

Na podlagi sedmega odstavka 21. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14, 55/17 in 163/22) izdaja Vlada Republike Slovenije

UREDBO

o izvajanju uredbe (EU) o digitalni operativni odpornosti za finančni sektor

1. člen (vsebina)

S to uredbo se določajo pristojni organi, način opravljanja nadzora, ukrepi pristojnih organov in globe v zvezi z izvajanjem Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in sprememb uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/2011 (UL L št. 333 z dne 27. 12. 2022, str. 1-79), zadnjič spremenjene z Delegirano uredbo Komisije (EU) 2024/1505 z dne 22. februarja 2024 o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z določitvijo zneska nadomestil za nadzor, ki jih glavni nadzornik zaračuna ključnim tretjim ponudnikom storitev IKT, in načina plačila teh nadomestil (UL L št. 2024/1505 z dne 30. 5. 2024), (v nadaljnjem besedilu: Uredba 2022/2554/EU).

2. člen (pomen izrazov)

Izrazi, uporabljeni v tej uredbi, pomenijo enako kot izrazi opredeljeni v Uredbi 2022/2554/EU.

3. člen (organi, pristojni za izvajanje Uredbe EU 2022/2554)

(1) Pristojni organi za izvajanje Uredbe 2022/2554/EU in te uredbe so organi, ki so določeni v skladu s 46. členom Uredbe 2022/2554/EU, in sicer za subjekte navedene pod točko:

- (a) in (b) Banka Slovenije, razen glede nalog in pristojnosti bonitetnega nadzora, za katere je v skladu z Uredbo 1024/2013/EU pristojna in odgovorna Evropska centralna banka,
- (c), (d) razen subjektov nadzora iz prve in tretje alineje tega odstavka, (e), (f), (g), (h), (i), (j), (n), (o), (p) in (q) Agencija za trg vrednostnih papirjev,
- (k), (l) in (m) je Agencija za zavarovalni nadzor.

(2) Pristojni organi iz prvega odstavka tega člena, pri nalogah povezanih s penetracijskim testiranjem na podlagi analize groženj v finančnem sektorju, lahko sporazumno sodelujejo z Uradom Republike Slovenije za informacijsko varnost (v nadaljevanju: URSIV).

4. člen (poročanje o IKT incidentih in kibernetičnih grožnjah)

(1) Finančni subjekti iz drugega odstavka 2. člena Uredbe 2022/2554/EU, o večjih incidentih, povezanih z IKT, v skladu z 19. členom Uredbe 2022/2554/EU, poročajo pristojnemu organu te uredbe.

(2) Finančni subjekti iz drugega odstavka 2. člena Uredbe 2022/2554/EU, ki jih v skladu z 19. členom Uredbe 2022/2554/EU določijo pristojni organi iz te uredbe, začetno uradno obvestilo in vsako poročilo iz četrtega odstavka 19. člena Uredbe 2022/2554/EU predložijo tudi pristojni skupini za odzivanje na incidente na področju računalniške varnosti (v nadaljevanju: CSIRT), v skladu z zakonom, ki ureja informacijsko varnost.

(3) Centralno depotne družbe in ponudniki storitev v zvezi s kriptosredstvi ali izdajatelji žetonov vezanih na sredstva, ki niso kreditne ali plačilne institucije in družbe za izdajo elektronskega denarja, o večjih incidentih, povezanih z IKT v skladu z 19. členom Uredbe 2022/2554/EU, poročajo Agenciji za trg vrednostnih papirjev.

(4) Kreditne institucije, plačilne institucije ter družbe za izdajo elektronskega denarja, o večjih incidentih, povezanih z IKT, v skladu z 19. členom Uredbe 2022/2554/EU, poročajo Banki Slovenije.

(5) Finančni subjekti lahko poleg obvezne priglasitve večjega incidenta, pristojni organ te uredbe in CSIRT prostovoljno obvestijo o pomembnih kibernetičnih grožnjah, če menijo, da je grožnja relevantna za finančni sistem, uporabnike storitev ali stranke, in jim predložijo ustrezne informacije.

