Uradni list
Evropske unije

SL
Serija L

2025/302

20.2.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/302

z dne 23. oktobra 2024

o določitvi izvedbenih tehničnih standardov za uporabo Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi s standardnimi obrazci, predlogami in postopki, v okviru katerih finančni subjekti poročajo o večjem incidentu, povezanem z IKT, in uradno obveščajo o pomembni kibernetski grožnji

(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, četrti odstavek, Uredbe,

ob upoštevanju naslednjega:

(1) Za zagotovitev, da finančni subjekti svojim pristojnim organom dosledno poročajo o večjih incidentih in da jim posredujejo kakovostne podatke, bi bilo treba določiti, katera podatkovna polja morajo finančni subjekti zagotoviti v različnih fazah poročanja iz člena 19(4) Uredbe (EU) 2022/2554. Pomembno je, da so te informacije predstavljene na način, ki omogoča enoten pregled incidenta. Zato je treba za te namene določiti enotno predlogo za poročanje.

(2) Finančni subjekti morajo izpolniti tista podatkovna polja predloge za poročanje, ki ustrezajo zahtevam glede informacij iz zadevnega uradnega obvestila ali poročila. Vendar bi bilo treba finančnim subjektom, ki že imajo informacije, ki jih morajo zagotoviti v poznejši fazi poročanja, tj. v vmesnem ali končnem poročilu, omogočiti, da predčasno predložijo podatke.

(3) Ker lahko več incidentov ali ponavljajoči se incidenti pomenijo večji incident iz člena 8 Delegirane uredbe Komisije (EU) 2024/1772 ([2]), bi moralo oblikovanje predloge za poročanje in podatkovnih polj finančnim subjektom omogočiti, da poročajo o takih ponavljajočih se incidentih.

(4) Za zagotovitev točnih in posodobljenih informacij bi morala predloga za poročanje finančnim subjektom omogočiti, da ob predložitvi vmesnega in končnega poročila posodobijo vse predhodno predložene informacije in po potrebi prerazvrstijo večje incidente med manjše.

(5) Pravno identifikacijo subjektov bi bilo treba uskladiti z identifikatorji, določenimi v izvedbenih tehničnih standardih, sprejetih v skladu s členom 28(9) Uredbe (EU) 2022/2554.

(6) Kadar finančni subjekti obveznosti poročanja o večjih incidentih, povezanih z IKT, oddajo v zunanje izvajanje tretji osebi, bi morali biti pristojni organi pred predložitvijo prvega uradnega obvestila ali poročanja seznanjeni z identiteto tretje osebe, ki poroča v imenu finančnega subjekta, da se preveri legitimnost tretje osebe, ki poroča.

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

([2]) 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).

(7) Za lažjo opredelitev vpliva incidenta, ki se je zgodil pri tretjem ponudniku ali ki ga je povzročil tretji ponudnik in vpliva na več finančnih subjektov v eni državi članici, ter za zmanjšanje poročanja za finančne subjekte bi morala predloga za poročanje omogočati predložitev zbirnega poročila, ki zajema zbirne informacije o vplivu incidenta na vse prizadete finančne subjekte, ki so incident razvrstili kot večji.

(8) Predloga za poročanje bi morala biti zasnovana na tehnološko nevtralen način, da se omogoči njena uporaba v različnih rešitvah za poročanje o incidentih, ki že obstajajo ali bi se lahko razvile za izvajanje zahtev iz Uredbe (EU) 2022/2554.

(9) Oblika predloge za poročanje in podatkovnih polj bi morala tretjim osebam, ki so jim finančni subjekti v skladu s členom 19(5) Uredbe (EU) 2022/2554 oddali svoje obveznosti poročanja v zunanje izvajanje, olajšati poročanje o večjih incidentih, povezanih z IKT.

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

(11) Evropski nadzorni organi so o osnutku izvedbenih tehničnih standardov, na katerih temelji ta uredba, izvedli odprta javna posvetovanja, analizirali morebitne s tem povezane stroške in koristi ter zaprosili za nasvet interesno skupino za bančništvo, ustanovljeno v skladu s členom 37 uredb (EU) št. 1093/2010 ([3]), (EU) št. 1094/2010 ([4]), (EU) št. 1095/2010 ([5]) Evropskega parlamenta in Sveta.

(12) 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. Vsako obdelavo osebnih podatkov v okviru področja uporabe te uredbe bi bilo treba izvesti v skladu z veljavnimi načeli in določbami o varstvu podatkov iz Uredbe (EU) 2018/1725 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Predloga za poročanje o večjih incidentih, povezanih z IKT

1. Finančni subjekti za predložitev začetnega uradnega obvestila, vmesnega poročila in končnega poročila iz člena 19(4) Uredbe (EU) 2022/2554 uporabijo predlogo iz Priloge I, kot sledi:

(a) finančni subjekti, ki predložijo začetno uradno obvestilo, izpolnijo podatkovna polja predloge, ki ustrezajo informacijam, ki jih je treba zagotoviti v skladu s členom 2 Delegirane uredbe Komisije (EU) 2025/301 ([7]), in lahko, kadar že imajo te informacije, izpolnijo tista podatkovna polja, katerih izpolnitev se ne zahteva za začetno uradno obvestilo, temveč za vmesno ali končno poročilo;

([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).

([7]) 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 (UL L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

(b) finančni subjekti, ki predložijo vmesno poročilo, izpolnijo podatkovna polja predloge, ki ustrezajo informacijam, ki jih je treba zagotoviti v skladu s členom 3 Delegirane uredbe (EU) 2025/301, in lahko, kadar že imajo relevantne informacije, izpolnijo podatkovna polja, katerih izpolnitev se ne zahteva za vmesno poročilo, temveč za končno poročilo;

(c) finančni subjekti, ki predložijo končno poročilo, izpolnijo podatkovna polja predloge, ki ustrezajo informacijam, ki jih je treba zagotoviti v skladu s členom 4 Delegirane uredbe (EU) 2025/301

2. Finančni subjekti zagotovijo, da so informacije v začetnem uradnem obvestilu ter v vmesnem in končnem poročilu popolne in točne.

3. Finančni subjekti zagotovijo ocenjene vrednosti na podlagi drugih razpoložljivih podatkov in informacij, kolikor je to mogoče, kadar v času poročanja za začetno uradno obvestilo ali vmesno poročilo točni podatki niso na voljo.

4. Finančni subjekti pri predložitvi vmesnega ali končnega poročila uporabijo predlogo iz Priloge I, da predložijo vse potrebne informacije in po potrebi posodobijo informacije, ki so bile predhodno predložene v začetnem uradnem obvestilu ali v vmesnem poročilu.

5. Finančni subjekti pri izpolnjevanju predloge iz Priloge I upoštevajo podatkovni glosar in navodila iz Priloge II.

Člen 2

Skupna predložitev začetnega uradnega obvestila, vmesnih in končnih poročil

Finančni subjekti lahko združijo predložitev začetnega uradnega obvestila, vmesnega poročila in končnega poročila, da zagotovijo dva ali vse hkrati, kadar so se redne dejavnosti obnovile ali je bila analiza temeljnih vzrokov zaključena in pod pogojem, da so upoštevani roki iz člena 5 Delegirane uredbe (EU) 2025/301.

Člen 3

Ponavljajoči se incidenti, povezani z IKT

Finančni subjekti, ki zagotavljajo informacije o manjših ponavljajočih se incidentih, povezanih z IKT, ki kumulativno izpolnjujejo pogoje za en večji incident, povezan z IKT, iz člena 8(2) Delegirane uredbe (EU) 2024/1772, te informacije zagotovijo v zbirni obliki.

Člen 4

Uporaba varnih elektronskih kanalov

1. Finančni subjekti za predložitev začetnega uradnega obvestila ter vmesnega in končnega poročila uporabljajo varne elektronske kanale, ki jih da na voljo njihov pristojni organ.

2. Finančni subjekti, ki ne morejo uporabljati varnih elektronskih kanalov, ki jih je dal na voljo njihov pristojni organ, svoj pristojni organ o večjem incidentu, povezanem z IKT, obvestijo na drug varen način, o katerem se dogovorijo s pristojnim organom. Če to zahteva pristojni organ, finančni subjekti, ko to lahko storijo, ponovno predložijo začetno uradno obvestilo ali vmesno ali končno poročilo prek varnega elektronskega kanala, ki ga da na voljo njihov pristojni organ.

Člen 5

Prerazvrstitev večjih incidentov, povezanih z IKT

Če finančni subjekt po nadaljnji oceni ugotovi, da incident, povezan z IKT, o katerem se je predhodno poročalo kot o večjem, nikoli ni izpolnjeval meril in pragov za razvrstitev iz člena 8 Delegirane uredbe (EU) 2024/1772, pristojni organ uradno obvesti, da je incident, povezan z IKT, prerazvrstil iz večjega v manjšega, tako da informacije o tej prerazvrstitvi navede v predlogi iz Priloge II k tej uredbi v zvezi s polji „vrsta poročila“ in „druge informacije“.

Člen 6

Uradno obveščanje o oddaji obveznosti poročanja v zunanje izvajanje

1. Finančni subjekti, ki so obveznost poročanja o večjih incidentih, povezanih z IKT, oddali v zunanje izvajanje v skladu s členom 19(5) Uredbe (EU) 2022/2554, o tem dogovoru o zunanjem izvajanju obvestijo svoj pristojni organ takoj po sklenitvi dogovora o zunanjem izvajanju in najpozneje pred začetnim uradnim obvestilom ali poročanjem.

2. Finančni subjekti pristojnemu organu predložijo ime, kontaktne podatke in identifikacijsko kodo tretje osebe, ki jim bo predložila uradna obvestila ali poročila o večjih incidentih, povezanih z IKT.

3. Finančni subjekti obvestijo svoj pristojni organ takoj, ko svojih obveznosti poročanja iz člena 19(5) Uredbe (EU) 2022/2554 ne oddajajo več v zunanje izvajanje.

Člen 7

Zbirno poročanje

1. Tretji ponudnik storitev, ki so mu bile obveznosti poročanja oddane v zunanje izvajanje, kot je navedeno v členu 19(5) Uredbe (EU) 2022/2554, lahko uporabi predlogo iz Priloge I k tej uredbi, da v enem samem uradnem obvestilu ali poročilu zagotovi zbirne informacije o večjem incidentu, povezanem z IKT, ki vpliva na več finančnih subjektov, ter to uradno obvestilo ali poročilo predloži pristojnemu organu v imenu vseh prizadetih finančnih subjektov, če so izpolnjeni vsi naslednji pogoji:

(a) večji incident, povezan z IKT, o katerem je treba poročati, izvira od tretjega ponudnika storitev IKT ali ga je povzročil tretji ponudnik storitev IKT;

(b) ta tretji ponudnik storitev zagotavlja zadevno storitev IKT več kot enemu finančnemu subjektu ali skupini;

(c) vsak finančni subjekt, zajet v zbirnem uradnem obvestilu ali poročilu, incident, povezan z IKT, razvrsti kot večji incident;

(d) večji incident, povezan z IKT, vpliva na finančne subjekte v eni sami državi članici, zbirno poročilo pa se nanaša na finančne subjekte, ki jih nadzira isti pristojni organ;

(e) pristojni organi so tej vrsti finančnih subjektov izrecno dovolili združevanje njihovega poročanja.

2. Odstavek 1 se ne uporablja za kreditne institucije, ki se štejejo za zelo pomembne v skladu s členom 2, točka 16, Uredbe (EU) št. 468/2014 Evropske centralne banke ([8]), upravljavce mest trgovanja in centralne nasprotne stranke, ki za predložitev uradnega obvestila ali poročil o večjih incidentih, povezanih z IKT, svojemu pristojnemu organu uporabljajo samo predlogo iz Priloge I.

3. Če pristojni organi zahtevajo informacije o posameznem vplivu večjega incidenta, povezanega z IKT, na en sam finančni subjekt, finančni subjekt na zahtevo pristojnega organa predloži individualno uradno obvestilo ali poročilo o večjem incidentu, povezanem z IKT.

