Euroopa Liidu
Teataja

ET
L-seeria

2025/301

20.2.2025

KOMISJONI DELEGEERITUD MÄÄRUS (EL) 2025/301,

23. oktoober 2024,

millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 regulatiivsete tehniliste standarditega, millega määratakse kindlaks tõsiste IKT intsidentide kohta esitatava esialgse teate, vaheraporti ja lõppraporti sisu ja tähtajad ning vabatahtliku olulistest küberohtudest teatamise sisu

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrust (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011, ([1]) eriti selle artikli 20 kolmandat lõiku,

ning arvestades järgmist:

(1) Selleks, et ühtlustada ja lihtsustada määruse (EL) 2022/2554 artikli 19 lõikes 4 osutatud tõsiste IKT intsidentide kohta teadete ja raportite esitamise nõudeid, tuleks tõsistest IKT intsidentidest teavitamise tähtaegade puhul järgida kõigi finantssektori ettevõtjate puhul järjepidevat lähenemisviisi. Seetõttu tuleks ka tähtaegade puhul järgida võimalikult suurel määral lähenemisviisi, mis on järjepidev ja oma mõjult vähemalt võrdväärne nõuetega, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2555 ([2]).

(2) Selleks, et mitte tekitada finantssektori ettevõtjatele IKT intsidendi lahendamise ajal põhjendamatut aruandluskoormust, peaks esialgse teate sisu piirduma kõige olulisema teabega. Pädevad asutused peavad nõuetekohaste järelevalvemeetmete võtmiseks saama teabe tõsiste IKT intsidentide kohta võimalikult kiiresti pärast seda, kui finantssektori ettevõtja on IKT intsidendi tõsiseks intsidendiks liigitanud. Seetõttu peaks määruse (EL) 2022/2554 artikli 19 lõike 4 punktis a osutatud esialgse teate esitamise tähtaeg olema võimalikult lühike ja algama esimesel võimalusel pärast IKT intsidendi liigitamist tõsiseks intsidendiks, võimaldades siiski paindlikkust, eelkõige selliste teenuse osutamise ärimudelite puhul, mille puhul aeg ei ole eriti kriitilise tähtsusega, kui finantssektori ettevõtjad vajavad IKT intsidendi lahendamiseks pärast sellest teada saamist rohkem aega.

(3) Pärast esialgse teate saamist peaksid pädevad asutused saama IKT intsidendi kohta üksikasjalikumat teavet vaheraportis ja kogu asjakohase teabe lõppraportis. Neis raportites esitatav teave peaks võimaldama pädevatel asutustel IKT intsidenti põhjalikumalt analüüsida ja kaaluda, milliseid järelevalvemeetmeid nad soovivad võtta.

(4) Määruse (EL) 2022/2554 artikli 20 esimese lõigu punkti a alapunktis ii osutatud teavitamise tähtaegade puhul tuleks seega leida tasakaal pädevate asutuste kiiresti teabe saamise vajaduse ning finantssektori ettevõtjatele tervikliku ja täpse teabe saamiseks piisava aja andmise vajaduse vahel.

(5) Määruse (EL) 2022/2554 artikli 20 esimese lõigu punktis a sätestatud kriteeriume arvesse võttes ei tohiks teavitamise tähtajad põhjustada mikroettevõtjatele ja muudele väikestele finantssektori ettevõtjatele ebaproportsionaalselt suurt koormust. Et mitte tekitada finantssektori ettevõtjatele ebaproportsionaalset koormust, tuleks teavitamise tähtaegade puhul võtta arvesse nädalavahetusi ja riigipühasid.

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

([2]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Kuna olulistest küberohtudest saab teatada vabatahtlikult, ei tohiks kõnealuste teadete sisu põhjustada koormust finantssektori ettevõtjatele ja see peaks olema piiratum kui tõsiste IKT intsidentide kohta nõutav teave.

