Zakon o provedbi Uredbe (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor

Sadržaj

I. OPĆE ODREDBE

Članak 1.

Predmet Zakona

Ovim se Zakonom utvrđuju nadležna tijela, ovlasti nadležnih tijela, postupak nadzora, nadzorne mjere te prekršajne odredbe za kršenje odredbi ovoga Zakona i uredbe Europske unije iz članka 2. ovoga Zakona.

Članak 2.

Pravo Europske unije

Ovim se Zakonom osigurava provedba Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (Tekst značajan za EGP) (SL L 333, 27. 12. 2022.) (u daljnjem tekstu: Uredba (EU) 2022/2554).

Članak 3.

Pojmovi

(1) U smislu ovoga Zakona pojedini pojmovi imaju sljedeće značenje:

1. Agencija je Hrvatska agencija za nadzor financijskih usluga čije su nadležnosti i područje rada propisani zakonom kojim se uređuje područje rada i nadležnosti Hrvatske agencije za nadzor financijskih usluga, ovim Zakonom i drugim zakonima

2. EBA (engl. European Banking Authority) je Europsko nadzorno tijelo za bankarstvo

3. EIOPA (engl. European Insurance and Occupational Pensions Authority) je Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje

4. ESB (engl. European Central Bank) je Europska središnja banka

5. ESMA (engl. European Securities and Markets Authority) je Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala

6. Hrvatska narodna banka je središnja banka Republike Hrvatske čiji su zadaci i nadležnosti propisani zakonom kojim se uređuje status, cilj, položaj i zadaci Hrvatske narodne banke, ovim Zakonom i drugim zakonima

7. nadležna tijela su Agencija i Hrvatska narodna banka

8. europska nadzorna tijela su EBA, ESMA i EIOPA

9. CSIRT (engl. Computer Security Incident Response Team) je tijelo za prevenciju i zaštitu od kibernetičkih incidenata kojem su u skladu sa zakonom kojim se uređuje kibernetička sigurnost dodijeljene zadaće te je imenovano nadležnim CSIRT-om za sektore bankarstva i infrastrukture financijskog tržišta

10. kibernetička prijetnja je kiberprijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (Tekst značajan za EGP) (SL L 151, 7. 6. 2019.)

11. ozbiljna kibernetička prijetnja je ozbiljna kiberprijetnja kako je definirana člankom 3. točkom 13. Uredbe (EU) 2022/2554

12. penetracijsko testiranje vođeno prijetnjama (engl. Threat-Led Penetration Testing, u daljnjem tekstu: »TLPT«) je okvir koji oponaša taktike, tehnike i procedure stvarnih aktera prijetnje koje se smatraju stvarnom kibernetičkom prijetnjom, koji omogućuje kontrolirano, prilagođeno testiranje ključnih produkcijskih sustava financijskog subjekta, vođeno saznanjima o prijetnjama.

(2) Ostali pojmovi u ovom Zakonu imaju jednako značenje kao pojmovi definirani u Uredbi (EU) 2022/2554.

Članak 4.

Korištenje pojmova s rodnim značenjem

Izrazi koji se koriste u ovom Zakonu, a imaju rodno značenje odnose se jednako na muški i ženski rod.

Članak 5.

Postupanje po smjernicama

(1) Smjernice koje europska nadzorna tijela donose u skladu sa svojim ovlastima iz Uredbe (EU) 2022/2554 obvezujuće su za Agenciju i subjekte nadzora čije su obveze određene odredbama ovoga Zakona i Uredbe (EU) 2022/2554 ako su ispunjeni sljedeći uvjeti:

1. da se, sukladno proceduri propisanoj uredbama kojima se osnivaju europska nadzorna tijela, Agencija očitovala da se obvezuje u cijelosti ili djelomično pridržavati odredbi pojedine smjernice ili da se do određenog roka namjerava uskladiti s pojedinom smjernicom

2. da je Agencija na svojim internetskim stranicama objavila obavijest o očitovanju iz točke 1. ovoga stavka, pri čemu su stupanje na snagu i početak primjene određeni pojedinom smjernicom, osim kada se Agencija očitovala o namjeri usklađenja s pojedinim smjernicama do određenog roka, u kojem su slučaju stupanje na snagu i početak primjene određeni očitovanjem iz točke 1. ovoga stavka.

(2) U izvršavanju svojih ovlasti Hrvatska narodna banka vodi računa o ujednačavanju nadzornih i supervizorskih alata i postupaka pri primjeni ovoga Zakona odnosno Uredbe (EU) 2022/2554 te poduzima sve aktivnosti u svrhu usklađivanja sa smjernicama i preporukama koje izdaju europska nadzorna tijela u skladu sa svojim ovlastima.

(3) Agencija i Hrvatska narodna banka na svojim internetskim stranicama objavljuju poveznice na tekstove smjernica kojih će se ta tijela i subjekti nadzora u cijelosti ili djelomično pridržavati ili s kojima se do određenog roka namjeravaju uskladiti, zajedno s obavijesti koja u odnosu na pojedine smjernice sadržava sljedeće informacije:

1. na koje se subjekte nadzora smjernica odnosi

2. primjenjuje li se smjernica u cijelosti ili djelomično i

3. datum stupanja na snagu i početka primjene smjernice, s određenim prijelaznim razdobljima ako su ona predviđena.

Članak 6.

Izuzeće od primjene

Sukladno članku 2. stavku 4. Uredbe (EU) 2022/2554, u Republici Hrvatskoj Uredba (EU) 2022/2554 i ovaj Zakon ne primjenjuju se na kreditne unije i Hrvatsku banku za obnovu i razvitak.

II. NADLEŽNA TIJELA, NJIHOVE NADLEŽNOSTI I PODRUČJE RADA

Članak 7.

Nadležna tijela

(1) Nadležna tijela za provedbu Uredbe (EU) 2022/2554 i ovoga Zakona su Agencija i Hrvatska narodna banka.

(2) Protiv rješenja koje nadležno tijelo donosi na temelju ovoga Zakona i Uredbe (EU) 2022/2554 nije dopuštena žalba, ali se može pokrenuti upravni spor.

(3) U postupku povodom tužbe protiv rješenja iz stavka 2. ovoga članka nadležni upravni sud ne može odlučiti da tužba ima odgodni učinak niti može izdati privremenu mjeru.

Članak 8.