(6) Pristojni organi te uredbe, o večjih incidentih, povezanih z IKT, s katerimi so bili seznanjeni na podlagi prvega, drugega, tretjega ali četrtega odstavka tega člena, tedensko poročajo CSIRT.

(7) Ne glede na rok iz prejšnjega odstavka, pristojni organi te uredbe, brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah od priglasitve, obvestijo CSIRT o zaznavi takšnega incidenta v primeru, da je incident iz prvega odstavka tega člena finančnemu subjektu:

- povzročil ali bi mu lahko povzročil znatne operativne motnje pri opravljanju storitev ali finančne izgube;
- vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

5. člen **(način opravljanja nadzora)**

(1) Pristojni organi iz prvega odstavka 3. člena te uredbe opravljajo nadzor nad izvajanjem te uredbe in Uredbe 2022/2554/EU:

- a) s spremljanjem, zbiranjem in preverjanjem objavljenih informacij in poročil ter obvestil institucij, ki morajo na podlagi Uredbe 2022/2554/EU poročati pristojnim organom,
- b) s pridobivanjem informacij in opravljanjem nadzora v skladu z drugim odstavkom 50. člena Uredbe 2022/2554/EU,
- c) z izvajanjem nalog glede izvajanja naprednega testiranja orodij, sistemov in postopkov IKT na podlagi penetracijskega testiranja na podlagi analize groženj oziroma s sporazumnim prenosom nekaterih ali vseh nalog na drug javni organ v finančnem sektorju v skladu z 10. točko 26. člena Uredbe 2022/2554/EU,
- d) z izrekanjem ukrepov iz 6. člena te uredbe,

- e) s sodelovanjem z glavnim nadzornikom in drugimi pristojnimi organi v nadzorniškem forumu za nadzor ključnih tretjih ponudnikov storitev IKT v skladu s prvim odstavkom 32. člena Uredbe 2022/2554/EU.

(2) Pristojni organi iz prvega odstavka 3. člena te uredbe, opravljajo nadzor iz prejšnjega odstavka in izrekajo nadzorne ukrepe v skladu z določbami te uredbe, Uredbe 2022/2554/EU, s smiselno uporabo določb o opravljanju nadzora zakona, ki ureja bančništvo, zakona, ki ureja plačilne storitve, storitve izdajanja elektronskega denarja in plačilne sisteme, zakona, ki ureja trg finančnih instrumentov oziroma zakona, ki ureja zavarovalništvo.

6. člen **(ukrepi pristojnih organov)**

(1) Pristojni organi iz prvega odstavka 3. člena te uredbe, za doseg namena nadzora iz prejšnjega člena in ob ugotovitvi kršitev Uredbe 2022/2554/EU ali te uredbe uporabijo nabor ukrepov:

- iz četrtega odstavka 50. člena in ob upoštevanju 51. člena Uredbe 2022/2554/EU
- izrečejo globe v skladu z 9. členom te uredbe.

(2) Pristojni organi se za izvajanje nadzornih aktivnosti po potrebi posvetujejo in izmenjajo informacije z enotno kontaktno točko, vzpostavljeno v skladu z zakonom, ki ureja informacijsko varnost in pristojno skupino CSIRT iz četrtega odstavka 4. člena te uredbe.

(3) Pristojni organi iz prvega odstavka 3. člena te uredbe v skladu s 54. členom Uredbe 2022/2554/EU na svojih uradnih spletiščih objavijo informacije v zvezi z ukrepi nadzora in sankcijami zaradi prekrška, ki jih izrečejo zaradi kršitev določb Uredbe 2022/2554/EU.

III. NADOMESTILO ZA OPRAVLJANJE NADZORA

7. člen **(tarifa)**

Agencija za trg vrednostnih papirjev v tarifi, ki jo izda v skladu z zakonom, ki ureja trg finančnih instrumentov, Agencija za zavarovalni nadzor v tarifi, ki jo izda v skladu z zakonom, ki ureja zavarovalništvo ter Banka Slovenija v tarifi, ki jo izda v skladu z zakonom, ki ureja delovanje Banke Slovenije, zakonom, ki ureja bančništvo, in zakonom, ki ureja plačilne storitve, storitve izdajanja elektronskega denarja in plačilne sisteme, določi višino:

- takse za odločanje o posamičnih zadevah na podlagi te uredbe in Uredbe 2022/2554/EU
- nadomestila za opravljanje drugih nalog v zvezi z izvajanjem te uredbe in Uredbe 2022/2554/EU ter
- letnega nadomestila za nadzor, ki ga opravlja na podlagi te uredbe in Uredbe 2022/2554/EU.