([8]) Uredba (EU) št. 468/2014 Evropske centralne banke z dne 16. aprila 2014 o vzpostavitvi okvira za sodelovanje znotraj enotnega mehanizma nadzora med Evropsko centralno banko in pristojnimi nacionalnimi organi ter z imenovanimi nacionalnimi organi (okvirna uredba o EMN) (ECB/20214/17) (UL L 141, 14.5.2014, str. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Člen 8

Uradno obveščanje o pomembnih kibernetskih grožnjah

1. Finančni subjekti, ki v skladu s členom 19(2) Uredbe (EU) 2022/2554 pristojnim organom priglasijo pomembne kibernetske grožnje, uporabijo predlogo iz Priloge III k tej uredbi ter upoštevajo podatkovni glosar in navodila iz Priloge IV k tej uredbi.

2. Finančni subjekti zagotovijo, da so informacije v uradnem obvestilu o pomembnih kibernetskih grožnjah popolne in točne.

Člen 9

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

PRILOGA I

PREDLOGE ZA POROČANJE O VEČJIH INCIDENTIH

Število polja	Podatkovno polje	
Splošne informacije o finančnem subjektu		
1.1	Vrsta predložitve	
1.2	Ime subjekta, ki predloži poročilo	
1.3	Identifikacijska koda subjekta, ki predloži poročilo	
1.4	Vrsta prizadetega finančnega subjekta	
1.5	Ime prizadetega finančnega subjekta	
1.6	Koda LEI prizadetega finančnega subjekta	
1.7	Ime glavne kontaktne osebe	
1.8	Elektronski naslov glavne kontaktne osebe	
1.9	Telefonska številka glavne kontaktne osebe	
1.10	Ime nadomestne kontaktne osebe	
1.11	Elektronski naslov nadomestne kontaktne osebe	
1.12	Telefonska številka nadomestne kontaktne osebe	
1.13	Ime končnega obvladujočega podjetja	
1.14	Koda LEI končnega obvladujočega podjetja	
1.15	Valuta poročanja	
Vsebina začetnega uradnega obvestila		
2.1	Referenčna koda incidenta, ki jo dodeli finančni subjekt	
2.2	Datum in čas odkritja večjega incidenta, povezanega z IKT	
2.3	Datum in čas razvrstitve incidenta, povezanega z IKT, med večje	
2.4	Opis večjega incidenta, povezanega z IKT	
2.5	Merila za razvrščanje, ki so sprožila poročilo o incidentu	
2.6	Pragovi pomembnosti za merilo za razvrščanje „geografska razpršenost“	
2.7	Odkritje večjega incidenta, povezanega z IKT	

Število polja	Podatkovno polje	
2.8	Navedba, ali večji incident, povezan z IKT, izvira od tretjega ponudnika ali drugega finančnega subjekta	
2.9	Aktivacija načrta neprekinjenega poslovanja, če je aktiviran	
2.10	Druge relevantne informacije	
Vsebina vmesnega poročila		
3.1	Referenčna koda incidenta, ki jo zagotovi pristojni organ	
3.2	Datum in čas pojave večjega incidenta, povezanega z IKT	
3.3	Datum in čas, ko so bile storitve, dejavnosti ali operacije obnovljene	
3.4	Število prizadetih strank	
3.5	Odstotek prizadetih strank	
3.6	Število prizadetih finančnih partnerjev	
3.7	Odstotek prizadetih finančnih partnerjev	
3.8	Vpliv na pomembne stranke ali finančne partnerje	
3.9	Število prizadetih transakcij	
3.10	Odstotek prizadetih transakcij	
3.11	Vrednost prizadetih transakcij	
3.12	Informacije o tem, ali gre za dejanske številke ali ocene oziroma ali ni bilo nobenega vpliva	
3.13	Vpliv na ugled	
3.14	Spremne informacije o vplivu na ugled	
3.15	Trajanje večjega incidenta, povezanega z IKT	
3.16	Nedelovanje storitve	
3.17	Informacije o tem, ali gre pri trajanju in nedelovanju storitev za dejanske podatke ali ocene	
3.18	Vrste učinkov v državah članicah	
3.19	Opis, kakšen je vpliv večjega incidenta, povezanega z IKT, v drugih državah članicah	
3.20	Pragovi pomembnosti za merilo za razvrščanje „izgube podatkov“	
3.21	Opis izgub podatkov	

Število polja	Podatkovno polje	
3.22	Merilo za razvrščanje „prizadete kritične storitve“	
3.23	Vrsta večjega incidenta, povezanega z IKT	
3.24	Druge vrste incidentov	
3.25	Grožnje in tehnike, ki jih uporablja akter groženj	
3.26	Druge vrste tehnik	
3.27	Informacije o prizadetih funkcionalnih področjih in poslovnih procesih	
3.28	Prizadete infrastrukturne komponente, ki podpirajo poslovne procese	
3.29	Informacije o prizadetih infrastrukturnih komponentah, ki podpirajo poslovne procese	
3.30	Vpliv na finančne interese strank	
3.31	Poročanje drugim organom	
3.32	Določitev „drugih“ organov	
3.33	Začasne dejavnosti/ukrepi, ki so bili sprejeti ali se načrtujejo za okrevanje po incidentu	
3.34	Opis vseh začasnih dejavnosti in ukrepov, ki so bili sprejeti ali se načrtujejo za okrevanje po incidentu	
3.35	Kazalniki ogroženosti	
Vsebina končnega poročila		
4.1	Razvrščanje temeljnih vzrokov incidenta na visoki ravni	
4.2	Podrobna razvrstitev temeljnih vzrokov incidenta	
4.3	Dodatna razvrstitev temeljnih vzrokov incidenta	
4.4	Druge vrste temeljnih vzrokov	
4.5	Informacije o temeljnih vzrokih incidenta	
4.6	Povzetek o reševanja incidentov	
4.7	Datum in čas, ko je bil obravnavan temeljni vzrok incidenta	
4.8	Datum in čas, ko je bil incident rešen	
4.9	Informacije, ali se datum trajne rešitve incidenta razlikuje od prvotno načrtovanega datuma izvedbe	
4.10	Ocena tveganja za kritične funkcije za namene reševanja	
4.11	Informacije, relevantne za organe za reševanje	

Število polja	Podatkovno polje	
4.12	Prag pomembnosti za merilo za razvrščanje „gospodarski učinek“	
4.13	Znesek bruto neposrednih in posrednih stroškov in izgub	
4.14	Znesek finančnih izterjav	
4.15	Informacije o tem, ali so se manjši incidenti ponavljali	
4.16	Datum in čas pojave ponavljajočih se incidentov	

PRILOGA II

PODATKOVNI GLOSAR IN NAVODILA ZA POROČANJE O VEČJIH INCIDENTIH

Podatkovno polje		Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
Splošne informacije o finančnem subjektu						
1.1	Vrsta predložitve	Navedite vrsto uradnega obvestila o incidentu ali poročila, ki se predloži pristojnemu organu.	Da	Da	Da	Izbira: — začetno uradno obvestilo; — vmesno poročilo; — končno poročilo; — večji incident, prerazvrščen med manjše incidente.
1.2	Ime subjekta, ki predloži poročilo	Polno pravno ime subjekta, ki predloži poročilo.	Da	Da	Da	Alfanumerično
1.3	Identifikacijska koda subjekta, ki predloži poročilo	Identifikacijska koda subjekta, ki predloži poročilo. Kadar finančni subjekti predložijo uradno obvestilo/poročilo, je identifikacijska koda identifikator pravnih subjektov (LEI), ki je edinstvena 20-mestna alfanumerična koda na podlagi standarda ISO 17442-1:2020. Tretji ponudnik, ki predloži poročilo za finančni subjekt, lahko uporabi identifikacijsko kodo, kot je določena v izvedbenih tehničnih standardih, sprejetih v skladu s členom 28(9) Uredbe (EU) 2022/2554 .	Da	Da	Da	Alfanumerično
1.4	Vrsta prizadetega finančnega subjekta	Vrsta subjekta iz člena 2(1), točke (a) do (t), Uredbe (EU) 2022/2554, za katerega se predloži poročilo. V primeru zbirnega poročanja iz člena 7 te uredbe se izberejo različne vrste finančnih subjektov, zajetih v zbirnem poročilu.	Da	Da	Da	Izbira (več možnosti): — kreditna institucija; — plačilna institucija; — izvzeta plačilna institucija; — ponudnik storitev zagotavljanja informacij o računih; — institucija za izdajo elektronskega denarja; — izvzeta institucija za izdajo elektronskega denarja; — investicijsko podjetje; — ponudnik storitev v zvezi s kriptosredstvi; — izdajatelj žetonov, vezanih na sredstva; — centralna depotna družba; — centralna nasprotna stranka; — mesto trgovanja; — repozitorij sklenjenih poslov;

Podatkovno polje		Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
						— upravitelj alternativnega investicijskega sklada; — družba za upravljanje; — izvajalec storitev sporočanja podatkov; — zavarovalnica in pozavarovalnica; — zavarovalni posrednik, pozavarovalni posrednik in posrednik dopolnilnih zavarovanj; — institucija za poklicno pokojninsko zavarovanje; — bonitetna agencija; — upravljavec ključnih referenčnih vrednosti; — ponudnik storitev množičnega financiranja; — repozitorij listinjenja.
1.5	Ime prizadetega finančnega subjekta	Polno pravno ime finančnega subjekta, ki ga je prizadel večji incident, povezan z IKT, in ki mora o večjem incidentu poročati svojemu pristojnemu organu v skladu s členom 19 Uredbe (EU) 2022/2554. V primeru zbirnega poročanja: (a) seznam vseh imen finančnih subjektov, ki jih je prizadel večji incident, povezan z IKT, ločenih s podpičjem; (b) tretji ponudnik, ki predloži uradno obvestilo ali poročilo o večjem incidentu ali, kot je navedeno v členu 7 te uredbe, v zbirni obliki navede imena vseh finančnih subjektov, na katere je incident vplival, ločena s podpičjem.	Da, če se finančni subjekt, ki ga je prizadel incident, razlikuje od subjekta, ki je predložil poročilo, in v primeru zbirnega poročanja.	Da, če se finančni subjekt, ki ga je prizadel incident, razlikuje od subjekta, ki je predložil poročilo, in v primeru zbirnega poročanja.	Da, če se finančni subjekt, ki ga je prizadel incident, razlikuje od subjekta, ki je predložil poročilo, in v primeru zbirnega poročanja.	Alfanumerično
1.6	Koda LEI prizadetega finančnega subjekta	Identifikator pravnih subjektov (LEI) finančnega subjekta, ki ga je prizadel večji incident, povezan z IKT, ki je dodeljen v skladu z Mednarodno organizacijo za standardizacijo. V primeru zbirnega poročanja: (a) seznam vseh kod LEI finančnih subjektov, ki jih je prizadel večji incident, povezan z IKT, ločenih s podpičjem;	Da, če se finančni subjekt, ki ga je prizadel večji incident, povezan z IKT,	Da, če se finančni subjekt, ki ga je prizadel večji incident, povezan z IKT, razlikuje od subjekta, ki	Da, če se finančni subjekt, ki ga je prizadel večji incident, povezan z IKT,	Edinstvena 20-mestna alfanumerična koda na podlagi standarda ISO 17442-1:2020

