo izvede do konca, vendar njen rezultat ni pozitiven.

Tovrstno identifikacijo je mogoče izvesti tudi po zunanjem izvajalcu.

Pravilnik določa še odgovornost izvajalca za škodo, ki jo povzroči zaradi nespoštovanja določb navedenega pravilnika. Na ta način se zasleduje cilj čim višje varnosti za uporabnike tovrstnih storitev.