Uradni list
Evropske unije

SL
Serija L

2025/301

20.2.2025

DELEGIRANA UREDBA KOMISIJE (EU) 2025/301

z dne 23. oktobra 2024

o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi, ki določajo vsebino in roke za začetno uradno obvestilo ter vmesno in končno poročilo o večjih incidentih, povezanih z IKT, ter vsebino prostovoljnega uradnega obvestila o pomembnih kibernetskih grožnjah

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 ([1]) ter zlasti člena 20, tretji pododstavek, Uredbe,

ob upoštevanju naslednjega:

(1) Za zagotovitev harmonizacije in racionalizacije zahtev glede uradnega obveščanja in poročanja o večjih incidentih, povezanih z IKT, iz člena 19(4) Uredbe (EU) 2022/2554 bi moral biti pri rokih za poročanje o večjih incidentih, povezanih z IKT, za vse vrste finančnih subjektov uporabljen dosleden pristop. Zato bi moral biti pri rokih tudi v največji možni meri uporabljen pristop, skladen z zahtevami iz Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta, in roki bi morali biti vsaj enakovredni tem zahtevam ([2]).

(2) Da finančni subjekti v času, ko obravnavajo incident, povezan z IKT, zaradi poročanja ne bi bili nepotrebno obremenjeni, bi morala biti vsebina začetnega uradnega obvestila omejena na najpomembnejše informacije. Da bi pristojni organi lahko sprejeli ustrezne nadzorne ukrepe, morajo informacije o večjih incidentih, povezanih z IKT, prejeti čim prej po tem, ko je finančni subjekt incident, povezan z IKT, razvrstil kot večji incident. Zato bi moral biti rok za predložitev začetnega uradnega obvestila iz člena 19(4), točka (a), Uredbe (EU) 2022/2554 čim prej po razvrstitvi incidenta, povezanega z IKT, kot večjega, hkrati pa še vedno omogočati prožnost, zlasti za poslovne modele storitev, ki niso posebej časovno občutljivi, če finančni subjekti potrebujejo več časa za obravnavo incidenta, povezanega z IKT, po tem, ko zanj izvejo.

(3) Po prejemu začetnega uradnega obvestila bi morali pristojni organi v vmesnem poročilu prejeti podrobnejše informacije o incidentu, povezanem z IKT, v končnem poročilu pa vse relevantne informacije. Informacije v teh poročilih bi morale pristojnim organom omogočiti, da nadalje ocenijo incidente, povezane z IKT, in ovrednotijo nadzorne ukrepe, ki bi jih morda želeli sprejeti.

(4) Roki za poročanje iz člena 20, prvi odstavek, točka (a)(ii), Uredbe (EU) 2022/2554 bi morali zato zagotavljati ravnotežje med potrebo, da pristojni organi prejmejo informacije hitro, in potrebo, da se finančnim subjektom da na voljo dovolj časa za pridobitev popolnih in točnih informacij.

(5) Ob upoštevanju meril iz člena 20, prvi odstavek, točka (a), Uredbe (EU) 2022/2554 roki za poročanja ne bi smeli nesorazmerno obremeniti mikropodjetij in drugih finančnih subjektov, ki niso pomembni finančni subjekti. Da bi se izognili nesorazmernemu bremenu za finančne subjekte, bi se morali pri rokih za poročanje upoštevati konci tedna in prazniki.

([1]) UL L 333, 27.12.2022, str. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Ker se o pomembnih kibernetskih grožnjah obvešča prostovoljno, vsebina takih uradnih obvestil ne bi smela obremeniti finančnih subjektov in bi morala biti bolj omejena kot informacije, ki se zahtevajo za večje incidente, povezane z IKT.

(7) Ta uredba temelji na osnutku regulativnih tehničnih standardov, ki so ga Komisiji predložili evropski nadzorni organi.

(8) Evropski nadzorni organi so opravili odprta javna posvetovanja o osnutku regulativnih tehničnih standardov, na katerem temelji ta uredba, analizirali morebitne povezane stroške in koristi ter zaprosili za nasvet interesne skupine, ustanovljene v skladu s členom 37 uredb (EU) št. 1093/2010 ([3]), (EU) št. 1094/2010 ([4]) in (EU) št. 1095/2010 ([5]) Evropskega parlamenta in Sveta.