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	(b) tretji ponudnik, ki predloži uradno obvestilo ali poročilo o večjem incidentu v zbirni obliki, kot je navedeno v členu 7 te uredbe, navede kode LEI vseh finančnih subjektov, na katere je incident vplival, ločene s podpičjem. Vrstni red kod LEI in imen finančnih subjektov je enak.	razlikuje od subjekta, ki je predložil poročilo, in v primeru zbirnega poročanja.	je predložil poročilo, in v primeru zbirnega poročanja.	razlikuje od subjekta, ki je predložil poročilo, in v primeru zbirnega poročanja.	
1.7 Ime glavne kontaktne osebe	Ime in priimek glavne kontaktne osebe finančnega subjekta. V primeru zbirnega poročanja iz člena 7 te uredbe ime glavne kontaktne osebe v subjektu, ki predloži zbirno poročilo.	Da	Da	Da	Alfanumerično
1.8 Elektronski naslov glavne kontaktne osebe	Elektronski naslov glavne kontaktne osebe, ki ga lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih. V primeru zbirnega poročanja iz člena 7 te uredbe elektronski naslov glavne kontaktne osebe v subjektu, ki predloži zbirno poročilo.	Da	Da	Da	Alfanumerično
1.9 Telefonska številka glavne kontaktne osebe	Telefonska številka glavne kontaktne osebe, ki jo lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih. V primeru zbirnega poročanja iz člena 7 te uredbe telefonska številka glavne kontaktne osebe v subjektu, ki predloži zbirno poročilo. Telefonska številka se sporoči z vsemi mednarodnimi klicnimi številkami (npr. +33XXXXXXXXX).	Da	Da	Da	Alfanumerično
1.10 Ime nadomestne kontaktne osebe	Ime in priimek nadomestne kontaktne osebe ali ime odgovorne skupine finančnega subjekta ali subjekta, ki je predložil poročilo v imenu finančnega subjekta.	Da	Da	Da	Alfanumerično
1.11 Elektronski naslov nadomestne kontaktne osebe	Elektronski naslov nadomestne kontaktne osebe ali namenski elektronski naslov skupine, ki ga lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih.	Da	Da	Da	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
1.12 Telefonska številka nadomestne kontaktne osebe	Telefonska številka nadomestne kontaktne osebe ali skupine, ki jo lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih. Telefonska številka se sporoči z vsemi mednarodnimi klicnimi številkami (npr. +33XXXXXXXXX).	Da	Da	Da	Alfanumerično
1.13 Ime končnega obvladujočega podjetja	Ime končnega obvladujočega podjetja skupine, ki ji pripada prizadeti finančni subjekt, če je ustrezno.	Da, če finančni subjekt pripada skupini.	Da, če finančni subjekt pripada skupini.	Da, če finančni subjekt pripada skupini.	Alfanumerično
1.14 Koda LEI končnega obvladujočega podjetja	Identifikator pravnih subjektov (LEI) končnega obvladujočega podjetja skupine, ki ji pripada prizadeti finančni subjekt, če je ustrezno. Dodeljen v skladu z Mednarodno organizacijo za standardizacijo.	Da, če finančni subjekt pripada skupini.	Da, če finančni subjekt pripada skupini.	Da, če finančni subjekt pripada skupini.	Edinstvena 20-mestna alfanumerična koda na podlagi standarda ISO 17442-1:2020.
1.15 Valuta poročanja	Valuta, ki se uporablja pri poročanju o incidentih	Da	Da	Da	Polje se izpolni s kodami valute po standardu ISO 4217.
Vsebina začetnega uradnega obvestila					
2.1 Referenčna koda incidenta, ki jo dodeli finančni subjekt	Edinstvena referenčna koda, ki jo izda finančni subjekt, ki na nedvoumen način opredeljuje večji incident, povezan z IKT. V primeru zbirnega poročanja iz člena 7 te uredbe referenčna koda incidenta, ki jo dodeli tretji ponudnik.	Da	Da	Da	Alfanumerično
2.2 Datum in čas odkritja incidenta, povezanega z IKT	Datum in čas, ko je finančni subjekt izvedel za incident, povezan z IKT. Za ponavljajoče se incidente datum in čas, ko je bil odkrit zadnji incident, povezan z IKT.	Da	Da	Da	Čas UTC v obliki zapisa po standardu 8601 (LLLL-MM-DD Thh. mm.ss)

Podatkovno polje		Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
2.3	Datum in čas razvrstitve incidenta kot večjega	Datum in čas, ko je bil incident, povezan z IKT, razvrščen kot večji v skladu z merili za razvrščanje iz Delegirane uredbe (EU) 2024/1772.	Da	Da	Da	Čas UTC v obliki zapisa po standardu 8601 (LLLL-MM-DD Thh. mm.ss)
2.4	Opis incidenta, povezanega z IKT	Opis najpomembnejših vidikov večjega incidenta, povezanega z IKT. Finančni subjekti zagotovijo pregled na visoki ravni naslednjih informacij, kot so možni vzroki, neposredni učinki, prizadeti sistemi in drugo. Finančni subjekti vključijo, kadar je znano ali razumno pričakovano, ali incident vpliva na tretje ponudnike ali druge finančne subjekte, vrsto ponudnika ali finančnega subjekta, njihovo ime, njihove identifikacijske kode in vrsto identifikacijske kode (npr. LEI ali EUID). V naslednjih poročilih se lahko vsebina polja sčasoma spremeni, da odraža stalno razumevanje incidenta, povezanega z IKT, in opisuje vse druge pomembne informacije o incidentu, povezanem z IKT, ki niso zajete v podatkovnih poljih, vključno z notranjo oceno resnosti, ki jo izvede finančni subjekt (npr. zelo nizka, nizka, srednja, visoka, zelo visoka), ter navedbo ravni in imena najvišjih organov struktur odločanja, ki so bile vključene v odziv na incident, povezan z IKT.	Da	Da	Da	Alfanumerično
2.5	Merila za razvrščanje, ki so sprožila poročilo o incidentu	Merila za razvrščanje na podlagi Delegirane uredbe (EU) 2024/1772, ki so sprožila določitev incidenta, povezanega z IKT, kot večjega ter poznejše obveščanje in poročanje. V primeru zbirnega poročanja iz člena 7 te uredbe merila za razvrščanje, ki so sprožila določitev incidenta, povezanega z IKT, kot večjega za vsaj enega ali več finančnih subjektov.	Da	Da	Da	Izbira (več možnosti): — prizadete stranke, finančni partnerji in transakcije; — vpliv na ugled; — trajanje in nedelovanje storitve; — geografska razpršenost; — izgube podatkov; — prizadete kritične storitve; — gospodarski učinek.
2.6	Pragovi pomembnosti za merilo za razvrščanje „geografska razpršenost“	Države članice EGP, na katere je vplival večji incident, povezan z IKT. Finančni subjekti pri ocenjevanju učinka večjega incidenta, povezanega z IKT, v drugih državah članicah upoštevajo člena 4 in 12 Delegirane uredbe (EU) 2024/1772.	Da, če je dosežen prag „geografska razpršenost“.	Da, če je dosežen prag „geografska razpršenost“.	Da, če je dosežen prag „geografska razpršenost“.	Izbira (več možnosti), izpolnjeno z uporabo kode ISO 3166 ALPHA-2 prizadetih držav

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
2.7 Odkritje večjega incidenta, povezanega z IKT	Navedba, kako je bil odkrit večji incident, povezan z IKT.	Da	Da	Da	Izbira: — varnost IT; — osebje; — notranja revizija; — zunanja revizija; — stranke; — finančni partnerji; — tretji ponudnik; — napadalec; — sistemi spremljanja; — organ/agencija/organ pregona; — drugo.
2.8 Navedba, ali incident izvira od tretjega ponudnika ali drugega finančnega subjekta	Navedba, ali večji incident, povezan z IKT, izvira od tretjega ponudnika ali drugega finančnega subjekta. Finančni subjekti navedejo, ali večji incident, povezan z IKT, izvira od tretjega ponudnika ali drugega finančnega subjekta (vključno s finančnimi subjekti, ki spadajo v isto skupino kot subjekt, ki poroča), ter ime, identifikacijsko kodo tretjega ponudnika ali finančnega subjekta in vrsto identifikacijske kode (npr. LEI ali EUID).	Da, če incident izvira od tretjega ponudnika ali drugega finančnega subjekta.	Da, če incident izvira od tretjega ponudnika ali drugega finančnega subjekta.	Da, če incident izvira od tretjega ponudnika ali drugega finančnega subjekta.	Alfanumerično
2.9 Aktivacija načrta neprekinjenega poslovanja, če je aktiviran	Navedba, ali je prišlo do uradne aktivacije ukrepov za odzivanje na neprekinjeno poslovanje finančnega subjekta.	Da	Da	Da	Boolova izbira (da ali ne)
2.10 Druge relevantne informacije	Vse dodatne informacije, ki niso zajete v predlogi. Finančni subjekti, ki so večji incident, povezan z IKT, prerazvrstili kot manjši incident, opišejo razloge, zakaj incident, povezan z IKT, ne izpolnjuje in se ne pričakuje, da bo izpolnjeval merila, da bi bil razvrščen kot večji incident, povezan z IKT.	Da, če obstajajo druge informacije, ki niso zajete v predlogi,	Da, če obstajajo druge informacije, ki niso zajete v predlogi, ali če je bil	Da, če obstajajo druge informacije, ki niso zajete v predlogi,	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
		ali če je bil večji incident, povezan z IKT, prerazvrščen kot manjši incident.	večji incident, povezan z IKT, prerazvrščen kot manjši incident.	ali če je bil večji incident, povezan z IKT, prerazvrščen kot manjši incident.	
Vsebina vmesnega poročila					
3.1 Referenčna koda incidenta, ki jo zagotovi pristojni organ	Edinstvena referenčna koda, ki jo pristojni organ dodeli ob prejemu začetnega uradnega obvestila za nedvoumno opredelitev večjega incidenta, povezanega z IKT.	Ne	Da, če se uporablja.	Da, če se uporablja.	Alfanumerično
3.2 Datum in čas pojave incidenta	Datum in čas, ko se je zgodil večji incident, povezan z IKT, če se razlikujeta od časa, ko je finančni subjekt izvedel za večji incident, povezan z IKT. Za ponavljajoče se večje incidente, povezane z IKT, datum in čas, ko se je zgodil zadnji večji incident, povezan z IKT.	Ne	Da	Da	Čas UTC v obliki zapisa po standardu 8601 (LLLL-MM-DD Thh. mm.ss)
3.3 Datum in čas, ko so bile storitve, dejavnosti ali operacije obnovljene	Informacije o datumu in času obnovitve storitev, dejavnosti ali operacij, na katere je vplival večji incident, povezan z IKT.	Ne	Da, če je bilo izpolnjeno podatkovno polje 3.16. „nedelovanje storitve“	Da, če je bilo izpolnjeno podatkovno polje 3.16. „nedelovanje storitve“	Čas UTC v obliki zapisa po standardu 8601 (LLLL-MM-DD Thh. mm.ss)
3.4 Število prizadetih strank	Število strank, ki jih je prizadel večji incident, povezan z IKT, in ki uporabljajo storitev, ki jo zagotavlja finančni subjekt. Finančni subjekti pri ocenjevanju števila prizadetih strank v svoji oceni upoštevajo člen 1(1) in člen 9(1), točka (b), Delegirane uredbe (EU) 2024/1772. Finančni subjekt, ki ne more določiti dejanskega števila prizadetih strank, uporabi ocene na podlagi razpoložljivih podatkov iz primerljivih referenčnih obdobij. V primeru zbirnega poročanja iz člena 7 te uredbe skupno število prizadetih strank pri vseh finančnih subjektih.	Ne	Da	Da	Celo število

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
3.5 Odstotek prizadetih strank	Odstotek strank, ki jih je prizadel večji incident, povezan z IKT, glede na skupno število strank, ki uporabljajo prizadeto storitev, ki jo zagotavlja finančni subjekt. V primeru več kot ene prizadete storitve se storitve združijo. Finančni subjekti pri svoji oceni upoštevajo člen 1(1) in člen 9(1), točka (a), Delegirane uredbe (EU) 2024/1772. Finančni subjekt, ki ne more določiti dejanskega odstotka prizadetih strank, uporabi ocene na podlagi razpoložljivih podatkov iz primerljivih referenčnih obdobij. V primeru zbirnega poročanja iz člena 7 te uredbe finančni subjekt vsoto vseh prizadetih strank deli s skupnim številom strank vseh prizadetih finančnih subjektov.	Ne	Da	Da	Izraženo v odstotkih, katera koli vrednost do 5 numeričnih znakov, vključno z največ 1 decimalnim mestom, izražena v odstotkih (npr. 2,4 namesto 2,4 %). Če ima vrednost za decimalno vejico več kot 1 številko, jo nasprotne stranke poročevalke zaokrožijo navzgor.
3.6 Število prizadetih finančnih partnerjev	Število finančnih partnerjev, ki jih je prizadel večji incident, povezan z IKT, in ki so sklenili pogodbo s finančnim subjektom. Finančni subjekti pri ocenjevanju števila prizadetih finančnih partnerjev v svoji oceni upoštevajo člen 1(2) Delegirane uredbe (EU) 2024/1772. Finančni subjekt, ki ne more določiti dejanskega števila prizadetih finančne partnerjev, uporabi ocene na podlagi razpoložljivih podatkov iz primerljivih referenčnih obdobij. V primeru zbirnega poročanja iz člena 7 te uredbe skupno število prizadetih finančnih partnerjev pri vseh finančnih subjektih.	Ne	Da	Da	Celo število