Subjekti nadzora nadležnih tijela

(1) Subjekti nadzora Agencije u smislu ovoga Zakona, a u vezi s ispunjavanjem obveza iz Uredbe (EU) 2022/2554 i ovoga Zakona su sljedeći subjekti iz članka 2. stavka 1. Uredbe (EU) 2022/2554:

1. investicijsko društvo kako je određeno zakonom kojim se uređuje tržište kapitala

2. pružatelj usluga povezanih s kriptoimovinom koji ima odobrenje Agencije u skladu s odredbama zakona kojim se osigurava provedba Uredbe (EU) 2023/1114 Europskog parlamenta i Vijeća od 31. svibnja 2023. o tržištima kriptoimovine i izmjeni uredaba (EU) br. 1093/2010 i (EU) br. 1095/2010 te direktiva 2013/36/EU i (EU) 2019/1937 (Tekst značajan za EGP) (SL L 150, 9. 6. 2023.) (u daljnjem tekstu: Uredba (EU) 2023/1114)

3. središnji depozitorij vrijednosnih papira kako je određen Uredbom (EU) br. 909/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o poboljšanju namire vrijednosnih papira u Europskoj uniji i o središnjim depozitorijima vrijednosnih papira te izmjeni direktiva 98/26/EZ i 2014/65/EU te Uredbe (EU) br. 236/2012 (Tekst značajan za EGP) (SL L 257, 28. 8. 2014.)

4. središnja druga ugovorna strana kako je određena Uredbom (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju (Tekst značajan za EGP) (SL L 201, 27. 7. 2012.)

5. operater uređenog tržišta kako je određen zakonom kojim se uređuje tržište kapitala

6. veliko društvo za upravljanje investicijskim fondovima (u daljnjem tekstu: UAIF) kako je određeno zakonom kojim se uređuje osnivanje i upravljanje alternativnim investicijskim fondovima

7. društvo za upravljanje otvorenim investicijskim fondovima s javnom ponudom kako je određeno zakonom kojim se uređuje osnivanje i upravljanje otvorenim investicijskim fondovima s javnom ponudom

8. pružatelj usluga dostave podataka kako je određen zakonom kojim se uređuje tržište kapitala

9. društvo za osiguranje kako je određeno zakonom kojim se uređuje osiguranje

10. društvo za reosiguranje kako je određeno zakonom kojim se uređuje osiguranje

11. posrednik u osiguranju, osim ako je mikro, mali ili srednji poduzetnik izuzet od primjene Uredbe (EU) 2022/2554 u skladu s odredbom članka 2. stavka 3. točke e) Uredbe (EU) 2022/2554

12. posrednik u reosiguranju, osim ako je mikro, mali ili srednji poduzetnik izuzet od primjene Uredbe (EU) 2022/2554 u skladu s odredbom članka 2. stavka 3. točke e) Uredbe (EU) 2022/2554

13. sporedni posrednik u osiguranju, osim ako je mikro, mali ili srednji poduzetnik izuzet od primjene Uredbe (EU) 2022/2554 u skladu s odredbom članka 2. stavka 3. točke e) Uredbe (EU) 2022/2554

14. društvo za upravljanje dobrovoljnim mirovinskim fondovima kako je određeno zakonom kojim se uređuje osnivanje i upravljanje dobrovoljnim mirovinskim fondovima

15. mirovinsko osiguravajuće društvo kako je određeno zakonom kojim se uređuje osnivanje i poslovanje mirovinskih osiguravajućih društava

16. administrator ključnih referentnih vrijednosti kako je određen zakonom kojim se osigurava provedba Uredbe (EU) 2016/1011 Europskog parlamenta i Vijeća od 8. lipnja 2016. o indeksima koji se upotrebljavaju kao referentne vrijednosti u financijskim instrumentima i financijskim ugovorima ili za mjerenje uspješnosti investicijskih fondova i o izmjeni direktiva 2008/48/EZ i 2014/17/EU te Uredbe (EU) br. 596/2014 (Tekst značajan za EGP) (SL L 171, 29. 6. 2016.) kako je zadnje izmijenjena Uredbom (EU) 2023/2869 Europskog parlamenta i Vijeća od 13. prosinca 2023. o izmjeni određenih uredbi u pogledu uspostave i funkcioniranja jedinstvene europske pristupne točke (Tekst značajan za EGP) (SL L, 2023/2869, 20. 12. 2023.)

17. pružatelj usluga skupnog financiranja kako je određen zakonom kojim se osigurava provedba Uredbe (EU) 2020 /1503 Europskog parlamenta i Vijeća od 7. listopada 2020. o europskim pružateljima usluga skupnog financiranja za poduzeća i izmjeni Uredbe (EU) 2017/1129 i Direktive (EU) 2019/1937 (Tekst značajan za EGP) (SL L 347, 20. 10. 2020.).

(2) Osim subjekata iz stavka 1. ovoga članka, ovaj Zakon i Uredbu (EU) 2022/2554 dužno je primjenjivati i društvo za upravljanje obveznim mirovinskim fondovima, kako je određeno zakonom kojim se uređuje osnivanje i upravljanje obveznim mirovinskim fondovima, koje je u smislu primjene ovoga Zakona subjekt nadzora Agencije.

(3) Subjekti nadzora Hrvatske narodne banke u smislu ovoga Zakona, a u vezi s ispunjavanjem obveza iz Uredbe (EU) 2022/2554 i ovoga Zakona su sljedeći subjekti iz članka 2. stavka 1. Uredbe (EU) 2022/2554:

1. kreditna institucija kako je određena zakonom kojim se uređuje osnivanje i poslovanje kreditnih institucija, osim kreditne institucije klasificirane kao značajne u skladu s člankom 6. stavkom 4. Uredbe Vijeća (EU) br. 1024/2013 od 15. listopada 2013. o dodjeli određenih zadaća Europskoj središnjoj banci u vezi s politikama bonitetnog nadzora kreditnih institucija (SL L 287, 29. 10. 2013.) (u daljnjem tekstu: Uredba Vijeća (EU) br. 1024/2013), za koje je nadležan ESB u skladu s ovlastima i zadaćama koje su mu dodijeljene Uredbom Vijeća (EU) br. 1024/2013

2. institucija za platni promet kako je određena zakonom kojim se uređuje platni promet, uključujući institucije za platni promet izuzete u skladu sa zakonom kojim se uređuje platni promet i nacionalnim odredbama drugih država članica kojima se prenosi Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (Tekst značajan za EGP) (SL L 337, 23. 12. 2015.)

3. pružatelj usluge informiranja o računu kako je određen zakonom kojim se uređuje platni promet

4. institucija za elektronički novac kako je određena zakonom kojim se uređuje elektronički novac, uključujući institucije za elektronički novac izuzete u skladu sa zakonom kojim se uređuje elektronički novac i nacionalnim odredbama drugih država članica kojima se prenosi Direktiva 2009/110/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o osnivanju, obavljanju djelatnosti i bonitetnom nadzoru poslovanja institucija za elektronički novac te o izmjeni direktiva 2005/60/EZ i 2006/48/EZ i stavljanju izvan snage Direktive 2000/46/EZ (Tekst značajan za EGP) (SL L 267, 10. 10. 2009.)