(7) Käesolev määrus põhineb Euroopa järelevalveasutuste poolt komisjonile esitatud regulatiivsete tehniliste standardite eelnõul.

(8) Euroopa järelevalveasutused on korraldanud avalikud konsultatsioonid käesoleva määruse aluseks oleva regulatiivsete tehniliste standardite eelnõu kohta, analüüsinud võimalikku asjaomast kulu ja kasu ning küsinud nõu Euroopa Parlamendi ja nõukogu määruste (EL) nr 1093/2010, ([3]) (EL) nr 1094/2010 ([4]) ja (EL) nr 1095/2010 ([5]) artikli 37 kohaselt loodud sidusrühmade kogult.

(9) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([6]) artikli 42 lõikele 1 konsulteeriti Euroopa Andmekaitseinspektoriga, kes esitas oma positiivse arvamuse 22. juulil 2024. Mis tahes isikuandmete töötlemine käesoleva määruse raames peaks toimuma kooskõlas määruse (EL) 2018/1725 alusel kohaldatavate andmekaitsealaste põhimõtete ja sätetega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Üldine teave, mis tuleb esitada tõsiseid IKT intsidente käsitlevates esialgsetes teadetes, vaheraportites ja lõppraportites

Finantssektori ettevõtjad peavad lisama määruse (EL) 2022/2554 artikli 19 lõikes 4 osutatud esialgsesse teatesse, vaheraportisse ja lõppraportisse järgmise üldise teabe:

a) esitatud teate liik (esialgne teade, vaheraport või lõppraport);

b) finantssektori ettevõtja nimi, selle juriidilise isiku tunnus ja finantssektori ettevõtja liik, nagu on osutatud määruse (EL) 2022/2554 artikli 2 lõikes 1;

c) finantssektori ettevõtja nimel esialgset teadet, vaheraportit või lõppraportit esitava üksuse nimi ja tunnuskood;

d) kui see on kohaldatav, siis kõigi koondatud esialgse teate, vaheraporti või lõppraportiga hõlmatud finantssektori ettevõtjate nimed ja juriidilise isiku tunnused;

e) nende isikute kontaktandmed, kes vastutavad pädeva asutusega tõsise IKT intsidendi asjus suhtlemise eest;

f) kui see on kohaldatav, siis finantssektori ettevõtja grupi emaettevõtja identifitseerimisandmed;

g) rahalise mõju korral valuuta, milles summad on esitatud.

([3]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1094/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Kindlustus- ja Tööandjapensionide Järelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/79/EÜ (ELT L 331, 15.12.2010, lk 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1095/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Väärtpaberiturujärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/77/EÜ (ELT L 331, 15.12.2010, lk 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikkel 2

Esialgsetes teadetes esitatav konkreetne teave

Määruse (EL) 2022/2554 artikli 19 lõike 4 punktis a osutatud esialgsed teated peavad sisaldama vähemalt kogu järgmist konkreetset teavet:

a) finantssektori ettevõtja määratud intsidendi viitekood;

b) intsidendi avastamise kuupäev, avastamise aeg ja liigitus kooskõlas komisjoni delegeeritud määruse (EL) 2024/1772 ([7]) artikliga 8;

c) IKT intsidendi kirjeldus;

d) delegeeritud määruse (EL) 2024/1772 artiklites 1–8 sätestatud kriteeriumid, mille alusel finantssektori ettevõtja liigitas IKT intsidendi tõsiseks intsidendiks;

e) IKT intsidendist mõjutatud liikmesriigid;

f) teave selle kohta, kuidas IKT intsident avastati;

g) kui see on kättesaadav, siis teave IKT intsidendi päritolu kohta;

h) teave selle kohta, kas finantssektori ettevõtja on rakendanud talitluspidevuse kava;

i) kui see on kohaldatav, siis teave IKT intsidendi ümberliigitamise kohta tõsisest intsidendist mittetõsiseks intsidendiks;

j) kui see on kättesaadav, siis mis tahes muu asjakohane teave.