Podatkovno polje		Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
3.7	Odstotek prizadetih finančnih partnerjev	Odstotek finančnih partnerjev, ki jih je prizadel večji incident, povezan z IKT, glede na skupno število finančnih partnerjev, ki so sklenili pogodbo s finančnim subjektom. Finančni subjekti pri ocenjevanju odstotka prizadetih finančnih partnerjev v svoji oceni upoštevajo člen 1(1) in člen 9(1), točka (c), Delegirane uredbe (EU) 2024/1772. Finančni subjekt, ki ne more določiti dejanskega odstotka prizadetih finančnih partnerjev, uporabi ocene na podlagi razpoložljivih podatkov iz primerljivih referenčnih obdobij. V primeru zbirnega poročanja iz člena 7 te uredbe navedite vsoto vseh prizadetih finančnih partnerjev, deljeno s skupnim številom finančnih partnerjev vseh prizadetih finančnih subjektov.	Ne	Da	Da	Izraženo v odstotkih, katera koli vrednost do 5 numeričnih znakov, vključno z največ 1 decimalnim mestom, izražena v odstotkih (npr. 2,4 namesto 2,4 %). Če ima vrednost za decimalno vejico več kot 1 številko, jo nasprotne stranke poročevalke zaokrožijo navzgor.
3.8	Vpliv na pomembne stranke ali finančne partnerje	Kakršen koli ugotovljen vpliv na pomembne stranke ali finančnega partnerja iz člena 1(3) in člena 9(1), točka (f), Delegirane uredbe (EU) 2024/1772.	Ne	Da, če je dosežen prag za „pomembnost strank in finančnih partnerjev“.	Da, če je dosežen prag za „pomembnost strank in finančnih partnerjev“.	Boolova izbira (da ali ne)
3.9	Število prizadetih transakcij	Število transakcij, prizadetih zaradi večjega incidenta, povezanega z IKT. Finančni subjekti pri ocenjevanju vpliva na transakcije upoštevajo člen 1(4) Delegirane uredbe (EU) 2024/1772, vključno z vsemi prizadetimi domačimi in čezmejnimi transakcijami, ki zajemajo denarni znesek, pri katerih je bil vsaj en del transakcije izveden v Uniji.	Ne	Da, če je incident prizadel katero koli transakcijo.	Da, če je incident prizadel katero koli transakcijo.	Celo število

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	Finančni subjekt, ki ne more določiti dejanskega števila prizadetih transakcij, uporabi ocene, ki temeljijo na razpoložljivih podatkih iz primerljivih referenčnih obdobij. V primeru zbirnega poročanja iz člena 7 te uredbe navedite skupno število prizadetih transakcij za vse finančne subjekte.				
3.10 Odstotek prizadetih transakcij	Odstotek prizadetih transakcij glede na dnevno povprečno število domačih in čezmejnih transakcij, ki jih je izvedel finančni subjekt v zvezi s prizadeto storitvijo. Finančni subjekti upoštevajo člen 1(4) in člen 9(1), točka (d), Delegirane uredbe (EU) 2024/1772. Finančni subjekt, ki ne more določiti dejanskega odstotka prizadetih transakcij, mora uporabiti ocene. V primeru zbirnega poročanja iz člena 7 te uredbe finančni subjekt sešteje vse prizadete transakcije in vsoto deli s skupnim številom transakcij vseh prizadetih finančnih subjektov.	Ne	Da, če je incident prizadel katero koli transakcijo.	Da, če je incident prizadel katero koli transakcijo.	Izraženo v odstotkih, katera koli vrednost do 5 numeričnih znakov, vključno z največ 1 decimalnim mestom, izražena v odstotkih (npr. 2,4 namesto 2,4 %). Če ima vrednost za decimalno vejico več kot 1 številko, jo nasprotne stranke poročevalke zaokrožijo navzgor.
3.11 Vrednost prizadetih transakcij	Skupna vrednost transakcij, ki jih je prizadel večji incident, povezan z IKT, se oceni v skladu s členom 1(4) in členom 9(1), točka (e), Delegirane uredbe (EU) 2024/1772. Finančni subjekt, ki ne more določiti dejanske vrednosti prizadetih transakcij, uporabi ocene, ki temeljijo na razpoložljivih podatkih iz primerljivih referenčnih obdobij. Finančni subjekt poroča o denarnem znesku kot pozitivni vrednosti. V primeru zbirnega poročanja iz člena 7 te uredbe skupna vrednost prizadetih transakcij pri vseh finančnih subjektih.	Ne	Da, če je incident prizadel katero koli transakcijo.	Da, če je incident prizadel katero koli transakcijo.	Monetarno Finančni subjekti poročajo o podatkovni točki v enotah z najmanjšo natančnostjo, ki je enakovredna tisoč enotam (npr. 2,5 namesto 2 500 EUR).

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
3.12 Informacije o tem, ali gre za dejanske številke ali ocene oziroma ali ni bilo nobenega vpliva	Informacije o tem, ali so vrednosti, poročane v podatkovnih poljih 3.4 do 3.11, dejanske vrednosti ali ocene oziroma ali ni bilo nobenega vpliva.	Ne	Da	Da	Izbira (več možnosti): — dejanski zneski za prizadete stranke; — dejanski zneski za prizadete finančne partnerje; — dejanski zneski za prizadete transakcije; — ocene za prizadete stranke; — ocene za prizadete finančne partnerje; — ocene za prizadete transakcije; — brez vpliva na stranke; — brez vpliva na finančne partnerje; — brez vpliva na transakcije.
3.13 Vpliv na ugled	Informacije o vplivu večjega incidenta, povezanega z IKT, na ugled iz členov 2 in 10 Delegirane uredbe (EU) 2024/1772. V primeru zbirnega poročanja iz člena 7 te uredbe kategorije vpliva na ugled, ki se uporabljajo za vsaj en finančni subjekt.	Ne	Da, če je izpolnjeno polje za merilo „vpliv na ugled“.	Da, če je izpolnjeno polje za merilo „vpliv na ugled“.	Izbira (več možnosti): — o večjem incidentu, povezanem z IKT, se je poročalo v medijih; — večji incident, povezan z IKT, je povzročil ponavljajoče se pritožbe različnih strank ali finančnih partnerjev v zvezi s storitvami, namenjenimi strankam, ali ključnimi poslovnimi odnosi; — finančni subjekt zaradi večjega incidenta, povezanega z IKT, ne bo mogel ali verjetno ne bo mogel izpolniti regulativnih zahtev; — finančni subjekt bo ali bo verjetno zaradi večjega incidenta, povezanega z IKT, izgubil stranke ali finančne partnerje, kar bo pomembno vplivalo na njegovo poslovanje.
3.14 Spremne informacije o vplivu na ugled	Informacije, ki opisujejo, kako je večji incident, povezan z IKT, vplival ali bi lahko vplival na ugled finančnega subjekta, vključno s kršitvami zakonodaje, neizpolnjenimi regulativnimi zahtevami, številom pritožb strank in drugim.	Ne	Da, če je izpolnjeno polje za merilo „vpliv na ugled“.	Da, če je izpolnjeno polje za merilo „vpliv na ugled“.	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	Spremne informacije vključujejo vrsto medijev (npr. tradicionalni in digitalni mediji, blogi, pretočne platforme) in medijsko pokritost, vključno z dosegom medijev (lokalni, nacionalni, mednarodni). Medijska pokritost v tem kontekstu ne pomeni nekaj negativnih komentarjev sledilcev ali uporabnikov družbenih omrežij. Finančni subjekt navede tudi, ali je medijska pokritost izpostavila pomembna tveganja za njegove stranke v zvezi z večjim incidentom, povezanim z IKT, vključno s tveganjem insolventnosti finančnega subjekta ali tveganjem izgube sredstev. Finančni subjekti navedejo tudi, ali so medijem, ki so bili uporabljeni za zanesljivo obveščanje javnosti o večjem incidentu, povezanem z IKT, in njegovih posledicah, zagotovili informacije. Finančni subjekti lahko navedejo tudi, ali so bile v medijih navedene napačne informacije v zvezi z incidentom, povezanim z IKT, vključno z informacijami, ki temeljijo na namernih napačnih informacijah, ki so jih širili akterji groženj, ali informacijami, ki se nanašajo na ali ponazarjajo poškodovanje spletnega mesta finančnega subjekta.				
3.15 Trajanje incidenta	Finančni subjekti merijo trajanje večjega incidenta, povezanega z IKT, od trenutka, ko se je večji incident, povezan z IKT, zgodil, do trenutka, ko je bil incident rešen. Finančni subjekti, ki ne morejo določiti trenutka, ko je prišlo do večjega incidenta, povezanega z IKT, merijo trajanje večjega incidenta, povezanega z IKT, od trenutka, ko ga je finančni subjekt odkril, ali od trenutka, ko ga je zabeležil v omrežnih ali sistemskih dnevnikih ali drugih virih podatkov, odvisno od tega, kaj se je zgodilo prej. Finančni subjekti, ki še ne vedo, kdaj bo večji incident, povezan z IKT, rešen, uporabijo ocene. Vrednost se izrazi v dnevih, urah in minutah. V primeru zbirnega poročanja iz člena 7 te uredbe finančni subjekti merijo najdaljše trajanje večjega incidenta, povezanega z IKT, če so med finančnimi subjekti razlike.	Ne	Da	Da	DD.HH.MM

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
3.16 Nedelovanje storitve	Nedelovanje storitve, merjeno od trenutka, ko storitev v celoti ali delno ni na voljo strankam, finančnim partnerjem ali drugim notranjim ali zunanjim uporabnikom, do trenutka, ko so bili redne dejavnosti ali delovanje obnovljeni na raven storitve, ki je bila zagotovljena pred večjim incidentom, povezanim z IKT. Kadar nedelovanje storitve povzroči zamudo pri zagotavljanju storitev po obnovitvi rednih dejavnosti ali operacij, finančni subjekti merijo čas nedelovanja od začetka večjega incidenta, povezanega z IKT, do trenutka, ko je navedena zapoznela storitev zagotovljena. Finančni subjekti, ki ne morejo določiti trenutka, ko se je začelo nedelovanje storitve, merijo nedelovanje storitve od trenutka, ko je bil incident odkrit, ali trenutka, ko je bil zabeležen, odvisno od tega, kaj se je zgodilo prej. V primeru zbirnega poročanja iz člena 7 te uredbe finančni subjekti merijo najdaljše trajanje nedelovanja storitve v primeru razlik med finančnimi subjekti.	Ne	Da, če je incident povzročil nedelovanje storitve.	Da, če je incident povzročil nedelovanje storitve.	DD.HH.MM
3.17 Informacije o tem, ali gre pri trajanju in nedelovanju storitev za dejanske podatke ali ocene.	Informacije o tem, ali gre pri vrednostih, ki so poročane v podatkovnih poljih 3.15 in 3.16, za dejanske podatke ali ocene	Ne	Da, če je izpolnjeno polje za merilo „trajanje in nedelovanje storitve“.	Da, če je izpolnjeno polje za merilo „trajanje in nedelovanje storitve“.	Izbira: — dejanski podatki; — ocene; — dejanski podatki in ocene; — podatki niso na voljo;
3.18 Vrste učinkov v državah članicah	Vrsta učinka v zadevnih državah članicah EGP. Navedba, ali je imel večji incident, povezan z IKT, učinek v drugih državah članicah EGP (ki niso država članica pristojnega organa, kateremu se incident neposredno poroča) v skladu s členom 4 Delegirane uredbe (EU) 2024/1772, zlasti pomen učinka na: (a) prizadete stranke in finančne partnerje v drugih državah članicah; ali	Ne	Da, če je dosežen prag „geografska razpršenost“.	Da, če je dosežen prag „geografska razpršenost“.	Izbira (več možnosti): — stranke; — finančni partnerji; — podružnica finančnega subjekta; — finančni subjekti v skupini, ki opravljajo dejavnosti v zadevni državi članici; — infrastruktura finančnega trga; — tretji ponudniki, ki lahko zagotavljajo storitve drugim finančnim subjektom.