(9) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([6]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je pozitivno mnenje podal 22. julija 2024. Vsaka obdelava osebnih podatkov v okviru področja uporabe te uredbe bi morala potekati v skladu z veljavnimi načeli in določbami o varstvu podatkov iz Uredbe (EU) 2018/1725 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Splošne informacije, ki jih je treba navesti v začetnih uradnih obvestilih ter vmesnih in končnih poročilih o večjih incidentih, povezanih z IKT

Finančni subjekti v začetno uradno obvestilo, vmesno in končno poročilo iz člena 19(4) Uredbe (EU) 2022/2554 vključijo naslednje splošne informacije:

(a) vrsto predložitve (začetno uradno obvestilo, vmesno ali končno poročilo);

(b) ime finančnega subjekta, njegovo kodo LEI in vrsto finančnega subjekta iz člena 2(1) Uredbe (EU) 2022/2554;

(c) ime in identifikacijsko kodo subjekta, ki predloži začetno uradno obvestilo ali vmesno ali končno poročilo za finančni subjekt;

(d) kjer je ustrezno, imena in kode LEI vseh finančnih subjektov, zajetih v zbirnem začetnem uradnem obvestilu ali vmesnem ali končnem poročilu;

(e) kontaktne podatke oseb, odgovornih za komunikacijo s pristojnim organom o večjem incidentu, povezanem z IKT;

(f) kjer je ustrezno, identifikacijo obvladujočega podjetja skupine, katere del je finančni subjekt;

(g) v primeru monetarnega učinka, valuto, na kateri temeljijo zneski.

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Uredba (EU) št. 1094/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za zavarovanja in poklicne pokojnine) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/79/ES (UL L 331, 15.12.2010, str. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Uredba (EU) št. 1095/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za vrednostne papirje in trge) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/77/ES (UL L 331, 15.12.2010, str. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Člen 2

Specifične informacije, ki jih je treba navesti v začetnih uradnih obvestilih

Začetna uradna obvestila iz člena 19(4), točka (a), Uredbe (EU) 2022/2554 vsebujejo vsaj vse naslednje specifične informacije:

(a) referenčno kodo incidenta, ki jo dodeli finančni subjekt;

(b) datum odkritja, čas odkritja in razvrstitev incidenta v skladu s členom 8 Delegirane uredbe Komisije (EU) 2024/1772 ([7]);

(c) opis incidenta, povezanega z IKT;

(d) merila iz členov 1 do 8 Delegirane uredbe (EU) 2024/1772, na podlagi katerih je finančni subjekt incident, povezan z IKT, razvrstil kot večji incident;

(e) države članice, na katere vpliva incident, povezan z IKT;

(f) informacije o tem, kako je bil odkrit incident, povezan z IKT;

(g) informacije o izvoru incidenta, povezanega z IKT, če so na voljo;

(h) informacije o tem, ali je finančni subjekt aktiviral načrt neprekinjenega poslovanja;

(i) kjer je ustrezno, informacije o prerazvrstitvi incidenta, povezanega z IKT, iz večjega v manjšega;

(j) vse druge relevantne informacije, če so na voljo.

Člen 3

Specifične informacije, ki jih je treba navesti v vmesnih poročilih

Vmesna poročila iz člena 19(4), točka (b), Uredbe (EU) 2022/2554 vsebujejo vsaj vse naslednje specifične informacije:

(a) kjer je ustrezno, referenčno kodo incidenta, ki jo zagotovi pristojni organ;

(b) datum in čas nastanka incidenta, povezanega z IKT;

(c) kjer je ustrezno, datum in čas, ko je finančni subjekt obnovil svoje redne dejavnosti;

(d) informacije o tem, kako so izpolnjena merila iz členov 1 do 8 Delegirane uredbe (EU) 2024/1772, na podlagi katerih je finančni subjekt incident, povezan z IKT, razvrstil kot večji;

(e) vrsto incidenta, povezanega z IKT;

(f) kjer je ustrezno, grožnje in tehnike, ki jih uporablja akter grožnje;

(g) prizadeta funkcionalna področja in poslovni procesi;

(h) prizadete infrastrukturne komponente, ki podpirajo poslovne procese;

(i) vpliv na finančne interese strank;

(j) informacije o poročanju o incidentu, povezanem z IKT, drugim organom;

(k) začasne ukrepe ali ukrepe, ki jih je finančni subjekt sprejel ali jih namerava sprejeti za okrevanje po incidentu, povezanem z IKT;

(l) kjer je ustrezno, informacije o kazalnikih ogroženosti.

([7]) Delegirana uredba Komisije (EU) 2024/1772 z dne 13. marca 2024 o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi o določitvi meril za razvrščanje incidentov, povezanih z IKT, in kibernetskih groženj, ter pragov pomembnosti in podrobnosti poročil o večjih incidentih (UL L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Člen 4

Specifične informacije, ki jih je treba navesti v končnih poročilih

Končna poročila iz člena 19(4), točka (c), Uredbe (EU) 2022/2554 vsebujejo vse naslednje specifične informacije:

(a) informacije o temeljnih vzrokih incidenta, povezanega z IKT;

(b) datume in čas, ko je bil incident, povezan z IKT, rešen in so bili obravnavani temeljni vzroki;

(c) informacije o reševanju incidenta, povezanega z IKT;

(d) kjer je ustrezno, informacije, ki so relevantne za organe za reševanje;

(e) informacije o neposrednih in posrednih stroških in izgubah zaradi incidenta, povezanega z IKT, ter informacije o finančnih izterjavah;

(f) kjer je ustrezno, informacije o ponavljajočih se incidentih, povezanih z IKT.