Artikkel 3

Vaheraportites esitatav konkreetne teave

Määruse (EL) 2022/2554 artikli 19 lõike 4 punktis b osutatud vaheraportid peavad sisaldama vähemalt kogu järgmist konkreetset teavet:

a) kui see on kohaldatav, siis pädeva asutuse esitatud intsidendi viitekood;

b) IKT intsidendi toimumise kuupäev ja kellaaeg;

c) kui see on kohaldatav, siis kuupäev ja kellaaeg, kui finantssektori ettevõtja taastas oma tavapärase tegevuse;

d) teave selle kohta, kuidas on täidetud delegeeritud määruse (EL) 2024/1772 artiklites 1–8 sätestatud kriteeriumid, mille alusel finantssektori ettevõtja liigitas IKT intsidendi tõsiseks intsidendiks;

e) IKT intsidendi liik;

f) kui see on kohaldatav, siis kõnealuse ohusubjekti kasutatud võtted ja ohud;

g) mõjutatud funktsionaalsed valdkonnad ja äriprotsessid;

h) mõjutatud taristukomponendid, mis toetavad äriprotsesse;

i) mõju klientide finantshuvidele;

j) teave IKT intsidentist muude asutuste teavitamise kohta;

k) finantssektori ettevõtja IKT intsidendist taastumiseks võetud või kavandatud meetmed või ajutised meetmed;

l) kui see on kohaldatav, siis teave ohunäitajate kohta.

([7]) Komisjoni 13. märtsi 2024. aasta delegeeritud määrus (EL) 2024/1772, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 regulatiivsete tehniliste standarditega, millega määratakse kindlaks IKT intsidentide ja küberohtude liigitamise kriteeriumid, kehtestatakse olulisuse läved ja täpsustatakse tõsiste intsidentide kohta esitatavate raportite üksikasju (ELT L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Artikkel 4

Lõppraportites esitatav konkreetne teave

Määruse (EL) 2022/2554 artikli 19 lõike 4 punktis c osutatud lõppraportid peavad sisaldama kogu järgmist konkreetset teavet:

a) teave IKT intsidendi algpõhjuste kohta;

b) IKT intsidendi lahendamise ja algpõhjuste kõrvaldamise kuupäevad ja kellaajad;

c) teave IKT intsidendi lahendamise kohta;

d) kui see on kohaldatav, siis kriisilahendusasutuste jaoks vajalik teave;

e) teave IKT intsidendist tekkinud otseste ja kaudsete kulude ja kahjude kohta ning teave tagasi saadud summade kohta;

f) kui see on kohaldatav, siis teave korduvate IKT intsidentide kohta.

Artikkel 5

Esialgsete teadete, vahearuannete ja lõpparuannete tähtajad

1. Finantssektori ettevõtjad peavad esitama määruse (EL) 2022/2554 artikli 19 lõike 4 punktides a, b ja c viidatud esialgse teate, vaheraporti ja lõppraporti järgmiste tähtaegade jooksul:

a) esialgne teade: esimesel võimalusel, aga igal juhul nelja tunni jooksul alates IKT intsidendi liigitamisest tõsiseks IKT intsidendiks ning hiljemalt 24 tunni jooksul alates ajast, kui finantssektori ettevõtja sai IKT intsidendist teada;

b) vaheraport: hiljemalt 72 tunni jooksul alates esialgse teate esitamisest isegi juhul, kui intsidendi staatus või käsitlemine ei ole muutunud, nagu on osutatud määruse (EL) 2022/2554 artikli 19 lõike 4 punktis b. Finantssektori ettevõtjad peavad esitama ajakohastatud vaheraporti ilma põhjendamatu viivituseta ja igal juhul, kui tavapärane tegevus on taastatud;

c) lõppraport: hiljemalt kuu aega pärast vaheraporti esitamist või, kui see on kohaldatav, pärast viimast ajakohastatud vaheraportit.