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	(b) podružnice ali druge finančne subjekte v skupini, ki opravljajo dejavnosti v drugih državah članicah; ali (c) infrastrukture finančnega trga ali tretje ponudnike, ki lahko vplivajo na finančne subjekte v drugih državah članicah, za katere opravljajo storitve.				
3.19 Opis, kakšen je vpliv incidenta v drugih državah članicah	Opis vpliva in resnosti večjega incidenta, povezanega z IKT, v vsaki prizadeti državi članici, vključno z oceno vpliva in resnosti na: (a) stranke; (b) finančne partnerje; (c) podružnice finančnega subjekta; (d) druge finančne subjekte v skupini, ki opravljajo dejavnosti v zadevni državi članici; (e) infrastrukture finančnega trga; (f) tretje ponudnike, ki lahko zagotavljajo storitve drugim finančnim subjektom, kakor je ustrezno v drugih državah članicah.	Ne	Da, če je dosežen prag „geografska razpršenost“.	Da, če je dosežen prag „geografska razpršenost“.	Alfanumerično
3.20 Pragovi pomembnosti za merilo za razvrščanje „izgube podatkov“	Vrsta izgub podatkov, ki jih povzroči večji incident, povezan z IKT, v smislu razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti podatkov. Finančni subjekti pri svoji oceni upoštevajo člena 5 in 13 Delegirane uredbe (EU) 2024/1772. V primeru zbirnega poročanja iz člena 7 te uredbe izgube podatkov, ki vplivajo na vsaj en finančni subjekt.	Ne	Da, če je izpolnjeno polje za merilo „izgube podatkov“.	Da, če je izpolnjeno polje za merilo „izgube podatkov“.	Izbira (več možnosti): — razpoložljivost; — avtentičnost; — celovitost; — zaupnost.
3.21 Opis izgub podatkov	Opis učinka večjega incidenta, povezanega z IKT, na razpoložljivost, avtentičnost, celovitost in zaupnost kritičnih podatkov v skladu s členoma 5 in 13 Delegirane uredbe (EU) 2024/1772. Informacije o vplivu na izvajanje poslovnih ciljev finančnega subjekta ali na izpolnjevanje regulativnih zahtev. Finančni subjekti v okviru obveščanja navedejo, ali gre pri zadevnih podatkih za podatke o strankah, podatke o drugih subjektih (npr. finančnih partnerjih) ali podatke o samem finančnem subjektu.	Ne	Da, če je izpolnjeno polje za merilo „izgube podatkov“.	Da, če je izpolnjeno polje za merilo „izgube podatkov“.	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	Finančni subjekt lahko navede tudi vrsto podatkov, ki so povezani z incidentom – zlasti, ali so podatki zaupni in katera vrsta zaupnosti je bila vključena (npr. poslovna zaupnost, osebni podatki, poslovna skrivnost: bančna tajnost, zavarovalniška skrivnost, tajnost glede izvajanja plačilnih storitev itd.). Informacije lahko vključujejo tudi morebitna tveganja, povezana z izgubami podatkov, na primer, ali se lahko podatki, na katere vpliva incident, uporabijo za identifikacijo posameznikov in ali bi jih lahko akter grožnje uporabil za pridobitev kredita ali posojil brez njihovega soglasja za izvedbo napadov z lažnim predstavljanjem ali za javno razkritje informacij. V primeru zbirnega poročanja iz člena 7 te uredbe splošni opis učinka incidenta na prizadete finančne subjekte. V primeru razlik v učinku se v opisu učinka jasno navede konkreten učinek na različne finančne subjekte.				
3.22 Merilo za razvrščanje „prizadete kritične storitve“	Informacije, povezane z merilom „prizadete kritične storitve“. Finančni subjekti pri svoji oceni upoštevajo člen 6 Delegirane uredbe (EU) 2024/1772, vključno z informacijami o: — prizadetih storitvah ali dejavnostih, za katere se zahteva dovoljenje ali registracija ali ki jih nadzorujejo pristojni organi; ali — storitvah IKT ali omrežnih in informacijskih sistemih, ki podpirajo kritične ali pomembne funkcije finančnega subjekta; in — naravi zlonamernega in nepooblaščenega dostopa do omrežnih in informacijskih sistemov finančnega subjekta. V primeru zbirnega poročanja iz člena 7 te uredbe učinek na kritične storitve, ki se uporabljajo za vsaj en finančni subjekt.	Ne	Da	Da	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
3.23 Vrsta incidenta	Razvrščanje incidentov po vrsti.	Ne	Da	Da	Izbira (več možnosti): — povezano s kibernetsko varnostjo; — napaka v postopku; — napaka v sistemu; — zunanji dogodek; — povezano s plačili; — drugo (navedite).
3.24 Druge vrste incidentov	Druge vrste incidentov, povezanih z IKT: finančni subjekti, ki so v podatkovnem polju 3.23 izbrali „druge“ vrste incidentov, navedejo vrsto incidenta, povezanega z IKT.	Ne	Da, če je v podatkovnem polju 3.23 izbrana „druga“ vrsta incidentov.	Da, če je v podatkovnem polju 3.23 izbrana „druga“ vrsta incidentov.	Alfanumerično
3.25 Grožnje in tehnike, ki jih uporablja akter groženj	Navedite grožnje in tehnike, ki jih uporablja akter grožnje, vključno z naslednjim: (a) socialni inženiring, vključno z lažnim predstavljanjem (phishing); (b) porazdeljeni napad za zavrnitev storitve ((D)DoS); (c) kraja identitete; (d) šifriranje podatkov za vpliv, vključno z izsiljevalsko programsko opremo; (e) ugrabitev virov; (f) nepooblaščeno filtriranje in manipulacija podatkov, razen kraje identitete; (g) uničenje podatkov; (h) poškodovanje; (i) napad na dobavno verigo; (j) drugo (navedite).	Ne	Da, če je vrsta incidenta, povezanega z IKT, v polju 3.23 „povezana s kibernetsko varnostjo“.	Da, če je vrsta incidenta, povezanega z IKT, v polju 3.23 „povezana skibernetsko varnostjo“.	Izbira (več možnosti): — socialni inženiring (vključno z lažnim predstavljanjem (phishing); — porazdeljeni napad za zavrnitev storitve ((D)DoS); — kraja identitete; — šifriranje podatkov za vpliv, vključno z izsiljevalsko programsko opremo; — ugrabitev virov; — nepooblaščeno filtriranje podatkov in manipulacija podatkov, razen kraje identitete; — uničenje podatkov; — poškodovanje; — napad na dobavno verigo; — drugo (navedite).
3.26 Druge vrste tehnik	Druge vrste tehnik Finančni subjekti, ki so v podatkovnem polju 3.25 izbrali „drugo“ vrsto tehnik, navedejo vrsto tehnike.	Ne	Da, če je v podatkovnem polju 3.25 izbrana druga vrsta tehnik.	Da, če je v podatkovnem polju 3.25 izbrana druga vrsta tehnik.	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
3.27 Informacije o prizadetih funkcionalnih področjih in poslovnih procesih	Navedba funkcionalnih področij in poslovnih procesov, na katere vpliva incident, vključno s produkti in storitvami. Funkcionalna področja med drugim vključujejo naslednje: (a) trženje in poslovni razvoj; (b) storitve za stranke; (c) upravljanje produktov; (d) skladnost s predpisi; (e) obvladovanje tveganj; (f) finance in računovodstvo; (g) splošne službe in službe za človeške vire; (h) informacijsko tehnologijo. Poslovni procesi med drugim vključujejo: — zagotavljanje informacij o računih; — aktuarske storitve; — pridobivanje plačilnih transakcij; — avtentikacijo/pooblastitev; — organ; — vstopanje organa/stranke; — upravljanje socialnih prejemkov; — upravljanje plačil socialnih prejemkov; — nakup in prodajo paketov zavarovalnih polic med zavarovalnicami; — kartična plačila; — upravljanje denarnih sredstev; — pologe ali dvige gotovine; — upravljanje zavarovalnih zahtevkov; — postopek uveljavljanja zahtevkov; — kliring; — konglomerate za podjetniška posojila; — kolektivna zavarovanja; — kreditna plačila; — skrbništvo in hrambo sredstev; — vstopanje strank; — vnos podatkov; — obdelavo podatkov; — direktne obremenitve; — izvozna zavarovanja; — dokončanje poslov/dogovorov; — izdajo finančnih instrumentov; — računovodstvo sklada;	Ne	Da	Da	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	— devizni denar; — investicijsko svetovanje; — upravljanje naložb; — izdajanje plačilnih instrumentov; — upravljanje posojil; — postopek izplačil življenjskih zavarovanj; — denarna nakazila; — izračun neto sredstev; — naročilo; — odrejanje plačil; — sklepanje zavarovanj — upravljanje portfeljev; — zbiranje premij; — sprejem/prenos/izvedbo; — pozavarovanje; — poravnavo; — spremljanje transakcij. V primeru zbirnega poročanja iz člena 7 te uredbe prizadeta funkcionalna področja in poslovni procesi pri vsaj enem finančnem subjektu.				
3.28 Prizadete infrastrukturne komponente, ki podpirajo poslovne procese	Informacije o tem, ali je večji incident, povezan z IKT, prizadel infrastrukturne komponente (strežnike, operacijske sisteme, programsko opremo, aplikacijske strežnike, vmesno programsko opremo, sestavne dele omrežja, drugo), ki podpirajo poslovne procese.	Ne	Da	Da	Izbira: — da; — ne; — informacije niso na voljo:
3.29 Informacije o prizadetih infrastrukturnih komponentah, ki podpirajo poslovne procese	Opis vpliva večjega incidenta, povezanega z IKT, na infrastrukturne komponente, ki podpirajo poslovne procese, vključno s strojno in programsko opremo. Strojna oprema vključuje strežnike, računalnike, podatkovne centre, stikala, usmerjevalnike, omrežne razdelilnike. Programska oprema vključuje operacijske sisteme, aplikacije, podatkovne zbirke, varnostna orodja, sestavne dele omrežja in drugo. Prosimo navedite. V opisih so vključene ali poimenovane prizadete infrastrukturne komponente ali sistemi in, če so na voljo: (a) informacije o različici; (b) notranja infrastruktura/delno oddano v zunanje izvajanje/v celoti oddano v zunanje izvajanje – ime tretjega ponudnika;	Ne	Da, če je incident prizadel infrastrukturne komponente, ki podpirajo poslovne procese.	Da, če je incident prizadel infrastrukturne komponente, ki podpirajo poslovne procese.	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	(c) ali infrastrukturo uporablja oziroma si jo deli več poslovnih funkcij; (d) vzpostavljene ustrezne ureditve za odpornost/neprekinjeno poslovanje/sanacijo/zamenljivost.				
3.30 Vpliv na finančne interese strank	Informacije o tem, ali je večji incident, povezan z IKT, vplival na finančne interese strank.	Ne	Da	Da	Izbira: — da; — ne; — informacije niso na voljo.
3.31 Poročanje drugim organom	Določitev, kateri organi so bili obveščeni o večjem incidentu, povezanem z IKT. Ob upoštevanju razlik, ki izhajajo iz nacionalnih zakonodaj držav članic, finančni subjekti pojem organov kazenskega pregona razumejo široko, tako da vključuje javne organe, pooblaščene za pregon kibernetske kriminalitete, vključno s policijo, organi kazenskega pregona in državnimi tožilci.	Ne	Da	Da	Izbira (več možnosti): — policijski organi/organi kazenskega pregona; — skupina CSIRT; — organ za varstvo podatkov; — nacionalna agencija za kibernetsko varnost; — nobeden; — drugo (navedite).
3.32 Določitev „drugih“ organov	Določitev „drugih“ vrst organov, ki so bili obveščeni o večjem incidentu, povezanem z IKT. Če je izbrano v podatkovnem polju 3.31. „Drugo“, opis vključuje podrobnejše informacije o organu, ki mu je finančni subjekt predložil informacije o večjem incidentu, povezanem z IKT.	Ne	Da, če je finančni subjekt o večjem incidentu, povezanem z IKT, obvestil „drugo“ vrsto organov.	Da, če je finančni subjekt o večjem incidentu, povezanem z IKT, obvestil „drugo“ vrsto organov.	Alfanumerično
3.33 Začasne dejavnosti/ ukrepi, ki so bili sprejeti ali se načrtujejo za okrevanje po incidentu	Navedba, ali je finančni subjekt izvedel (ali namerava izvesti) kakršne koli začasne ukrepe, ki so bili sprejeti (ali so načrtovani) za odpravo posledic večjega incidenta, povezanega z IKT.	Ne	Da	Da	Boolova izbira (da ali ne)