5. izdavatelj tokena vezanih uz imovinu kako je određen Uredbom (EU) 2023/1114 koji ima odobrenje Hrvatske narodne banke u skladu s odredbama zakona kojim se osigurava provedba Uredbe (EU) 2023/1114.

Članak 9.

Podjela nadležnosti

(1) Nadležnosti Agencije za potrebe provedbe Uredbe (EU) 2022/2554 i ovoga Zakona odnose se na:

1. provođenje nadzora u smislu pridržavanja odredbi Uredbe (EU) 2022/2554 i ovoga Zakona nad subjektima nadzora Agencije iz članka 8. stavaka 1. i 2. ovoga Zakona

2. izricanje nadzornih mjera subjektima nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona

3. podnošenje optužnih prijedloga kod utvrđenih povreda odredbi Uredbe (EU) 2022/2554 i ovoga Zakona od strane subjekata nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona.

(2) Nadležnosti Hrvatske narodne banke za potrebe provedbe Uredbe (EU) 2022/2554 i ovoga Zakona odnose se na:

1. provođenje nadzora u smislu pridržavanja odredbi Uredbe (EU) 2022/2554 i ovoga Zakona nad subjektima nadzora Hrvatske narodne banke iz članka 8. stavka 3. ovoga Zakona

2. izricanje nadzornih mjera subjektima nadzora iz članka 8. stavka 3. ovoga Zakona

3. podnošenje optužnih prijedloga kod utvrđenih povreda odredbi Uredbe (EU) 2022/2554 i ovoga Zakona od strane subjekata nadzora iz članka 8. stavka 3. ovoga Zakona.

(3) Opseg razmjene informacija te koordinacija postupaka i aktivnosti pri provedbi ovoga Zakona i Uredbe (EU) 2022/2554 uredit će se sporazumom o suradnji između Agencije i Hrvatske narodne banke.

III. NADZOR

Članak 10.

Postupak nadzora koji provodi Agencija

(1) Nadzor nad provedbom Uredbe (EU) 2022/2554 i ovoga Zakona prema podjeli nadležnosti iz članka 9. ovoga Zakona obavlja Agencija u skladu s odredbama Uredbe (EU) 2022/2554, ovoga Zakona i zakona kojima je uređeno osnivanje i poslovanje subjekata nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona.

(2) Agencija može obavljanje pojedinih zadataka u vezi s nadzorom nad provedbom Uredbe (EU) 2022/2554 i ovoga Zakona povjeriti ovlaštenom revizoru, revizorskom društvu ili drugoj stručno osposobljenoj osobi.

(3) Agencija u postupku nadzora može:

1. od subjekta nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona i njihovih radnika zatražiti pisana i usmena objašnjenja

2. obaviti razgovore za potrebe prikupljanja informacija s bilo kojom osobom za koju ocijeni da ima relevantna saznanja, uz uvjet njezina izričitog pristanka.

Članak 11.

Postupak nadzora koji provodi Hrvatska narodna banka

(1) Nadzor nad provedbom Uredbe (EU) 2022/2554 i ovoga Zakona, sukladno podjeli nadležnosti iz članka 9. ovoga Zakona, obavlja Hrvatska narodna banka, sukladno odredbama Uredbe (EU) 2022/2554, ovoga Zakona i zakona kojima je uređeno osnivanje i poslovanje subjekata nadzora iz članka 8. stavka 3. ovoga Zakona.

(2) Hrvatska narodna banka može obavljanje pojedinih zadataka u vezi s nadzorom nad provedbom Uredbe (EU) 2022/2554 i ovoga Zakona povjeriti ovlaštenom revizoru, revizorskom društvu ili drugoj stručno osposobljenoj osobi.

(3) Hrvatska narodna banka u postupku nadzora može:

1. od subjekta nadzora iz članka 8. stavka 3. ovoga Zakona i njihovih radnika zatražiti pisana i usmena objašnjenja

2. obaviti razgovore za potrebe prikupljanja informacija s bilo kojom osobom za koju ocijeni da ima relevantna saznanja, uz uvjet njezina izričitog pristanka.

Članak 12.

Nadzorne mjere Agencije

(1) Osim mjera koje je ovlaštena izricati sukladno zakonima kojima se uređuje osnivanje i poslovanje subjekata nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona, Agencija je ovlaštena pri obavljanju nadzora nad provedbom Uredbe (EU) 2022/2554 i ovoga Zakona:

1. izdavati nalog subjektu nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona i odgovornoj osobi tog subjekta nadzora da prestane s ponašanjem koje predstavlja povredu Uredbe (EU) 2022/2554 i ovoga Zakona i da se suzdrži od ponavljanja takvog ponašanja

2. upućivati zahtjev za privremeni ili trajni prestanak postupanja ili ponašanja koje smatra protivnim odredbama Uredbe (EU) 2022/2554 i ovoga Zakona te sprječavati ponavljanja takvog postupanja ili ponašanja

3. izricati ili odrediti mjere u skladu s Uredbom (EU) 2022/2554 i ovim Zakonom i podnositi optužne prijedloge kako bi se osiguralo da subjekt nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona uspostavi postupanje koje je u skladu s Uredbom (EU) 2022/2554 i ovim Zakonom

4. upućivati zahtjev, u mjeri u kojoj je to propisima dopušteno, za dostavu postojeće evidencije telekomunikacijskog operatera o podatkovnom prometu ako postoji opravdana sumnja u povredu Uredbe (EU) 2022/2554 i ovoga Zakona te ako takva evidencija može biti važna za istragu povreda Uredbe (EU) 2022/2554 i ovoga Zakona i

5. izdavati javne obavijesti, uključujući javne objave u kojima se navodi identitet subjekta nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona i odgovorne osobe subjekta nadzora te priroda povrede.

(2) Ako utvrdi da je član upravljačkog tijela subjekta nadzora ili druga osoba odgovorna za povrede Uredbe (EU) 2022 /2554, Agencija može kao posebnu nadzornu mjeru naložiti nadzornom odboru subjekta nadzora da razriješi člana uprave ili drugu osobu razriješi rukovodeće funkcije u subjektu nadzora.

(3) Pravna ili fizička osoba kojoj je Agencija izrekla nadzornu mjeru dužna ju je izvršiti na način i u roku kako je to određeno rješenjem.

(4) Agencija je u svrhu ujednačavanja nadzorne prakse ovlaštena raznim vrstama objava izvještavati određene skupine subjekata nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona o objašnjenju ili načinu primjene ovoga Zakona.

Članak 13.