Člen 5

Roki za začetno uradno obvestilo ter vmesna in končna poročila

1. Finančni subjekti predložijo začetno uradno obvestilo ter vmesno in končno poročilo iz člena 19(4), točke (a), (b) in (c), Uredbe (EU) 2022/2554 v naslednjih rokih:

(a) za začetno poročilo: čim prej, vsekakor pa v štirih urah po tem, ko je bil incident, povezan z IKT, razvrščen kot večji incident, povezan z IKT, in najpozneje v 24 urah od trenutka, ko je finančni subjekt izvedel za incident, povezan z IKT;

(b) za vmesno poročilo: najpozneje v 72 urah od predložitve začetnega uradnega obvestila, tudi če se status ali obravnava incidenta nista spremenila, kot je navedeno v členu 19(4), točka (b), Uredbe (EU) 2022/2554. Finančni subjekti brez nepotrebnega odlašanja, v vsakem primeru pa po obnovitvi rednih dejavnosti, predložijo posodobljeno vmesno poročilo;

(c) za končno poročilo: najpozneje en mesec po predložitvi vmesnega poročila ali, kjer je ustrezno, po zadnjem posodobljenem vmesnem poročilu.

2. Če finančni subjekt incidenta, povezanega z IKT, ni razvrstil kot večjega v 24 urah od trenutka, ko je finančni subjekt izvedel za incident, povezan z IKT, a ga je kot večjega razvrstil pozneje, finančni subjekt predloži začetno uradno obvestilo v štirih urah po tem, ko je bil incident, povezan z IKT, razvrščen kot večji incident.

3. Finančni subjekti, ki ne morejo predložiti začetnega uradnega obvestila, vmesnega ali končnega poročila v rokih iz odstavka 1, o tem brez nepotrebnega odlašanja, vendar najpozneje v ustreznih rokih za predložitev uradnega obvestila ali poročila, obvestijo pristojni organ in pojasnijo razloge za zamudo.

4. Če je rok za predložitev začetnega uradnega obvestila, vmesnega ali končnega poročila konec tedna ali praznik v državi članici finančnega subjekta, ki poroča, lahko finančni subjekt predloži začetno uradno obvestilo, vmesno ali končno poročilo do 12.00 naslednjega delovnega dne.

5. Odstavek 4 se ne uporablja za predložitev začetnega uradnega obvestila ali vmesnega poročila kreditnih institucij, centralnih nasprotnih strank, upravljavcev mest trgovanja in drugih finančnih subjektov, ki so opredeljeni kot bistveni ali pomembni subjekti v skladu s členom 3 Direktive (EU) 2022/2555.

6. Pristojni organi lahko odločijo, da se odstavek 4 ne uporablja za predložitev začetnega uradnega obvestila ali vmesnega poročila finančnih subjektov, pri čemer so izvzeti tisti finančni subjekti iz odstavka 5, ki so pomembni ali imajo sistemski značaj za finančni sektor na nacionalni ravni ali ravni Unije. Pristojni organi o svoji odločitvi uradno obvestijo ustrezne finančne subjekte. Odločitev pristojnega organa se uporablja samo v zvezi z incidenti, o katerih se poroča po datumu, ko pristojni organ ustrezne finančne subjekte uradno obvesti o odločitvi.

Člen 6

Vsebina prostovoljnega uradnega obvestila o pomembnih kibernetskih grožnjah

Vsebina prostovoljnega uradnega obvestila o pomembnih kibernetskih grožnjah iz člena 19(2) Uredbe (EU) 2022/2554 zajema vse naslednje:

(a) splošne informacije o finančnem subjektu predložitelju, kot je določeno v členu 1;

(b) datum in čas odkritja pomembne kibernetske grožnje in vse druge relevantne časovne žige, povezane s pomembno kibernetsko grožnjo;

(c) opis pomembne kibernetske grožnje;

(d) informacije o morebitnem vplivu pomembne kibernetske grožnje na finančni subjekt, njegove stranke ali finančne partnerje;

(e) merila za razvrstitev, ki bi sprožila poročilo o večjem incidentu iz členov 1 do 8 Delegirane uredbe (EU) 2024/1772, če bi se kibernetska grožnja uresničila;

(f) informacije o statusu pomembne kibernetske grožnje in vseh spremembah grožnje;

(g) kjer je ustrezno, opis ukrepov, ki jih je finančni subjekt sprejel za preprečitev uresničitve pomembnih kibernetskih groženj;

(h) informacije o vsakem uradnem obvestilu o pomembni kibernetski grožnji drugim finančnim subjektom ali organom;

(i) kjer je ustrezno, informacije o kazalnikih ogroženosti;

(j) vse druge relevantne informacije, če so na voljo.

Člen 7

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 23. oktobra 2024

Za Komisijo
predsednica
Ursula VON DER LEYEN