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
3.34 Opis vseh začasnih dejavnosti in ukrepov, ki so bili sprejeti ali se načrtujejo za okrevanje po incidentu	Te informacije opisujejo sprejetje takojšnjih ukrepov, vključno z izločitvijo incidenta na ravni omrežja, aktiviranimi nadomestnimi rešitvami, blokiranimi vhodi USB, aktiviranim mestom za vnovično vzpostavitev po katastrofi in vsemi drugimi začasno vzpostavljenimi dodatnimi varnostnimi kontrolami. Finančni subjekti navedejo datum in čas izvajanja začasnih ukrepov ter predvideni datum vrnitve na primarno lokacijo. Za vse začasne ukrepe, ki niso bili izvedeni, vendar so še vedno načrtovani, navedite datum, do katerega se pričakuje njihovo izvajanje. Če začasne dejavnosti/ukrepi niso bili sprejeti, navedite razlog.	Ne	Da, če so bile začasne dejavnosti/ukrepi sprejete/-i ali se načrtujejo (podatkovno polje 3.33).	Da, če so bile začasne dejavnosti/ukrepi sprejete/-i ali se načrtujejo (podatkovno polje 3.33).	Alfanumerično
3.35 Kazalniki ogroženosti	Informacije v zvezi z večjim incidentom, povezanim z IKT, ki lahko pomagajo prepoznati zlonamerno dejavnost v omrežju ali informacijskem sistemu (kazalniki ogroženosti ali IoC), kadar je to ustrezno. Polje se uporablja samo za tiste finančne subjekte, ki spadajo na področje uporabe Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta ([1]). in tiste finančne subjekte, ki so opredeljeni kot bistveni ali pomembni subjekti na podlagi nacionalnih pravil za prenos člena 3 Direktive (EU) 2022/2555, kadar je to ustrezno. IoC, ki ga zagotovi finančni subjekt, vključuje naslednje kategorije podatkov: (a) naslove IP; (b) naslove URL; (c) domene; (d) razprševanje datotek; (e) podatke o zlonamerni programski opremi (ime zlonamerne programske opreme, imena datotek in njihove lokacije, posebni registrski ključi, povezani z dejavnostjo zlonamerne programske opreme); (f) podatke o dejavnosti omrežja (vrata, protokoli, naslovi, napotitelji, uporabniški agenti, glave, posebni dnevniki ali značilni vzorci v omrežnem prometu); (g) podatke o e-poštnih sporočilih (pošiljatelj, prejemnik, zadeva, glava, vsebina);	Ne	Da, če je v podatkovnem polju 3.23 kot vrsta incidenta izbrana možnost „povezano s kibernetsko varnostjo“.	Da, če je v podatkovnem polju 3.23 kot vrsta incidenta izbrana možnost „povezano skibernetsko varnostjo“.	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	(h) zahteve DNS in konfiguracije registrov; (i) dejavnosti uporabniškega računa (prijave, dejavnosti računov privilegiranih uporabnikov, eskalacija pravic); (j) promet podatkovne zbirke (branje/pisanje), zahteve za isto datoteko. V praksi lahko ta vrsta informacij vključuje podatke, ki se med drugim nanašajo na: kazalnike, ki opisujejo vzorce omrežnega prometa, ki ustrezajo znanim napadom/komunikaciji, ki jo uporabljajo botneti, naslove IP naprav, okuženih z zlonamerno programsko opremo (boti), podatke v zvezi s strežniki za „nadzor in vodenje“, ki jih uporablja zlonamerna programska oprema (običajno domene ali naslovi IP), in URL-je v zvezi s spletnimi mesti za lažno predstavljanje ali spletnimi mesti, za katere je bilo ugotovljeno, da gostujejo zlonamerno programsko opremo ali izkoriščevalske komplete.				
Vsebina končnega poročila					
4.1 Razvrščanje temeljnih vzrokov incidenta na visoki ravni	Razvrstitev temeljnih vzrokov večjih incidentov, povezanih z IKT, na visoki ravni v okviru vrst incidentov, vključno z naslednjimi kategorijami na visoki ravni: (a) zlonamerna dejanja; (b) napaka v postopku; (c) napaka/okvara sistema; (d) človeška napaka; (e) zunanji dogodek.	Ne	Ne	Da	Izbira (več možnosti): — zlonamerna dejanja; — napaka v postopku; — napaka/okvara sistema; — človeška napaka; — zunanji dogodek.
4.2 Podrobna razvrstitev temeljnih vzrokov incidenta	Podrobna razvrstitev temeljnih vzrokov večjega incidenta, povezanega z IKT, v okviru vrst incidentov, vključno z naslednjimi podrobnimi kategorijami, povezanimi s kategorijami na visoki ravni, ki se poročajo v podatkovnem polju 4.1: 1. **Zlonamerna dejanja** (če je izbrana ta možnost, izberite eno ali več od naslednjih možnosti): (a) namerni notranji ukrepi; (b) namerna fizična poškodba/manipulacija/kraja; (c) goljufive dejavnosti. 2. **Napaka v postopku** (če je izbrana ta možnost, izberite eno ali več od naslednjih možnosti): (a) nezadostno spremljanje ali opustitev dolžnosti spremljanja in nadzora;	Ne	Ne	Da	Izbira (več možnosti): — zlonamerna dejanja: namerni notranji ukrepi; — zlonamerna dejanja: namerna fizična poškodba/manipulacija/kraja; — zlonamerna dejanja: goljufive dejavnosti; — napaka v postopku: nezadostno spremljanje ali opustitev dolžnosti spremljanja in nadzora; — napaka v postopku: **n**ezadovoljive/nejasne vloge in odgovornosti; — napaka v postopku: napaka v postopku pri obvladovanju tveganj na področju IKT; — napaka v postopku: nezadostne operacije IKT in operacije za varnost IKT ali neuspešno delovanje le teh;

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	(b) nezadovoljive/nejasne vloge in odgovornosti; (c) napaka v postopku pri obvladovanju tveganj na področju IKT; (d) nezadostne operacije IKT in operacije za varnost IKT ali neuspešno delovanje le teh; (e) nezadostno ali neuspešno upravljanje projektov IKT; (f) neustrezne notranje politike, postopki in dokumentacija; (g) neustrezna pridobitev, razvoj ali vzdrževanje sistemov IKT; (h) drugo (navedite). 3. **Napaka/okvara sistema** (če je izbrana ta možnost, izberite eno ali več od naslednjih možnosti): (a) zmogljivost in učinkovitost strojne opreme: večji incidenti, povezani z IKT, ki jih povzročijo viri strojne opreme, ki se izkažejo za nezadostne v smislu zmogljivosti ali učinkovitosti za izpolnjevanje veljavnih zakonodajnih zahtev; (b) vzdrževanje strojne opreme: večji incidenti, povezani z IKT, ki so posledica neustreznega ali nezadostnega vzdrževanja komponent strojne opreme, razen „zastarelost/staranje strojne opreme“; (c) zastarelost/staranje strojne opreme: ta vrsta temeljnega vzroka vključuje večje incidente, povezane z IKT, ki so posledica zastarelih ali starajočih se komponent strojne opreme; (d) združljivost/konfiguracija programske opreme: večji incidenti, povezani z IKT, ki jih povzročijo sestavni deli programske opreme, ki niso združljivi z drugo programsko opremo ali konfiguracijami sistema, vključno z večjimi incidenti, povezanimi z IKT, ki so posledica medsebojnega oviranja programske opreme, nepravilnih nastavitev ali napačno konfiguriranih parametrov, ki vplivajo na splošno funkcionalnost sistema; (e) učinkovitost programske opreme: večji incidenti, povezani z IKT, ki so posledica sestavnih delov programske opreme, ki ni učinkovita ali je neučinkovita zaradi razlogov, ki niso navedeni v razdelku „združljivost/konfiguracija programske opreme“, vključno z večjimi incidenti, povezanimi z IKT, ki so posledica počasnih odzivnih časov, prekomerne porabe virov ali neučinkovitega izvajanja poizvedb, ki vpliva na delovanje programske opreme ali sistema;				— napaka v postopku: nezadostno ali neuspešno upravljanje projektov IKT; — napaka v postopku: neustreznost notranje politike, postopkov in dokumentacije; — napaka v postopku: neustrezna pridobitev, razvoj in vzdrževanje sistemov IKT; — napaka v postopku: drugo (navedite); — napaka v sistemu: zmogljivost in učinkovitost strojne opreme; — napaka v sistemu: vzdrževanje strojne opreme; — napaka v sistemu: zastarelost/staranje strojne opreme; — napaka v sistemu: združljivost/konfiguracija programske opreme; — napaka v sistemu: učinkovitost programske opreme; — napaka v sistemu: konfiguracija omrežja; — napaka v sistemu: fizična škoda; — napaka v sistemu: drugo (navedite); — človeška napaka: opustitev; — človeška napaka: napaka; — človeška napaka: spretnosti in znanja; — človeška napaka: nezadostni človeški viri; — človeška napaka neustrezna komunikacija; — človeška napaka: drugo (navedite); — zunanji dogodek: naravne nesreče/višja sila; — zunanji dogodek: napake tretje osebe; — zunanji dogodek: drugo (navedite).

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	(f) konfiguracija omrežja: večji incidenti, povezani z IKT, ki so posledica nepravilnih ali napačno konfiguriranih omrežnih nastavitev ali infrastrukture, vključno z večjimi incidenti, povezanimi z IKT, ki so jih povzročile napake v konfiguraciji omrežja, težave z usmerjanjem, napačne konfiguracije požarnega zidu ali druge težave, povezane z omrežjem, ki vplivajo na povezljivost ali komunikacijo; (g) fizična škoda: večji incidenti, povezani z IKT, ki jih povzroči fizična škoda na infrastrukturi IKT, kar vodi do okvar sistema; (h) drugo (navedite). 4. **Človeška napaka** (če je izbrana ta možnost, izberite eno ali več od naslednjih možnosti): (a) opustitev (nenamerna); (b) napaka; (c) spretnosti in znanja: večji incidenti, povezani z IKT, ki so posledica pomanjkanja strokovnega znanja ali usposobljenosti za upravljanje sistemov ali postopkov IKT, kar je lahko posledica neustreznega usposabljanja, nezadostnega znanja ali vrzeli v spretnostih, potrebnih za opravljanje posebnih nalog ali reševanje tehničnih izzivov; (d) nezadostni človeški viri: večji incidenti, povezani z IKT, ki jih povzroči pomanjkanje potrebnih virov, vključno s strojno opremo, programsko opremo, infrastrukturo ali osebjem, in vključno s situacijami, v katerih nezadostna sredstva povzročijo neučinkovitosti pri delovanju, sistemske napake ali nezmožnost izpolnjevanja poslovnih zahtev; (e) neustrezna komunikacija; (f) drugo (navedite). 5. **Zunanji dogodek** (če je izbrana ta možnost, izberite eno ali več od naslednjih možnosti): (a) naravne nesreče/višja sila; (b) napake tretje osebe;				

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	(c) drugo (navedite). Finančni subjekti upoštevajo, da se za ponavljajoče se večje incidente, povezane z IKT, upošteva specifični očitni temeljni vzrok incidenta in ne širše kategorije, vključene v to področje.				
4.3 Dodatna razvrstitev temeljnih vzrokov incidenta	Dodatna razvrstitev temeljnih vzrokov večjega incidenta, povezanega z IKT, v okviru vrst incidentov, vključno z naslednjimi dodatnimi razvrstitvenimi kategorijami, povezanimi s podrobnimi kategorijami, ki se poročajo v podatkovnem polju 4.2. Polje je obvezno za končno poročilo, če se v podatkovnem polju 4.2 poročajo posebne kategorije, ki zahtevajo dodatno razčlenjenost. 2(a) **Nezadostno spremljanje in nadzor ali opustitev le-tega:** (a) spremljanje zavezanosti politiki; (b) spremljanje tretjih ponudnikov storitev; (c) spremljanje in preverjanje sanacije ranljivosti; (d) upravljanje identitete in dostopa; (e) šifriranje in kriptografija; (f) beleženje v dnevnike. 2(c) **Napaka v postopku pri obvladovanju tveganj na področju IKT:** (a) napaka pri določanju točnih tolerančnih ravni tveganja; (b) nezadostne ocene ranljivosti in ogroženosti; (c) neustrezni ukrepi za obravnavo tveganja; (d) slabo obvladovanje preostalih tveganj na področju IKT. 2(d) **Nezadostne operacije IKT in operacije za varnost IKT ali neuspešno delovanje le teh:** (a) upravljanje ranljivosti in popravkov; (b) upravljanje sprememb; (c) upravljanje zmogljivosti in učinkovitosti delovanja; (d) upravljanje sredstev IKT in razvrščanje informacij;	Ne	Ne	Da	Izbira (več možnosti): — spremljanje zavezanosti politiki; — spremljanje tretjih ponudnikov storitev; — spremljanje in preverjanje sanacije ranljivosti; — upravljanje identitete in dostopa; — šifriranje in kriptografija; — beleženje v dnevnike; — napaka pri določanju točnih tolerančnih ravni tveganja; — nezadostne ocene ranljivosti in ogroženosti; — neustrezni ukrepi za obravnavo tveganja; — slabo obvladovanje preostalih tveganj na področju IKT; — upravljanje ranljivosti in popravkov; — upravljanje sprememb; — upravljanje zmogljivosti in učinkovitosti delovanja; — upravljanje sredstev IKT in razvrščanje informacij; — varnostno kopiranje in obnovitev; — obravnavanje napak; — neustrezna pridobitev, razvoj in vzdrževanje sistemov IKT; — nezadostno ali neuspešno preskušanje programske opreme.