Nadzorne mjere Hrvatske narodne banke

(1) Osim mjera koje je ovlaštena izricati sukladno zakonima kojima se uređuje osnivanje i poslovanje subjekata nadzora iz članka 8. stavka 3. ovoga Zakona, Hrvatska narodna banka ovlaštena je pri obavljanju nadzora nad provedbom Uredbe (EU) 2022/2554 i ovoga Zakona:

1. izdavati nalog subjektu nadzora iz članka 8. stavka 3. ovoga Zakona da prestane s ponašanjem koje predstavlja povredu Uredbe (EU) 2022/2554 i ovoga Zakona i da se suzdrži od ponavljanja takvog ponašanja

2. upućivati zahtjev za privremeni ili trajni prestanak postupanja ili ponašanja koje smatra protivnim odredbama Uredbe (EU) 2022/2554 i ovoga Zakona te sprječavati ponavljanja takvog postupanja ili ponašanja

3. izricati ili odrediti mjere u skladu s Uredbom (EU) 2022/2554 i ovim Zakonom i podnositi optužne prijedloge kako bi se osiguralo da subjekt nadzora iz članka 8. stavka 3. ovoga Zakona uspostavi postupanje koje je u skladu s Uredbom (EU) 2022/2554 i ovim Zakonom

4. upućivati zahtjev, u mjeri u kojoj je to propisima dopušteno, za dostavu postojeće evidencije telekomunikacijskog operatera o podatkovnom prometu ako postoji opravdana sumnja u povredu Uredbe (EU) 2022/2554 i ovoga Zakona te ako takva evidencija može biti važna za istragu povreda Uredbe (EU) 2022/2554 i ovoga Zakona i

5. izdavati javne obavijesti, uključujući javne objave u kojima se navodi identitet subjekta nadzora iz članka 8. stavka 3. ovoga Zakona i odgovorne osobe subjekta nadzora te priroda povrede.

(2) Ako utvrdi da je član upravljačkog tijela subjekta nadzora ili druga osoba odgovorna za povrede Uredbe (EU) 2022 /2554, Hrvatska narodna banka može kao posebnu nadzornu mjeru naložiti nadzornom odboru subjekta nadzora da razriješi člana uprave ili drugu osobu ukloni s rukovodeće funkcije u subjektu nadzora.

(3) Pravna ili fizička osoba kojoj je Hrvatska narodna banka izrekla nadzornu mjeru dužna ju je izvršiti na način i u roku kako je to određeno rješenjem.

(4) Hrvatska narodna banka ovlaštena je, u svrhu ujednačavanja nadzorne prakse, raznim vrstama objava izvještavati određene skupine subjekata nadzora iz članka 8. stavka 3. ovoga Zakona o objašnjenju ili načinu primjene ovoga Zakona.

IV. OSTALE ODREDBE VEZANE UZ PROVEDBU UREDBE (EU) 2022/2554

Članak 14.

Izvještavanje o značajnim IKT incidentima

(1) Subjekti nadzora iz članka 8. stavaka 1. i 2. ovoga Zakona dužni su o značajnim IKT incidentima izvještavati Agenciju.

(2) Subjekti nadzora iz članka 8. stavka 3. ovoga Zakona dužni su o značajnim IKT incidentima izvještavati Hrvatsku narodnu banku.

(3) Subjekti nadzora iz članka 8. ovoga Zakona o značajnom IKT incidentu dužni su izvijestiti i CSIRT.

Članak 15.

Nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima

(1) Subjekti nadzora iz članka 8. ovoga Zakona dužni su o značajnim IKT incidentima izvještavati putem nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima koja je uspostavljena zakonom kojim se uređuje kibernetička sigurnost.

(2) Subjekti nadzora iz članka 8. ovoga Zakona koji na dobrovoljnoj osnovi izvještavaju o ozbiljnoj kibernetičkoj prijetnji za izvještavanje koriste se nacionalnom platformom iz stavka 1. ovoga članka.

(3) Agencija i Hrvatska narodna banka smjernicom određuju pojedinosti u svezi s izvještavanjem o značajnim IKT incidentima i ozbiljnim kibernetičkim prijetnjama putem nacionalne platforme iz stavka 1. ovoga članka.

Članak 16.

Predstavnik u Nadzornom forumu

(1) Nadležna tijela u smislu članka 32. stavka 5. Uredbe (EU) 2022/2554 su Agencija i Hrvatska narodna banka.

(2) Agencija i Hrvatska narodna banka će u sporazumu o suradnji iz članka 9. stavka 3. ovoga Zakona detaljnije urediti sudjelovanje u Nadzornom forumu iz članka 32. Uredbe (EU) 2022/2554, a posebno:

1. pravo svake od njih da svake dvije godine imenuje svog predstavnika u Nadzorni forum te način i rokove obavještavanja glavnog nadzornog tijela o promjenama predstavnika

2. način međusobnog informiranja o aktivnostima Nadzornog foruma

3. obvezu međusobnog savjetovanja radi zauzimanja zajedničkih stajališta u području IKT rizika i obavještavanja drugog nadzornog tijela o svim aktivnostima vezanim uz upravljanje IKT rizikom iz područja nadležnosti pojedinog nadležnog tijela.

(3) Agencija i Hrvatska narodna banka će nakon sklapanja sporazuma o imenovanju predstavnika u Nadzorni forum obavijestiti glavno nadzorno tijelo u skladu s člankom 32. stavkom 5. Uredbe (EU) 2022/2554.

(4) Ako Agencija i Hrvatska narodna banka ne sklope sporazum o suradnji iz članka 9. stavka 3. ovoga Zakona ili ako Agencija i Hrvatska narodna banka u sporazumu o suradnji iz članka 9. stavka 3. ovoga Zakona ne urede sudjelovanje u Nadzornom forumu iz članka 32. Uredbe (EU) 2022/2554 u skladu sa stavkom 2. ovoga članka, Vlada Republike Hrvatske, na prijedlog ministra financija, imenuje iz reda članova osoblja nadležnih tijela predstavnika i promatrača u Nadzorni forum te o imenovanju Ministarstvo financija obavještava glavno nadzorno tijelo.

V. PREKRŠAJNE ODREDBE

Članak 17.

Opće odredbe

(1) Ako je počinitelj prekršaja poduzetnik/pravna osoba, u smislu propisa kojima se uređuje računovodstvo poduzetnika, ukupnim prihodom za osnovicu izračuna visine kazne za prekršaje iz ove glave smatra se ukupan godišnji prihod prema posljednjim dostupnim financijskim izvještajima koje je odobrilo upravljačko tijelo počinitelja prekršaja.

(2) Ako je počinitelj prekršaja matično društvo ili društvo kći matičnoga društva od kojega se zahtijeva priprema konsolidiranih financijskih izvještaja u skladu sa zakonom kojim se uređuje računovodstvo poduzetnika, ukupnim prihodom za osnovicu izračuna visine kazne za prekršaje iz ove glave smatra se ukupan godišnji prihod ili odgovarajuća vrsta prihoda u skladu s relevantnim računovodstvenim propisima prema posljednjim dostupnim konsolidiranim financijskim izvještajima koje je odobrilo upravljačko tijelo krajnjega matičnog društva.

(3) Kada nadležna tijela iz ovoga Zakona zbog postupanja koja su protivna Uredbi (EU) 2022/2554 izvršavaju svoje ovlasti:

– za izricanje nadzornih mjera

– za izricanje drugih mjera koje su ovlaštena izricati sukladno zakonima kojima se uređuje poslovanje subjekata nadzora iz članka 8. ovoga Zakona ili

– odlučivanja o podnošenju optužnih prijedloga,

obvezna su uzeti u obzir sve relevantne okolnosti iz članka 51. stavka 2. Uredbe (EU) 2022/2554.

Članak 18.

Objava izrečenih prekršajnih sankcija

(1) Nadležna tijela odluke o prekršaju objavljuju na svojim internetskim stranicama u skladu s člankom 54. Uredbe (EU) 2022/2554.

(2) Podaci iz stavka 1. ovoga članka dostupni su na internetskim stranicama nadležnih tijela samo tijekom razdoblja koje je potrebno za provedbu članka 54. Uredbe (EU) 2022/2554, a najdulje pet godina od dana njihove objave.

(3) Nadležna tijela u skladu s odredbama o rehabilitaciji u smislu zakona kojim je uređen prekršajni postupak istekom roka od tri godine od dana pravomoćnosti odluke o prekršaju sa svojih internetskih stranica uklanjaju osobne podatke u smislu propisa kojima je uređena zaštita osobnih podataka, a iz kojih bi bilo moguće utvrditi identitet počinitelja prekršaja.

Članak 19.

Prekršaji

(1) Novčanom kaznom koja ne može biti veća od 3 % ukup-nog prihoda iz članka 17. stavka 1. ili 2. ovoga Zakona kaznit će se pravna osoba ako:

1. nije uspostavila okvir za unutarnje upravljanje i kontrolu kojim se osigurava djelotvorno i razborito upravljanje IKT rizicima, u skladu s člankom 5. stavkom 1. Uredbe (EU) 2022/2554

2. nije uvela funkciju za praćenje aranžmana o upotrebi IKT usluga sklopljenih s trećim stranama pružateljima IKT usluga ili imenovala člana višeg rukovodstva koji će biti odgovoran za nadzor nad povezanom izloženosti rizicima i relevantnom dokumentacijom, u skladu s člankom 5. stavkom 3. Uredbe (EU) 2022/2554

3. nije uspostavila okvir za upravljanje IKT rizicima, u skladu s člankom 6. stavcima 1. i 2. Uredbe (EU) 2022/2554

4. nije svela učinak IKT rizika na najmanju moguću mjeru ili nije na zahtjev nadležnog tijela dostavila sve informacije, u skladu s člankom 6. stavkom 3. Uredbe (EU) 2022/2554

5. nije odgovornost za upravljanje IKT rizicima i nadzor nad njima dodijelila kontrolnoj funkciji ili nije osigurala odgovarajuće razdvajanje i neovisnost funkcija upravljanja IKT rizicima, kontrolnih funkcija i funkcija unutarnje revizije, u skladu s člankom 6. stavkom 4. Uredbe (EU) 2022/2554

6. ne dokumentira okvir za upravljanje IKT rizicima ili ne preispituje okvir za upravljanje IKT rizicima ili ne poboljšava okvir za upravljanje IKT rizicima ili nije dostavila izvješće o preispitivanju okvira za upravljanje IKT rizicima, u skladu s člankom 6. stavkom 5. Uredbe (EU) 2022/2554

7. nije osigurala da okvir za upravljanje IKT rizicima podliježe unutarnjoj reviziji, u skladu s člankom 6. stavkom 6. Uredbe (EU) 2022/2554

8. nije uspostavila formalni proces daljnjeg postupanja na temelju zaključaka unutarnjeg revizijskog pregleda, u skladu s člankom 6. stavkom 7. Uredbe (EU) 2022/2554

9. okvir za upravljanje IKT rizicima ne obuhvaća strategiju za digitalnu otpornost uspostavljenu u skladu s člankom 6. stavkom 8. Uredbe (EU) 2022/2554

10. ne upotrebljava ili ne održava ažuriranima IKT sustave, protokole i alate koji su u skladu s člankom 7. Uredbe (EU) 2022/2554

11. nije utvrdila ili nije klasificirala ili nije na odgovarajući način dokumentirala sve poslovne funkcije ili uloge i odgovornosti koje se podupiru IKT-om ili informacijsku imovinu i IKT imovinu kojom se te funkcije podupiru ili njihove uloge i ovisnosti u odnosu na IKT rizik, u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2554

12. ne utvrđuje kontinuirano sve izvore IKT rizika ili ne procjenjuje kibernetičke prijetnje ili ne procjenjuje ranjivosti IKT-a, u skladu s člankom 8. stavkom 2. Uredbe (EU) 2022/2554

13. nije provela procjenu rizika nakon značajne promjene, u skladu s člankom 8. stavkom 3. Uredbe (EU) 2022/2554

14. nije utvrdila svu informacijsku i IKT imovinu ili nije mapirala onu koju smatra ključnom ili nije odredila veze među imovinom, u skladu s člankom 8. stavkom 4. Uredbe (EU) 2022/2554

15. nije utvrdila ili nije dokumentirala sve procese koji ovise o trećim stranama pružateljima IKT usluga, u skladu s člankom 8. stavkom 5. Uredbe (EU) 2022/2554

16. ne vodi ili ne ažurira redovito relevantne evidencije, u skladu s člankom 8. stavkom 6. Uredbe (EU) 2022/2554

17. ne provodi posebnu procjenu IKT rizika za sve zastarjele IKT sustave, u skladu s člankom 8. stavkom 7. Uredbe (EU) 2022/2554

18. ne prati ili ne kontrolira sigurnost i funkcioniranje IKT sustavâ i alatâ, u skladu s člankom 9. stavkom 1. Uredbe (EU) 2022/2554

19. ne izrađuje ili ne provodi politike ili postupke ili protokole ili alate za sigurnost IKT-a, u skladu s člankom 9. stavcima 2. i 3. Uredbe (EU) 2022/2554

20. uspostavljeni okvir za upravljanje IKT rizicima ne obuhvaća elemente u skladu s člankom 9. stavkom 4. Uredbe (EU) 2022/2554