8. člen **(prekrškovni organ)**

Prekrškovni organi, ki vodijo postopke in odločajo o prekrških ter izrekajo globe po tej uredbi, so organi iz prvega odstavka 3. člena te uredbe, in sicer zoper subjekte iz drugega odstavka 2. člena Uredbe 2022/2554/EU, za katere je posamezni organ pristojen izvajati tudi postopek nadzora skladno s prvim odstavkom 3. člena te uredbe.

IV. KAZENSKÉ DOLOČBE

9. člen (prekrški)

(1) Z globo od 25.000 do 250.000 evrov se za prekršek kaznuje pravna oseba, z globo od 25.000 do 500.000 evrov pa pravna oseba, ki se po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, če:

- a) nimajo urejenega, enkrat letno pregledanega in ustrezno dokumentiranega okvirja obvladovanja tveganj na področju IKT, kot je določeno v poglavju II Uredbe 2022/2554/EU, vključno s finančnimi subjekti, ki jim je določen poenostavljen okvir obvladovanja tveganj na področju IKT, za katere velja 16. člen Uredbe 2022/2554/EU,
- b) nimajo vzpostavljenega postopka obvladovanja incidentov, povezanih z IKT, skladno s 17. členom Uredbe 2022/2554/EU,
- c) ne poročajo o večjih incidentih in v roku, ki je/bo določen z regulativnimi tehničnimi standardi v skladu z 19. členom Uredbe 2022/2554/EU,
- d) nimajo urejenega programa za testiranja digitalne operativne odpornosti v skladu s 24, 25. in 26. členom Uredbe 2022/2554/EU,
- e) vsaj enkrat letno ne testirajo vseh sistemov in aplikacij IKT, ki podpirajo kritične ali pomembne funkcije, skladno s 24. členom Uredbe 2022/2554/EU in to ustrezno dokumentirajo,
- f) finančni subjekti, določeni s prvim odstavkom 26. člena Uredbe 2022/2554/EU, vsaj enkrat na tri leta oziroma tako pogosto kot zahteva pristojni organ, ne izvajajo naprednega testiranja orodij, sistemov in postopkov IKT na podlagi penetracijskega testiranja na podlagi analize groženj,
- g) ne izpolnjujejo določil glede obvladovanja tveganj tretjih strani na področju IKT, kot je določeno v 28., 29. in 30. členu Uredbe 2022/2554/EU ter najmanj enkrat letno ne poročajo pristojnemu organu,
- h) pristojnemu organu ne pošlje poročil, pojasnil, podatkov ali dokumentacije ali ne omogoči pregleda poslovanja v skladu s prvim in drugim odstavkom 50. člena Uredbe 2022/2554/EU.

(2) Z globo od 2.500 do 10.000 evrov se za prekršek kaznuje odgovorna oseba pravne osebe ali izdajatelj, ki stori prekršek iz prvega odstavka tega člena.

10. člen (višina globe v hitrem prekrškovnem postopku)

Za prekrške iz te uredbe, se sme v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje predpisane globe, določene s to uredbo.

V. PRITOŽBA IN SODNO VARSTVO

11. člen (pravica do sodnega varstva)

(1) Odločitve pristojnih organov iz prvega odstavka 3. člena te uredbe, sprejete na podlagi Uredbe 2022/2554/EU, morajo biti ustrezno utemeljene, proti odločbam pristojnih organov pa je dovoljeno začeti postopek sodnega varstva.

(2) Za postopek sodnega varstva zoper odločbe pristojnih organov se smiselno uporablja zakon, ki ureja upravni spor, če ni s to uredbo, zakonom, ki ureja trg finančnih instrumentov, zakonom, ki ureja bančništvo, ali zakonom, ki ureja zavarovalništvo, določeno drugače.