Podatkovno polje		Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
		(e) varnostno kopiranje in obnovitev; (f) obravnavanje napak. 2(g) **Neustrezna pridobitev, razvoj in vzdrževanje sistemov IKT:** (a) neustrezna pridobitev, razvoj in vzdrževanje sistemov IKT; (b) nezadostno ali neuspešno preskušanje programske opreme.				
4.4	Druge vrste temeljnih vzrokov	Finančni subjekti, ki so v podatkovnem polju 4.2 izbrali „drugo“ vrsto temeljnega vzroka, navedejo druge vrste temeljnih vzrokov	Ne	Ne	Da, če je v podatkovnem polju 4.2 izbrana „druga“ vrsta temeljnih vzrokov.	Alfanumerično
4.5	Informacije o temeljnih vzrokih incidenta	Opis zaporedja dogodkov, ki so privedli do večjega incidenta, povezanega z IKT, in opis, kako ima večji incident, povezan z IKT, podoben očiten temeljni vzrok, če je ta incident razvrščen kot ponavljajoči se incident, vključno s kratkim opisom vseh temeljnih razlogov in temeljnih dejavnikov, ki so prispevali k nastanku večjega incidenta, povezanega z IKT. V primeru zlonamernih dejanj opis načina delovanja zlonamernega dejanja, vključno z uporabljenimi taktikami, tehnikami in postopki ter vhodnim vektorjem večjega incidenta, povezanega z IKT, po potrebi vključno z opisom preiskav in analiz, na podlagi katerih so bili ugotovljeni temeljni vzroki.	Ne	Ne	Da	Alfanumerično
4.6	Reševanje incidentov	Dodatne informacije o sprejetih/načrtovanih dejavnostih/ukrepih za trajno rešitev večjega incidenta, povezanega z IKT, in za preprečitev, da bi se ta incident ponovil. Izkušnje, pridobljene pri večjem incidentu, povezanem z IKT.	Ne	Ne	Da	Alfanumerično

Podatkovno polje		Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
		Opis vključuje naslednje točke: 1. **Opis ukrepov za reševanje** (a) ukrepi, sprejete za trajno rešitev večjega incidenta, povezanega z IKT (razen začasnih ukrepov); (b) za vsak sprejeti ukrep navedite morebitno udeležbo tretjega ponudnika in finančnega subjekta; (c) navedite, ali so bili postopki po večjem incidentu, povezanem z IKT, prilagojeni; (d) navedite morebitne dodatne kontrole, ki so bile vzpostavljene ali se načrtujejo, s povezanim časovnim razporedom izvajanja. Morebitne ugotovljene težave v zvezi z zanesljivostjo prizadetih informacijskih sistemov/ali v zvezi z vzpostavljenimi postopki ali kontrolami, če je to ustrezno. Finančni subjekti jasno navedejo, kako bodo predvideni popravni ukrepi obravnavali ugotovljene temeljne vzroke in kdaj naj bi bil večji incident, povezan z IKT, trajno rešen. 2. **Pridobljene izkušnje** Finančni subjekti opišejo ugotovitve pregleda po incidentu.				
4.7	Datum in čas, ko je bil obravnavan temeljni vzrok incidenta	Datum in čas, ko je bil obravnavan temeljni vzrok incidenta.	Ne	Ne	Da	Čas UTC v obliki zapisa po standardu 8601 (LLLL-MM-DD Thh. mm.ss)
4.8	Datum in čas, ko je bil incident rešen	Datum in čas, ko je bil incident rešen.	Ne	Ne	Da	Čas UTC v obliki zapisa po standardu 8601 (LLLL-MM-DD Thh. mm.ss)

Podatkovno polje		Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
4.9	Informacije o tem, ali se datum trajne rešitve incidentov razlikuje od prvotno načrtovanega datuma začetka izvajanja	Opisi razlogov, zakaj se datum trajne rešitve večjih incidentov, povezanih z IKT, razlikuje od prvotno načrtovanega datuma začetka izvajanja, kjer je to primerno.	Ne	Ne	Da	Alfanumerično
4.10	Ocena tveganja za kritične funkcije za namene reševanja	Ocena, ali večji incident, povezan z IKT, predstavlja tveganje za kritične funkcije v smislu člena 2(1), točka 35, Direktive 2014/59/EU Evropskega parlamenta in Sveta ([2]). Subjekti iz člena 1(1) Direktive 2014/59/EU navedejo, ali incident predstavlja tveganje za kritične funkcije v smislu člena 2(1), točka 35, Direktive 2014/59/EU, kot se poročajo v predlogi Z07.01 Izvedbene uredbe Komisije (EU) 2018/1624 ([3]) in se razporedijo določenemu subjektu v predlogi Z07.02.	Ne	Ne	Da, če incident predstavlja tveganje za kritične funkcije finančnih subjektov v skladu s členom 2(1), točka 35, Direktive 2014/59/E-U.	Alfanumerično
4.11	Informacije, relevantne za organe za reševanje	Opis, ali in kako je večji incident, povezan z IKT, vplival na rešljivost subjekta ali skupine. Subjekti iz člena 1(1) Direktive 2014/59/EU zagotovijo informacije o tem, ali in kako je večji incident, povezan z IKT, vplival na rešljivost subjekta ali skupine. Ti subjekti navedejo tudi, ali večji incident, povezan z IKT, vpliva na solventnost ali likvidnost finančnega subjekta in morebitno količinsko opredelitev učinka. Ti subjekti zagotovijo tudi informacije o učinku na neprekinjeno poslovanje, učinku na rešljivost subjekta, morebitnem dodatnem učinku na stroške in izgube zaradi večjega incidenta, povezanega z IKT, vključno s kapitalskim položajem finančnega subjekta, ter o tem, ali so pogodbeni dogovori o uporabi storitev IKT v primeru reševanja subjekta še vedno zanesljivi in v celoti izvršljivi.	Ne	Ne	Da, če je incident vplival na rešljivost subjekta ali skupine.	Alfanumerično

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
4.12 Prag pomembnosti za merilo za razvrščanje „gospodarski učinek“	Podrobne informacije o pragovih, ki jih je na koncu dosegel večji incident, povezan z IKT, v zvezi z merilom „gospodarski učinek“ iz členov 7 in 14 Delegirane uredbe (EU) 2024/1772.	Ne	Ne	Da	Alfanumerično
4.13 Znesek bruto neposrednih in posrednih stroškov in izgub	Skupni znesek bruto neposrednih in posrednih stroškov ter izgub, ki jih ima finančni subjekt zaradi večjega incidenta, povezanega z IKT, vključno z: (a) zneskom razlaščenih ali finančnih sredstev, za katera je odgovoren finančni subjekt; (b) zneskom stroškov zamenjave ali premestitve programske opreme, strojne opreme ali infrastrukture; (c) zneskom stroškov za osebje, vključno s stroški, povezanimi z nadomeščanjem ali premestitvijo osebja, zaposlovanjem dodatnih zaposlenih, plačilom nadur in ponovno pridobitvijo izgubljenih ali oslabljenih spretnosti osebja; (d) zneskom nadomestil zaradi neizpolnjevanja pogodbenih obveznosti; (e) zneskom stroškov pravnih sredstev in nadomestil za stranke; (f) zneskom izgub zaradi izpada prihodkov; (g) zneskom stroškov, povezanih z notranjo in zunanjo komunikacijo; (h) zneskom stroškov svetovanja, vključno s stroški, povezanimi s pravnim svetovanjem, forenzičnimi storitvami in storitvami ponovne vzpostavitve; (i) zneskom drugih stroškov in izgub, vključno z naslednjim: (i) neposrednimi stroški, vključno z oslabitvami in stroški poravnave, v breme izkaza poslovnega izida ter odpisi zaradi večjega incidenta, povezanega z IKT; (ii) rezervacijami ali rezervami, obračunanimi v izkazu poslovnega izida, za verjetne izgube, povezane z večjim incidentom, povezanim z IKT;	Ne	Ne	Da	Monetarno

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	(iii) pričakovanimi izgubami v obliki izgub zaradi večjega incidenta, povezanega z IKT, ki so začasno knjižene v prehodnih ali začasnih kontih in še niso izražene v izkazu poslovnega izida ter za katere se načrtuje, da bodo vključene v obdobju, sorazmernem z obsegom in starostjo pričakovane izgube; (iv) dejanskimi nepobrani prihodki, povezanimi s pogodbenimi obveznostmi do tretjih oseb, vključno z odločitvijo o povrnitvi škode stranki po večjem incidentu, povezanem z IKT, z opustitvijo prilagoditve prihodkov ali znižanjem pogodbenih pristojbin za določeno prihodnje obdobje namesto s povračilom ali neposrednim plačilom; (v) časovno naravnanimi izgubami, če se nanašajo na več kot eno fiskalno leto in povzročajo pravno tveganje. Finančni subjekti pri svoji oceni upoštevajo člen 7(1) in (2) Delegirane uredbe (EU) 2024/1772. Finančni subjekti v to številko ne vključijo nobenih vrst finančnih izterjav. Finančni subjekti poročajo o denarnem znesku kot pozitivni vrednosti. V primeru zbirnega poročanja iz člena 7 te uredbe finančni subjekti upoštevajo skupni znesek stroškov in izgub za vse finančne subjekte. Finančni subjekti poročajo o podatkovni točki v enotah z najmanjšim ekvivalentom natančnosti na tisoč enot.				
4.14 Znesek finančnih izterjav	Skupni znesek finančnih izterjav. Finančne izterjave se nanašajo na prvotno izgubo, ki jo je povzročil incident, ne glede na to, kdaj so finančne izterjave v obliki sredstev ali prilivov gospodarskih koristi prejete.	Ne	Ne	Da	Monetarno Finančni subjekti poročajo o podatkovni točki v enotah z najmanjšim ekvivalentom natančnosti na tisoč enot

Podatkovno polje	Opis:	Obvezno za začetno uradno obvestilo	Obvezno za vmesno poročilo	Obvezno za končno poročilo	Vrsta polja
	Finančni subjekti poročajo o denarnem znesku kot pozitivni vrednosti. V primeru zbirnega poročanja iz člena 7 te uredbe finančni subjekti upoštevajo skupni znesek finančnih izterjav za vse finančne subjekte.				
4.15 Informacije o tem, ali so se manjši incidenti ponavljali	Informacije o tem, ali se je ponovil več kot en manjši incident, povezan z IKT, in ali se skupaj štejejo za večji incident v smislu člena 8(2) Delegirane uredbe (EU) 2024/1772. Finančni subjekti navedejo, ali so se manjši incidenti, povezani z IKT, ponavljali in se skupaj štejejo za en večji incident, povezan z IKT. Finančni subjekti navedejo tudi število pojavov teh manjših incidentov, povezanih z IKT.	Ne	Ne	Da, če večji incident obsega več kot en manjši ponavljajoči se incident.	Alfanumerično
4.16 Datum in čas pojave ponavljajočih se incidentov	Kadar finančni subjekti poročajo o ponavljajočih se incidentih, povezanih z IKT, datum in čas, ko se je zgodil prvi incident, povezan z IKT.	Ne	Ne	Da, za ponavljajoče se incidente.	Čas UTC v obliki zapisa po standardu 8601 (LLLL-MM-DD Thh. mm.ss)

([1]) 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).