2. Kui finantssektori ettevõtja ei ole liigitanud IKT intsidenti tõsiseks intsidendiks 24 tunni jooksul ajast, kui finantssektori ettevõtja sai IKT intsidendist teada, aga liigitab IKT intsidendi tõsiseks intsidendiks hilisemas etapis, siis peab finantssektori ettevõtja esitama esialgse teate nelja tunni jooksul alates IKT intsidendi liigitamisest tõsiseks intsidendiks.

3. Finantssektori ettevõtjad, kes ei saa esitada esialgset teadet, vaheraportit või lõppraportit lõikes 1 märgitud tähtaja jooksul, peavad teavitama pädevat asutust sellest põhjendamatu viivituseta, aga hiljemalt teate või raporti esitamise vastava tähtaja jooksul, ning selgitama viivituse põhjuseid.

4. Kui esialgse teate, vaheraporti või lõppraporti esitamise tähtpäev jääb nädalavahetusele või riigipühale teavitava finantssektori ettevõtja liikmesriigis, siis võib finantssektori ettevõtja esitada esialgse teate, vaheraporti või lõppraporti järgmise tööpäeva lõunaks.

5. Lõiget 4 ei kohaldata juhul, kui esialgse teate või vaheraporti esitavad krediidiasutused, kesksed vastaspooled, kauplemiskohtade korraldajad ja muud finantssektori ettevõtjad, kes on määratletud direktiivi (EL) 2022/2555 artikli 3 kohaselt elutähtsate või oluliste üksustena.

6. Pädevad asutused võivad otsustada, et lõiget 4 ei kohaldata finantssektori ettevõtjate esialgse teate või vaheraporti esitamise suhtes, kui tegemist ei ole lõikes 5 osutatud finantssektori ettevõtjatega, mis on riigi või liidu tasandil finantssektori jaoks olulised või süsteemselt olulised. Pädevad asutused teatavad oma otsusest kindlaksmääratud finantssektori ettevõtjatele. Pädeva asutuse otsust kohaldatakse üksnes intsidentide suhtes, millest on teatatud pärast kuupäeva, mil pädev asutus teatas otsusest kindlaksmääratud finantssektori ettevõtjatele.

Artikkel 6

Vabatahtliku olulistest küberohtudest teatamise sisu

Määruse (EL) 2022/2554 artikli 19 lõikes 2 osutatud vabatahtliku olulistest küberohtudest teavitamise sisu peab hõlmama kõike järgmist:

a) üldine teave teatava finantssektori ettevõtja kohta, nagu on sätestatud artiklis 1;

b) olulise küberohu avastamise kuupäev ja kellaaeg ning olulise küberohuga seotud mis tahes muud olulised ajatemplid;

c) olulise küberohu kirjeldus;

d) teave olulise küberohu potentsiaalse mõju kohta finantssektori ettevõtjale, selle klientidele või finantssektori vastaspooltele;

e) liigitamise kriteeriumid, mille alusel oleks delegeeritud määruse (EL) 2024/1772 artiklite 1–8 kohaselt teavitatud tõsisest intsidendist, kui küberoht oleks realiseerunud;

f) teave olulise küberohu staatuse kohta ja mis tahes muutuste kohta ohu tegevuses;

g) kui see on kohaldatav, siis nende meetmete kirjeldus, mille finantssektori ettevõtja on võtnud, et vältida olulise küberohu realiseerumist;

h) teave olulisest küberohust teistele finantssektori ettevõtjatele või asutustele teatamise kohta;

i) kui see on kohaldatav, siis teave ohunäitajate kohta;

j) kui see on kättesaadav, siis mis tahes muu asjakohane teave.

Artikkel 7

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 23. oktoober 2024

Komisjoni nimel
president
Ursula VON DER LEYEN