12. člen (začetek veljavnosti)

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

III. OBRAZLOŽITEV

K 1. členu (vsebina)

Člen določa vsebino uredbe. Z uredbo se določa pristojne organe in njihove pristojnosti za izvajanje nalog iz Uredbe 2022/2554/EU.

K 2. členu (pomen izrazov)

Člen določa, da so izrazi v tej uredbi pomensko usklajeni z izrazi, opredeljenimi v Uredbi 2022/2554/EU.

K 3. členu (pristojnost organov)

Člen določa pristojnost organov nad finančnimi subjekti. Pristojnost organov v tej uredbi je določena glede na določila 46. člena Uredbe 2022/2554/EU, izvajajo pa jih Agencija za trg vrednostnih papirjev, Agencija za zavarovalni nadzor in Banka Slovenije. Člen dodatno določa, da Agencija za trg vrednostnih papirjev pristojna le za ponudnike storitev v zvezi s kriptosredstvi, pooblašene na podlagi uredbe o trgih kriptosredstev in izdajatelje žetonov, vezanih na sredstva, ki ne spadajo pod pristojnost ostalih pristojnih organov. Glede pristojnosti, ki so povezane s penetracijskim testiranjem, lahko pristojni organi sporazumno sodelujejo z Uradom RS za informacijsko varnost.

K 4. členu (poročanje o IKT incidentih in kibernetiskih grožnjah)

S členom se ureja poročanje finančnih subjektov o večjih IKT incidentih in kibernetiskih grožnjah. Finančni subjekti poročajo pristojnemu organu te uredbe, hkrati pa, kadar tako določi pristojni organ, tudi CSIRT-u. V skladu 19. členom Uredbe 2022/2554/EU, ki določa, da države članice imenujejo en sam pristojni organ, odgovoren za izvajanje funkcij in dolžnosti iz 19. člena Uredbe 2022/2554/EU, člen določa pristojna organa za poročanje o večjih incidentih povezanih z IKT in pomembnih kibernetiskih grožnjah. Člen nadalje ureja, da pristojni organi tedensko poročajo o večjih incidentih CSIRT-u. Člen nazadnje še ureja, da finančni subjekti lahko prostovoljno poročajo o pomembnih kibernetiskih grožnjah tako pristojnemu organu kot CSIRT-u.

K 5. členu (način opravljanja nadzora)

S tem členom se določa, kako pristojni organi opravljajo nadzor nad spoštovanjem določb Uredbe 2022/2554/EU.

K 6. členu (ukrepi pristojnih organov)

Člen določa ukrepe pristojnih organov. Uredba 2022/2554/EU določa katere ukrepe lahko uporabi pristojni organ za doseg namena nadzora glede spoštovanja določb Uredbe 2022/2554/EU in obveznost javne objave le teh.

K 7. členu (tarifa)

Agencija za trg vrednostnih papirjev, Agencija za zavarovalni nadzor in Banka Slovenije za svoje delo v zvezi z delom in nadzorom, vezanim na Uredbo 2022/2554/EU, določijo višino takse za odločanje o posamičnih zadevah. Tarifa je izdana v skladu z zakoni, ki urejajo delovanje posameznega nadzornega organa.

K 8. členu (prekrškovni organ)

Člen določa prekrškovne organe po tej uredbi, ki so organi iz prvega odstavka 3. člena te uredbe.

K 9. členu (prekrški)

Uredba 2022/2554/EU v četrtem odstavku 50. člena določa, da lahko pristojni organi zaradi kršitev določb Uredbe 2022/2554/EU izrečejo tudi denarne ukrepe. Ta člen določa višino globe, ki jo lahko izreče pristojni organ za neizpolnjevanje obveznosti subjektov Uredbe 2022/2554/EU.

K 10. členu (višine globe v hitrem prekrškovnem postopku)

Člen določa, da se lahko za prekrške iz te uredbe, v hitrem postopku izreče globa tudi v znesku, ki je višji od najnižje predpisane globe, določene s tem zakonom.

K 11. členu pravica do sodnega varstva)

Ta člen ureja pravico do sodnega varstva.

K 12. členu (začetek veljavnosti)

Člen določa začetek veljavnosti uredbe.