([2]) Direktiva 2014/59/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o vzpostavitvi okvira za sanacijo ter reševanje kreditnih institucij in investicijskih podjetij ter o spremembi Šeste direktive Sveta 82/891/EGS ter direktiv 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EU, 2012/30/EU in 2013/36/EU in uredb (EU) št. 1093/2010 ter (EU) št. 648/2012 Evropskega parlamenta in Sveta (UL L 173, 12.6.2014, str. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Izvedbena uredba Komisije (EU) 2018/1624 z dne 23. oktobra 2018 o določitvi izvedbenih tehničnih standardov v zvezi s postopki, standardnimi obrazci in predlogami za zagotavljanje informacij za potrebe načrtov reševanja za kreditne institucije in investicijska podjetja v skladu z Direktivo 2014/59/EU Evropskega parlamenta in Sveta ter o razveljavitvi Izvedbene uredbe Komisije (EU) 2016/1066 (UL L 277, 7.11.2018, str. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

PRILOGA III

PREDLOGE ZA OBVEŠČANJE O POMEMBNIH KIBERNETSKIH GROŽNJAH

Število polja	Podatkovno polje	
1	Ime subjekta, ki predloži uradno obvestilo	
2	Identifikacijska koda subjekta, ki predloži uradno obvestilo	
3	Vrsta finančnega subjekta, ki predloži uradno obvestilo	
4	Ime finančnega subjekta	
5	Koda LEI finančnega subjekta	
6	Ime glavne kontaktne osebe	
7	Elektronski naslov glavne kontaktne osebe	
8	Telefonska številka glavne kontaktne osebe	
9	Ime nadomestne kontaktne osebe	
10	Elektronski naslov nadomestne kontaktne osebe	
11	Telefonska številka nadomestne kontaktne osebe	
12	Datum in čas odkritja kibernetske grožnje	
13	Opis pomembne kibernetske grožnje	
14	Informacije o možnem učinku	
15	Merila za razvrščanje morebitnih incidentov	
16	Stanje kibernetske grožnje	
17	Ukrepi, sprejeti za preprečitev uresničitve	
18	Uradno obvestilo drugim deležnikom	
19	Kazalniki ogroženosti	
20	Druge relevantne informacije	

PRILOGA IV

PODATKOVNI GLOSAR IN NAVODILA ZA OBVEŠČANJE O POMEMBNIH KIBERNETSKIH GROŽNJAH

Podatkovno polje	Opis:	Obvezno polje	Vrsta polja
1. Ime subjekta, ki predloži uradno obvestilo	Polno pravno ime subjekta, ki predloži uradno obvestilo.	Da	Alfanumerično
2. Identifikacijska koda subjekta, ki predloži uradno obvestilo	Identifikacijska koda subjekta, ki predloži uradno obvestilo. Kadar finančni subjekti predložijo uradno obvestilo/poročilo, je identifikacijska koda identifikator pravnih subjektov (LEI), ki je edinstvena 20-mestna alfanumerična koda na podlagi standarda ISO 17442-1:2020. Kadar tretji ponudnik predloži poročilo za finančni subjekt, lahko uporabi identifikacijsko kodo, kot je določena v izvedbenih tehničnih standardih, sprejetih v skladu s členom 28(9) Uredbe (EU) 2022/2554.	Da	Alfanumerično
3. Vrsta finančnega subjekta, ki predloži poročilo	Vrsta subjekta iz člena 2(1), točke (a) do (t), Uredbe (EU) 2022/2554, ki predloži poročilo.	Da, če poročila ne predloži neposredno prizadeti finančni subjekt.	Izbira (več možnosti): — kreditna institucija; — plačilna institucija; — izvzeta plačilna institucija; — ponudnik storitev zagotavljanja informacij o računih; — institucija za izdajo elektronskega denarja; — izvzeta institucija za izdajo elektronskega denarja; — investicijsko podjetje; — ponudnik storitev v zvezi s kriptosredstvi; — izdajatelj žetonov, vezanih na sredstva; — centralna depotna družba; — centralna nasprotna stranka; — mesto trgovanja; — repozitorij sklenjenih poslov; — upravitelj alternativnega investicijskega sklada; — družba za upravljanje; — izvajalec storitev sporočanja podatkov;

Podatkovno polje	Opis:	Obvezno polje	Vrsta polja
			— zavarovalnica in pozavarovalnica; — zavarovalni posrednik, pozavarovalni posrednik in posrednik dopolnilnih zavarovanj; — institucija za poklicno pokojninsko zavarovanje; — bonitetna agencija; — upravljavec ključnih referenčnih vrednosti; — ponudnik storitev množičnega financiranja; — repozitorij listinjenja.
4. Ime finančnega subjekta	Polno pravno ime finančnega subjekta, ki priglaša pomembno kibernetsko grožnjo.	Da, če se finančni subjekt razlikuje od subjekta, ki je predložil uradno obvestilo.	Alfanumerično
5. Koda LEI finančnega subjekta	Identifikator pravnih subjektov (LEI) finančnega subjekta, ki priglaša pomembno kibernetsko grožnjo, ki je dodeljen v skladu z Mednarodno organizacijo za standardizacijo.	Da, če se finančni subjekt, ki je priglasil pomembno kibernetsko grožnjo, razlikuje od subjekta, ki je predložil poročilo.	Edinstvena 20-mestna alfanumerična koda na podlagi standarda ISO 17442-1:2020
6. Ime glavne kontaktne osebe	Ime in priimek glavne kontaktne osebe finančnega subjekta.	Da	Alfanumerično
7. Elektronski naslov glavne kontaktne osebe	Elektronski naslov glavne kontaktne osebe, ki ga lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih.	Da	Alfanumerično
8. Telefonska številka glavne kontaktne osebe	Telefonska številka glavne kontaktne osebe, ki jo lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih. Telefonska številka se sporoči z vsemi mednarodnimi klicnimi številkami (npr. +33XXXXXXXXX).	Da	Alfanumerično
9. Ime nadomestne kontaktne osebe	Ime in priimek nadomestne kontaktne osebe finančnega subjekta ali subjekta, ki predloži uradno obvestilo v imenu finančnega subjekta, če je na voljo.	Da, če sta na voljo ime in priimek nadomestne kontaktne osebe finančnega subjekta ali subjekta, ki predloži uradno obvestilo za finančni subjekt.	Alfanumerično

Podatkovno polje	Opis:	Obvezno polje	Vrsta polja
10. Elektronski naslov nadomestne kontaktne osebe	Elektronski naslov nadomestne kontaktne osebe ali namenski elektronski naslov skupine, ki ga lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih, če je na voljo.	Da, če je na voljo elektronski naslov nadomestne kontaktne osebe ali namenski elektronski naslov skupine, ki ga lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih.	Alfanumerično
11. Telefonska številka nadomestne kontaktne osebe	Telefonska številka nadomestne kontaktne osebe, ki jo lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih, če je na voljo. Telefonska številka se sporoči z vsemi mednarodnimi klicnimi številkami (npr. +33XXXXXXXXX).	Da, če je na voljo telefonska številka nadomestne kontaktne osebe, ki jo lahko pristojni organ uporabi za sporočila o nadaljnjih ukrepih.	Alfanumerično
12. Datum in čas odkritja kibernetske grožnje	Datum in čas, ko je finančni subjekt izvedel za pomembno kibernetsko grožnjo.	Da	Čas UTC v obliki zapisa po standardu 8601 (LLLL-MM-DD Thh. mm.ss)
13. Opis pomembne kibernetske grožnje	Opis najpomembnejših vidikov pomembne kibernetske grožnje. Finančni subjekti zagotovijo: (a) pregled najpomembnejših vidikov pomembne kibernetske grožnje na visoki ravni; (b) s tem povezana tveganja, ki izhajajo iz tega, vključno z morebitnimi ranljivostmi sistemov finančnega subjekta, ki jih je mogoče izkoristiti; (c) informacije o verjetnosti uresničitve pomembne kibernetske grožnje; in (d) informacije o viru informacij o kibernetski grožnji.	Da	Alfanumerično
14. Informacije o možnem učinku	Informacije o možnem učinku kibernetske grožnje na finančni subjekt, njegove stranke ali finančne partnerje, če se je kibernetska grožnja uresničila	Da	Alfanumerično
15. Merila za razvrščanje morebitnih incidentov	Merila za razvrščanje, ki bi lahko sprožila poročilo o večjem incidentu, če bi se kibernetska grožnja uresničila.	Da	Izbira (več možnosti): — prizadete stranke, finančni partnerji in transakcije; — vpliv na ugled; — trajanje in nedelovanje storitve; — geografska razpršenost; — izgube podatkov; — prizadete kritične storitve; — gospodarski učinek.

Podatkovno polje		Opis:	Obvezno polje	Vrsta polja
16.	Stanje kibernetske grožnje	Informacije o stanju kibernetske grožnje za finančni subjekt in o tem, ali je prišlo do kakršnih koli sprememb pri grožnji. Kadar je kibernetska grožnja prenehala komunicirati z informacijskimi sistemi finančnega subjekta, se lahko stanje označi kot neaktivno. Če ima finančni subjekt informacije, da je grožnja še vedno aktivna proti drugim strankam ali finančnemu sistemu kot celoti, se stanje označi kot aktivno.	Da	Izbira: — aktivno; — neaktivno.
17.	Ukrepi, sprejeti za preprečitev uresničitve	Informacije o ukrepih na visoki ravni, ki jih je finančni subjekt sprejel za preprečitev uresničitve pomembnih kibernetskih groženj, če je to ustrezno.	Da	Alfanumerično
18.	Uradno obvestilo drugim deležnikom	Informacije o obveščanju drugih finančnih subjektov ali organov o kibernetski grožnji.	Da, če so bili drugi finančni subjekti ali organi seznanjeni s kibernetsko grožnjo.	Alfanumerično
19.	Kazalniki ogroženosti	Informacije v zvezi s pomembno grožnjo, ki lahko pomagajo prepoznati zlonamerno dejavnost v omrežju ali informacijskem sistemu (kazalniki ogroženosti ali IoC), kadar je to ustrezno. IoC, ki ga zagotovi finančni subjekt, lahko med drugim vključuje naslednje kategorije podatkov: (a) naslove IP; (b) naslove URL; (c) domene; (d) razprševanje datotek; (e) podatke o zlonamerni programski opremi (ime zlonamerne programske opreme, imena datotek in njihove lokacije, posebni registrski ključi, povezani z dejavnostjo zlonamerne programske opreme); (f) podatke o dejavnosti omrežja (vrata, protokoli, naslovi, napotitelji, uporabniški agenti, glave, posebni dnevniki ali značilni vzorci v omrežnem prometu); (g) podatke o e-poštnih sporočilih (pošiljatelj, prejemnik, zadeva, glava, vsebina); (h) zahteve DNS in konfiguracije registrov; (i) dejavnosti uporabniškega računa (prijave, dejavnosti računov privilegiranih uporabnikov, eskalacija pravic); (j) promet podatkovne zbirke (branje/pisanje), zahteve za isto datoteko. Ta vrsta informacij lahko vključuje podatke, ki se nanašajo na: kazalnike, ki opisujejo vzorce omrežnega prometa, ki ustrezajo znanim napadom/komunikacijam, ki jo uporabljajo botneti, naslove IP naprav, okuženih z zlonamerno programsko opremo (boti), podatke v zvezi s strežniki za „nadzor in vodenje“, ki jih uporablja zlonamerna programska oprema (običajno domene ali naslovi IP), in URL-je v zvezi s spletnimi mesti za lažno predstavljanje ali spletnimi mesti, za katera je bilo ugotovljeno, da gostujejo zlonamerno programsko opremo ali izkoriščevalske komplete.	Da, če so na voljo informacije o kazalnikih ogroženosti, povezanih s kibernetsko grožnjo.	Alfanumerično
20.	Druge relevantne informacije	Vse druge relevantne informacije o pomembni kibernetski grožnji	Da, če je ustrezno in če so na voljo druge informacije, ki niso zajete v predlogi.	Alfanumerično

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj