# DELEGIRANA UREDBA KOMISIJE (EU) 2025/301

## od 23. listopada 2024.

## o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju sadržaj i rokovi za početnu obavijest, prijelazno i završno izvješće o značajnim IKT incidentima te sadržaj dobrovoljne obavijesti o ozbiljnim kiberprijetnjama

**(Tekst značajan za EGP)**

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (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 ([1]), a posebno njezin članak 20. treći stavak,

budući da:

(1) Radi usklađivanja i pojednostavnjenja zahtjeva u pogledu obavješćivanja i izvješćivanja o značajnim IKT incidentima iz članka 19. stavka 4. Uredbe (EU) 2022/2554, rokovi za izvješćivanje o značajnim IKT incidentima trebali bi biti dosljedni za sve vrste financijskih subjekata. Zbog toga bi se u pogledu rokova u najvećoj mogućoj mjeri trebao primjenjivati pristup koji je usklađen sa i po učinku barem istovjetan zahtjevima utvrđenima u Direktivi (EU) 2022/2555 Europskog parlamenta i Vijeća ([2]).

(2) Kako bi se izbjeglo nepotrebno opterećivanje financijskih subjekata zahtjevima za izvješćivanje u trenutku kad pokušavaju riješiti IKT incident, sadržaj početne obavijesti trebao bi biti ograničen na najvažnije informacije. Kako bi mogla poduzeti odgovarajuće nadzorne mjere, nadležna tijela trebaju dobiti informacije o značajnim IKT incidentima u najkraćem roku nakon što financijski subjekt klasificira IKT incident kao značajan. Stoga bi rok za dostavu početne obavijesti iz članka 19. stavka 4. točke (a) Uredbe (EU) 2022/2554 nakon klasifikacije IKT incidenta kao značajnog trebao biti što kraći, ali bi se istodobno trebala omogućiti određena fleksibilnost, posebno kad je riječ o poslovnim modelima usluga koji nisu osobito vremenski osjetljivi, u slučaju da financijskim subjektima zatreba više vremena za rješavanje IKT incidenta nakon što ga otkriju.

(3) Nakon primitka početne obavijesti nadležna tijela trebala bi primiti prijelazno izvješće s detaljnijim informacijama o IKT incidentu i završno izvješće sa svim relevantnim informacijama. Informacije u tim izvješćima trebale bi nadležnim tijelima omogućiti da dodatno procijene IKT incident i razmotre nadzorne mjere koje bi možda trebalo poduzeti.

(4) Rokovima za izvješćivanje iz članka 20. prvog stavka točke (a) podtočke ii. Uredbe (EU) 2022/2554 trebala bi se stoga postići ravnoteža između potrebe da nadležna tijela brzo dobiju informacije i potrebe da se financijskim subjektima osigura dovoljno vremena za prikupljanje potpunih i točnih informacija.

(5) Uzimajući u obzir kriterije utvrđene u članku 20. prvom stavku točki (a) Uredbe (EU) 2022/2554, rokovi za izvješćivanje ne bi trebali predstavljati nerazmjerno opterećenje za mikropoduzeća i druge financijske subjekte koji nisu značajni. Osim toga, kako bi se izbjeglo nerazmjerno opterećenje za financijske subjekte, pri utvrđivanju rokova za izvješćivanje trebalo bi voditi računa o vikendima i neradnim danima.

([1]) SL L 333, 27.12.2022., str. 1., ELI: http://data.europa.eu/eli/reg/2022/2554/oj.
([2]) Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80., ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Budući da se o ozbiljnim kiberprijetnjama izvješćuje dobrovoljno, sadržaj takvih obavijesti ne bi trebao opteretiti financijske subjekte te bi trebao biti ograničeniji od informacija koje se traže za značajne IKT incidente.

(7) Ova se Uredba temelji na nacrtu regulatornih tehničkih standarda koji su Komisiji dostavila europska nadzorna tijela.

(8) Europska nadzorna tijela provela su otvorena javna savjetovanja o nacrtu regulatornih tehničkih standarda na kojem se temelji ova Uredba, analizirala moguće povezane troškove i koristi te zatražila mišljenje interesnih skupina osnovanih u skladu s člankom 37. uredbi (EU) br. 1093/2010 ([3]), (EU) br. 1094/2010 ([4]) i (EU) br. 1095/2010 ([5]) Europskog parlamenta i Vijeća.

(9) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([6]) te je on dao pozitivno mišljenje 22. srpnja 2024. Svaka obrada osobnih podataka obuhvaćena područjem primjene ove Uredbe trebala bi se provoditi u skladu s primjenjivim načelima i odredbama o zaštiti podataka utvrđenima u Uredbi (EU) 2018/1725,

DONIJELA JE OVU UREDBU:

*Članak 1.*

**Opće informacije koje se navode u početnim obavijestima te prijelaznim i završnim izvješćima o značajnim IKT incidentima**

Financijski subjekti u početnoj obavijesti, prijelaznom izvješću i završnom izvješću iz članka 19. stavka 4. Uredbe (EU) 2022/2554 navode sljedeće opće informacije:

(a) vrstu podneska (početna obavijest, prijelazno izvješće ili završno izvješće);

(b) naziv, oznaku LEI i vrstu financijskog subjekta iz članka 2. stavka 1. Uredbe (EU) 2022/2554;

(c) naziv i identifikacijsku oznaku subjekta koji dostavlja početnu obavijest, prijelazno ili završno izvješće u ime financijskog subjekta;

(d) ako je primjenjivo, nazive i oznake LEI svih financijskih subjekata obuhvaćenih agregiranom početnom obavijesti ili agregiranim prijelaznim ili završnim izvješćem;

(e) podatke za kontakt osoba zaduženih za komunikaciju s nadležnim tijelom o značajnom IKT incidentu;

(f) ako je primjenjivo, identifikacijske podatke matičnog društva grupe kojoj financijski subjekt pripada;

(g) ako postoji monetarni učinak, valutu na kojoj se temelje iznosi.

([3]) Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SL L 331, 15.12.2010., str. 12., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju Europskog nadzornog tijela (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), o izmjeni Odluke br. 716/2009/EZ i o stavljanju izvan snage Odluke Komisije 2009/79/EZ (SL L 331, 15.12.2010., str. 48., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Uredba (EU) br. 1095/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), izmjeni Odluke br. 716/2009/EZ i stavljanju izvan snage Odluke Komisije 2009/77/EZ (SL L 331, 15.12.2010., str. 84., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

*Članak 2.*

**Posebne informacije koje se navode u početnim obavijestima**

Početne obavijesti iz članka 19. stavka 4. točke (a) Uredbe (EU) 2022/2554 sadržavaju barem sve sljedeće posebne informacije:

(a) referentnu oznaku incidenta koju je dodijelio financijski subjekt;

(b) datum i vrijeme otkrivanja i klasifikaciju incidenta u skladu s člankom 8. Delegirane uredbe Komisije (EU) 2024/1772 ([7]);

(c) opis IKT incidenta;

(d) kriterije utvrđene u člancima od 1. do 8. Delegirane uredbe (EU) 2024/1772 na temelju kojih je financijski subjekt klasificirao IKT incident kao značajan;

(e) države članice na koje IKT incident utječe;

(f) informacije o tome kako je IKT incident otkriven;

(g) ako su dostupne, informacije o izvoru IKT incidenta;

(h) informacije o tome je li financijski subjekt aktivirao plan kontinuiteta poslovanja;

(i) ako je primjenjivo, informacije o promjeni klasifikacije IKT incidenta iz značajnog u manje značajan;

(j) sve druge dostupne relevantne informacije.

*Članak 3.*

**Posebne informacije koje se navode u prijelaznim izvješćima**

Prijelazna izvješća iz članka 19. stavka 4. točke (b) Uredbe (EU) 2022/2554 sadržavaju barem sve sljedeće posebne informacije:

(a) ako je primjenjivo, referentnu oznaku incidenta koju je dodijelilo nadležno tijelo;

(b) datum i vrijeme nastanka IKT incidenta;

(c) ako je primjenjivo, datum i vrijeme kad je financijski subjekt ponovno uspostavio redovne aktivnosti;

(d) informacije o tome kako su ispunjeni kriteriji utvrđeni u člancima od 1. do 8. Delegirane uredbe (EU) 2024/1772 na temelju kojih je financijski subjekt klasificirao IKT incident kao značajan;

(e) vrstu IKT incidenta;

(f) ako je primjenjivo, prijetnje i tehnike aktera prijetnje;

(g) zahvaćena funkcionalna područja i poslovne procese;

(h) zahvaćene infrastrukturne komponente koje podupiru poslovne procese;

(i) učinak na financijske interese klijenata;

(j) informacije o izvješćivanju drugih tijela o IKT incidentu;

(k) privremene radnje ili mjere koje je financijski subjekt poduzeo ili planira poduzeti kako bi se oporavio od IKT incidenta;

(l) ako je primjenjivo, informacije o pokazateljima ugroženosti.

([7]) Delegirana uredba Komisije (EU) 2024/1772 od 13. ožujka 2024. o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju kriteriji za klasifikaciju IKT incidenata i kiberprijetnji, pragovi značajnosti i pojedinosti izvješća o značajnim incidentima (SL L, 2024/1772, 25.6.2024., ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

*Članak 4.*

**Posebne informacije koje se navode u završnim izvješćima**

Završna izvješća iz članka 19. stavka 4. točke (c) Uredbe (EU) 2022/2554 sadržavaju barem sve sljedeće posebne informacije:

(a) informacije o temeljnim uzrocima IKT incidenta;

(b) datum i vrijeme rješavanja IKT incidenta i otklanjanja njegovih temeljnih uzroka;

(c) informacije o rješavanju IKT incidenta;

(d) ako je primjenjivo, informacije relevantne za sanacijska tijela;

(e) informacije o izravnim i neizravnim troškovima i gubicima koje je prouzročio IKT incident te informacije o financijskim povratima;

(f) ako je primjenjivo, informacije o IKT incidentima koji se ponavljaju.

*Članak 5.*

**Rokovi za dostavu početne obavijesti, prijelaznog i završnog izvješća**

1. Financijski subjekti dostavljaju početnu obavijest te prijelazno i završno izvješće iz članka 19. stavka 4. točaka (a), (b) i (c) Uredbe (EU) 2022/2554 u sljedećim rokovima:

(a) početno izvješće: što je prije moguće, ali u svakom slučaju u roku od četiri sata od klasifikacije IKT incidenta kao značajnog, a najkasnije 24 sata od trenutka u kojem je financijski subjekt otkrio IKT incident;

(b) prijelazno izvješće: najkasnije u roku od 72 sata od dostave početne obavijesti, čak i ako se status incidenta ili postupanje u vezi s njim nisu promijenili kako je utvrđeno u članku 19. stavku 4. točki (b) Uredbe (EU) 2022/2554. Financijski subjekti dužni su dostaviti ažurirano prijelazno izvješće bez nepotrebne odgode, a u svakom slučaju kad se redovne aktivnosti ponovno uspostave;

(c) završno izvješće: najkasnije mjesec dana nakon dostave prijelaznog izvješća ili, ovisno o slučaju, nakon dostave najnovijeg ažuriranog prijelaznog izvješća.

2. Ako financijski subjekt nije klasificirao IKT incident kao značajan u roku od 24 sata od trenutka u kojem je taj incident otkrio, ali ga naknadno klasificira kao značajan, financijski subjekt dostavlja početnu obavijest u roku od četiri sata od klasifikacije IKT incidenta kao značajnog.

3. Financijski subjekti koji ne mogu dostaviti početnu obavijest, prijelazno izvješće ili završno izvješće u rokovima utvrđenima u stavku 1. o tome obavješćuju nadležno tijelo bez nepotrebne odgode, a najkasnije u rokovima za dostavu obavijesti odnosno izvješća, te navode razloge za kašnjenje.

4. Ako rok za dostavu početne obavijesti, prijelaznog izvješća ili završnog izvješća pada na dan vikenda ili neradni dan u državi članici izvještajnog financijskog subjekta, financijski subjekt može početnu obavijest, prijelazno ili završno izvješće dostaviti do podneva prvog sljedećeg radnog dana.

5. Stavak 4. ne primjenjuje se na početne obavijesti ili prijelazna izvješća koje dostavljaju kreditne institucije, središnje druge ugovorne strane, operatori mjesta trgovanja i drugi financijski subjekti koji su utvrđeni kao ključni ili važni subjekti u skladu s člankom 3. Direktive (EU) 2022/2555.

6. Nadležna tijela mogu odlučiti da se stavak 4. ne primjenjuje na početne obavijesti ili privremena izvješća koje dostavljaju financijski subjekti koji nisu navedeni u stavku 5., ali su značajni ili imaju sistemski značaj za financijski sektor na nacionalnoj razini ili razini Unije. Nadležna tijela obavješćuju predmetne financijske subjekte o svojoj odluci. Odluka nadležnog tijela primjenjuje se samo na incidente prijavljene nakon datuma na koji je nadležno tijelo o odluci obavijestilo predmetne financijske subjekte.

*Članak 6.*

**Sadržaj dobrovoljnih obavijesti o ozbiljnim kiberprijetnjama**

Dobrovoljna obavijest o ozbiljnim kiberprijetnjama iz članka 19. stavka 2. Uredbe (EU) 2022/2554 sadržava sve sljedeće informacije:

(a) opće informacije o financijskom subjektu koji dostavlja obavijest kako su utvrđene u članku 1.;

(b) datum i vrijeme otkrivanja ozbiljne kiberprijetnje i sve druge relevantne vremenske žigove povezane s ozbiljnom kiberprijetnjom;

(c) opis ozbiljne kiberprijetnje;

(d) informacije o mogućem učinku ozbiljne kiberprijetnje na financijski subjekt, njegove klijente ili partnerske financijske subjekte;

(e) klasifikacijske kriterije iz članaka od 1. do 8. Delegirane uredbe (EU) 2024/1772 koji bi rezultirali izradom izvješća o značajnom incidentu da se kiberprijetnja ostvarila;

(f) informacije o statusu ozbiljne kiberprijetnje i svim promjenama u aktivnosti prijetnje;

(g) ako je primjenjivo, opis mjera koje je financijski subjekt poduzeo kako bi spriječio ostvarenje ozbiljnih kiberprijetnji;

(h) informacije o svakoj obavijesti o ozbiljnoj kiberprijetnji koja je dostavljena drugim financijskim subjektima ili tijelima;

(i) ako je primjenjivo, informacije o pokazateljima ugroženosti;

(j) ako su dostupne, sve druge relevantne informacije.

*Članak 7.*

**Stupanje na snagu**

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 23. listopada 2024.

*Za Komisiju*
*Predsjednica*
Ursula VON DER LEYEN