21. nije uspostavila ili nije testirala mehanizam za brzo otkrivanje neobičnih aktivnosti, u skladu s člankom 10. stavcima 1. i 2. Uredbe (EU) 2022/2554

22. nije osigurala dostatne resurse ili sposobnosti za praćenje aktivnosti korisnika ili nastanka neobičnih pojava u IKT-u ili IKT incidenata, u skladu s člankom 10. stavkom 3. Uredbe (EU) 2022/2554

23. nije uspostavila mehanizme za provjeru u skladu s člankom 10. stavkom 4. Uredbe (EU) 2022/2554

24. nije uvela sveobuhvatnu politiku kontinuiteta poslovanja u području IKT-a, u skladu s člankom 11. stavkom 1. Uredbe (EU) 2022/2554

25. ne provodi politiku kontinuiteta poslovanja u području IKT-a, u skladu s člankom 11. stavkom 2. Uredbe (EU) 2022 /2554

26. ne provodi planove odgovora ili planove oporavka u području IKT-a, u skladu s člankom 11. stavkom 3. Uredbe (EU) 2022/2554

27. nije uvela ili ne održava ili ne testira planove kontinuiteta poslovanja u području IKT-a, u skladu s člankom 11. stavkom 4. Uredbe (EU) 2022/2554

28. nije provela analizu učinka na poslovanje, u skladu s člankom 11. stavkom 5. Uredbe (EU) 2022/2554

29. nije testirala planove kontinuiteta poslovanja u području IKT-a ili planove odgovora i oporavka u području IKT-a ili planove komunikacije u krizi, u skladu s člankom 11. stavkom 6. Uredbe (EU) 2022/2554

30. nema funkciju za upravljanje krizama, u skladu s člankom 11. stavkom 7. Uredbe (EU) (EU) 2022/2554

31. nije vodila evidenciju aktivnosti u slučaju aktivacije planova kontinuiteta poslovanja u području IKT-a ili planova odgovora i oporavka u području IKT-a, u skladu s člankom 11. stavkom 8. Uredbe (EU) 2022/2554

32. kao središnji depozitorij vrijednosnih papira ne dostavi Agenciji preslike rezultata testova kontinuiteta poslovanja u području IKT-a, u skladu s člankom 11. stavkom 9. Uredbe (EU) 2022/2554

33. nadležnom tijelu na zahtjev ne dostavi procjenu ukupnih godišnjih troškova i gubitaka prouzročenih značajnim IKT incidentima, u skladu s člankom 11. stavkom 10. Uredbe (EU) 2022/2554

34. nije razvila ili dokumentirala politike i postupke za izradu sigurnosnih kopija ili postupke i metode za ponovnu uspostavu i oporavak, u skladu s člankom 12. stavkom 1. Uredbe (EU) 2022/2554

35. nije uspostavila sustave za izradu sigurnosnih kopija, u skladu s člankom 12. stavkom 2. Uredbe (EU) 2022/2554

36. IKT sustav koji upotrebljava pri vraćanju podataka sa sigurnosne kopije ne ispunjava zahtjeve iz članka 12. stavka 3. Uredbe (EU) 2022/2554

37. kao središnja druga ugovorna stana nema plan oporavka koji omogućuje oporavak svih transakcija koje su bile u tijeku u trenutku poremećaja u skladu s člankom 12. stavkom 3. Uredbe (EU) 2022/2554

38. kao pružatelj usluga dostave podataka nema infrastrukturu u skladu s člankom 12. stavkom 3. podstavkom 3. Uredbe (EU) 2022/2554

39. ne održava redundantne IKT kapacitete, u skladu s člankom 12. stavkom 4. Uredbe (EU) 2022/2554

40. kao središnji depozitorij vrijednosnih papira ne održava najmanje jedno sekundarno mjesto obrade koje ispunjava uvjete iz članka 12. stavka 5. Uredbe (EU) 2022/2554

41. nije osigurala održavanje najviše razine cjelovitosti podataka pri oporavljanju od IKT incidenta, u skladu s člankom 12. stavkom 7. Uredbe (EU) 2022/2554

42. ne raspolaže sposobnostima ili osobljem za prikupljanje informacija o ranjivostima ili kibernetičkim prijetnjama ili IKT incidentima, u skladu s člankom 13. stavkom 1. Uredbe (EU) 2022/2554

43. ne raspolaže sposobnostima ili osobljem za analizu učinka ranjivosti ili kibernetičkih prijetnji ili IKT incidenata na digitalnu operativnu otpornost, u skladu s člankom 13. stavkom 1. Uredbe (EU) 2022/2554

44. nije provela preispitivanje nakon IKT incidenta ili nije na zahtjev obavijestila nadležno tijelo o promjenama koje su provedene slijedom preispitivanja nakon IKT incidenata, u skladu s člankom 13. stavkom 2. Uredbe (EU) 2022/2554

45. nije provela odgovarajuća preispitivanja relevantnih komponenata okvira za upravljanje IKT rizicima, u skladu s člankom 13. stavkom 3. Uredbe (EU) 2022/2554

46. ne prati djelotvornost provedbe strategije za digitalnu operativnu otpornost, u skladu s člankom 13. stavkom 4. Uredbe (EU) 2022/2554

47. nije osmislila ili ne primjenjuje programe za podizanje svijesti o sigurnosti u području IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti, u skladu s člankom 13. stavkom 6. Uredbe (EU) 2022/2554

48. ne prati relevantna tehnološka dostignuća ili nije u toku s najnovijim procesima upravljanja IKT rizicima, u skladu s člankom 13. stavkom 7. Uredbe (EU) 2022/2554

49. nije izradila planove komunikacije u krizi kojima se osigurava odgovorna objava, u skladu s člankom 14. stavkom 1. Uredbe (EU) 2022/2554

50. ne provodi komunikacijske politike za interno osoblje ili vanjske dionike, sukladno članku 14. stavku 2. Uredbe (EU) 2022/2554

51. nije zadužila najmanje jednu osobu za provedbu komunikacijske strategije za IKT incidente, sukladno članku 14. stavku 3. Uredbe (EU) 2022/2554

52. ne postupi u skladu s regulatornim tehničkim standardom koji je donesen na temelju članka 15. Uredbe (EU) 2022 /2554

53. kao subjekt koji u skladu s člankom 16. stavkom 1. Uredbe (EU) 2022/2554 primjenjuje pojednostavljeni okvir za upravljanje IKT rizicima ne ispunjava uvjete iz članka 16. stavka 1. podstavka 2. Uredbe (EU) 2022/2554

54. kao subjekt koji u skladu s člankom 16. stavkom 1. Uredbe (EU) 2022/2554 primjenjuje pojednostavljeni okvir za upravljanje IKT rizicima nije dokumentirala ili preispitala okvir za upravljanje IKT rizicima ili nije izvješće o preispitivanju okvira za upravljanje IKT rizicima dostavila nadležnom tijelu na njegov zahtjev, u skladu s člankom 16. stavkom 2. Uredbe (EU) 2022/2554

55. kao subjekt koji u skladu s člankom 16. stavkom 1. Uredbe (EU) 2022/2554 primjenjuje pojednostavljeni okvir za upravljanje IKT rizicima ne postupi u skladu s regulatornim tehničkim standardom koji je donesen na temelju članka 16. stavka 3. Uredbe (EU) 2022/2554

56. nije definirala ili nije uspostavila ili ne provodi proces upravljanja IKT incidentima, u skladu s člankom 17. stavkom 1. Uredbe (EU) 2022/2554

57. nije evidentirala sve IKT incidente ili ozbiljne kibernetičke prijetnje ili nije uspostavila odgovarajuće postupke i procese za praćenje, postupanje i poduzimanje daljnjih mjera, u skladu s člankom 17. stavkom 2. Uredbe (EU) 2022/2554

58. uspostavljeni proces upravljanja IKT incidentima iz članka 17. stavka 1. Uredbe (EU) 2022/2554 ne obuhvaća elemente iz članka 17. stavka 3. Uredbe (EU) 2022/2554

59. nije klasificirala IKT incidente ili nije utvrdila njihov učinak, u skladu s člankom 18. stavkom 1. Uredbe (EU) 2022/2554

60. nije klasificirala kibernetičke prijetnje, u skladu s člankom 18. stavkom 2. Uredbe (EU) 2022/2554

61. ne postupi u skladu s regulatornim tehničkim standardom koji je donesen na temelju članka 18. stavka 3. Uredbe (EU) 2022/2554

62. nije nadležno tijelo izvijestila o značajnom IKT incidentu, u skladu s člankom 19. stavkom 1. Uredbe (EU) 2022/2554 ili člankom 14. ovoga Zakona ili člankom 15. stavkom 1. ovoga Zakona

63. nije klijente obavijestila o značajnom IKT incidentu koji utječe na financijske interese klijenata ili o mjerama koje su poduzete, u skladu s člankom 19. stavkom 3. Uredbe (EU) 2022/2554

64. ne dostavi u zadanim rokovima početnu obavijest ili prijelazno izvješće ili završno izvješće, u skladu s člankom 19. stavkom 4. Uredbe (EU) 2022/2554

65. ne postupi u skladu s regulatornim tehničkim standardom ili provedbenim tehničkim standardom donesenima na temelju članka 20. Uredbe (EU) 2022/2554

66. nije izradila ili ne održava ili ne preispituje program testiranja digitalne operativne otpornosti, u skladu s člankom 24. stavkom 1. Uredbe (EU) 2022/2554

67. program testiranja digitalne operativne otpornosti ne uključuje procjene ili testove ili metodologije ili postupke ili alate, u skladu s člankom 24. stavkom 2. Uredbe (EU) 2022/2554

68. u provođenju programa testiranja digitalne operativne otpornosti ne primjenjuje pristup koji se temelji na procjeni rizika, u skladu s člankom 24. stavkom 3. Uredbe (EU) 2022/2554

69. nije osigurala da testove digitalne operativne otpornosti provode neovisne strane, u skladu s člankom 24. stavkom 4. Uredbe (EU) 2022/2554

70. nije uvela postupke ili politike za određivanje prioriteta, klasifikaciju i ispravljanje svih problema otkrivenih tijekom testova ili nije utvrdila metodologiju unutarnje provjere, u skladu s člankom 24. stavkom 5. Uredbe (EU) 2022/2554

71. nije osigurala da se provedu testovi IKT sustava i aplikacija, u skladu s člankom 24. stavkom 6. Uredbe (EU) 2022/2554

72. program testiranja digitalne operativne otpornosti iz članka 24. Uredbe (EU) 2022/2554 ne predviđa sve elemente propisane člankom 25. stavkom 1. Uredbe (EU) 2022/2554

73. kao središnji depozitorij vrijednosnih papira ili središnja druga ugovorna strana nije provela procjenu ranjivosti, u skladu s člankom 25. stavkom 2. Uredbe (EU) 2022/2554

74. kao mikro poduzetnik ne provodi testove IKT alata i sustava, u skladu s člankom 25. stavkom 3. Uredbe (EU) 2022/2554

75. kao subjekt koji je u skladu s člankom 26. stavkom 8. podstavkom 3. Uredbe (EU) 2022/2554 dužan provoditi TLPT:

a) nije barem jednom u tri godine ili po zahtjevu nadležnog tijela provela napredno testiranje u obliku TLPT-a, u skladu s člankom 26. stavkom 1. Uredbe (EU) 2022/2554

b) nije TLPT-om obuhvatila više ključnih ili važnih funkcija financijskog subjekta ili sve takve funkcije ili se TLPT ne provodi na produkcijskim sustavima kojima se te funkcije podupiru, u skladu sa zahtjevima iz članka 26. stavka 2. Uredbe (EU) 2022/2554

c) kada TLTP obuhvaća i treće strane pružatelje IKT usluga, nije poduzela mjere za osiguranje sudjelovanja trećih strana, u skladu s člankom 26. stavkom 3. Uredbe (EU) 2022/2554

d) ne provodi djelotvorne kontrole upravljanja rizicima kako bi ublažila rizike od mogućeg učinka na podatke ili od oštećenja imovine i od poremećaja u radu ključnih ili važnih funkcija, usluga ili operacija, u skladu s člankom 26. stavkom 5. Uredbe (EU) 2022/2554

e) ne dostavi sažetak relevantnih nalaza ili planove za ispravljanje nedostataka ili dokumentaciju kojom se potvrđuje da je TLPT proveden u skladu sa zahtjevima, u skladu s člankom 26. stavcima 6. i 7. Uredbe (EU) 2022/2554

f) nije angažirala provoditelje testiranja, u skladu s člankom 26. stavkom 8. ili člankom 27. Uredbe (EU) 2022/2554

g) ne postupi u skladu s regulatornim tehničkim standardom koji je donesen na temelju članka 26. stavka 11. Uredbe (EU) 2022/2554

76. ne upravlja IKT rizikom povezanim s trećim stranama, u skladu s člankom 28. stavkom 1. Uredbe (EU) 2022/2554

77. nije donijela ili ne preispituje redovito strategiju za IKT rizik povezan s trećim stranama, u skladu s člankom 28. stavkom 2. Uredbe (EU) 2022/2554

78. ne vodi ili ne ažurira registar informacija o svim ugovornim aranžmanima o upotrebi IKT usluga koje pružaju treće strane pružatelji IKT usluga, u skladu s člankom 28. stavkom 3. Uredbe (EU) 2022/2554

79. nije nadležno tijelo izvijestila u skladu s člankom 28. stavkom 3. podstavkom 3. Uredbe (EU) 2022/2554 ili u skladu s člankom 28. stavkom 3. podstavkom 5. Uredbe (EU) 2022/2554

80. prije sklapanja ugovornog aranžmana o upotrebi IKT usluga nije provela sve elemente iz članka 28. stavka 4. Uredbe (EU) 2022/2554 ili članka 29. stavka 1. Uredbe (EU) 2022/2554

81. sklopi ugovor s trećom stranom pružateljem IKT usluga koji ne ispunjava odgovarajuće standarde informacijske sigurnosti, u skladu s člankom 28. stavkom 5. Uredbe (EU) 2022/2554

82. pri ostvarivanju prava na pristup, inspekcijski nadzor i reviziju u odnosu na treću stranu pružatelja IKT usluga nije utvrdila učestalost ili nije utvrdila područja revizije ili nije provjerila imaju li revizori odgovarajuće vještine i znanje, u skladu s člankom 28. stavkom 6. Uredbe (EU) 2022/2554

83. nije osigurala mogućnost raskida ugovornog angažmana o uporabi IKT usluga, u skladu s člankom 28. stavkom 7. Uredbe (EU) 2022/2554

84. nije uvela izlaznu strategiju ili nije osigurala da se može povući iz ugovornih aranžmana ili nije dokumentirala ili nije testirala izlazne planove, u skladu s člankom 28. stavkom 8. Uredbe (EU) 2022/2554

85. nije utvrdila alternativna rješenja ili nije izradila tranzicijske planove ili nije uspostavila odgovarajuće mjere za nepredvidive situacije, u skladu s člankom 28. stavkom 8. Uredbe (EU) 2022/2554

86. ne postupi u skladu s provedbenim tehničkim standardom koji je donesen na temelju članka 28. stavka 9. Uredbe (EU) 2022/2554

87. ne postupi u skladu s regulatornim tehničkim standardom koji je donesen na temelju članka 28. stavka 10. Uredbe (EU) 2022/2554

88. ne analizira koristi i troškove alternativnih rješenja, u skladu s člankom 29. stavkom 1. Uredbe (EU) 2022/2554

89. u slučaju podugovaranja IKT usluga kojima se podupiru ključne ili važne funkcije nije analizirala potencijalne koristi i rizike tog podugovaranja, u skladu s člankom 29. stavkom 2. Uredbe (EU) 2022/2554

90. nije utvrdila prava i obveze u pisanom obliku, u skladu s člankom 30. stavkom 1. Uredbe (EU) 2022/2554

91. ugovorni aranžmani o upotrebi IKT usluga koje će pružati treća strana pružatelj IKT usluga ne sadrže elemente kako je propisano člankom 30. stavkom 2. Uredbe (EU) 2022/2554

92. ugovorni aranžmani o upotrebi IKT usluga koje podupiru ključne ili važne funkcije koje će pružati treća strana pružatelj IKT usluga ne sadrže elemente kako je propisano člankom 30. stavkom 3. Uredbe (EU) 2022/2554

93. ne postupi u skladu s provedbenim tehničkim standardom koji je donesen na temelju članka 30. stavka 5. Uredbe (EU) 2022/2554

94. na zahtjev Agencije ili Hrvatske narodne banke za potrebe nadzora ne dostavi pisana objašnjenja ili odbije dati usmena objašnjenja, što je protivno članku 10. stavku 3. ovoga Zakona odnosno članku 11. stavku 3. ovoga Zakona

95. ne izvrši nadzornu mjeru koju je izrekla Agencija ili Hrvatska narodna banka ili nadzornu mjeru koju je izrekla Agencija ili Hrvatska narodna banka ne izvrši u roku koji je određen rješenjem, što je protivno članku 12. stavku 3. ovoga Zakona odnosno članku 13. stavku 3. ovoga Zakona.

(2) Novčanom kaznom u iznosu do 15.000,00 eura može se kazniti za prekršaj iz stavka 1. ovoga članka i odgovorna osoba u pravnoj osobi.

(3) Novčanom kaznom u iznosu do 15.000,00 eura kaznit će se član upravljačkog tijela pravne osobe ako:

1. ne utvrdi, ne odobri ili ne nadzire sve aranžmane povezane s okvirom za upravljanje IKT rizicima u skladu s člankom 5. stavkom 2. Uredbe (EU) 2022/2554

2. aktivno ne osvježava znanje i vještine koji su mu dostatni kako bi mogao razumjeti i procijeniti IKT rizik i njegov učinak na poslovanje, u skladu s člankom 5. stavkom 4. Uredbe (EU) 2022/2554

3. ne osigura da ga više IKT osoblje najmanje jedanput godišnje izvijesti o nalazima ili iznese preporuke, u skladu s člankom 13. stavkom 5. Uredbe (EU) 2022/2554

4. ne preispituje redovito rizike koji su utvrđeni u vezi s ugovornim aranžmanima o upotrebi IKT usluga u skladu s člankom 28. stavkom 2. Uredbe (EU) 2022/2554.

VI. PRIJELAZNE I ZAVRŠNA ODREDBA

Članak 20.

Usklađivanje s odredbama ovoga Zakona i Uredbe (EU) 2022/2554

Subjekti nadzora Agencije iz članka 8. stavka 2. ovoga Zakona dužni su uskladiti se s odredbama ovoga Zakona i Uredbe (EU) 2022/2554 najkasnije do 1. siječnja 2026.

Članak 21.

Rok za sklapanje sporazuma o suradnji između nadležnih tijela

(1) Agencija i Hrvatska narodna banka sklopit će sporazum o suradnji iz članka 9. stavka 3. ovoga Zakona u roku od šest mjeseci od dana stupanja na snagu ovoga Zakona.

(2) Ako Agencija i Hrvatska narodna banka ne sklope sporazum o suradnji iz članka 9. stavka 3. ovoga Zakona u roku iz stavka 1. ovoga članka ili ako Agencija i Hrvatska narodna banka u sporazumu o suradnji iz članka 9. stavka 3. ovoga Zakona ne urede sudjelovanje u Nadzornom forumu iz članka 32. Uredbe (EU) 2022/2554, Vlada Republike Hrvatske, na prijedlog ministra financija, imenovat će iz reda članova osoblja nadležnih tijela predstavnika i promatrača u Nadzorni forum u roku od šest mjeseci od dana isteka roka iz stavka 1. ovoga članka.

Članak 22.

Stupanje na snagu

Ovaj Zakon objavit će se u »Narodnim novinama«, a stupa na snagu 17. siječnja 2025.ž