2025/301

20.2.2025

KOMMISSIONENS DELEGEREDE FORORDNING (EU) 2025/301

af 23. oktober 2024

om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 for så vidt angår reguleringsmæssige tekniske standarder, der præciserer indholdet af og fristerne for den indledende underretning, den foreløbige og endelige rapport om større IKT-relaterede hændelser og indholdet af den frivillige underretning om væsentlige cybertrusler

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 ([1]), særlig artikel 20, tredje afsnit, og

ud fra følgende betragtninger:

(1) For at sikre harmonisering og forenkling af kravene til underretninger og rapporter om større IKT-relaterede hændelser, jf. artikel 19, stk. 4, i forordning (EU) 2022/2554, bør fristerne for indberetning af større IKT-relaterede hændelser følge en konsekvent tilgang for alle typer finansielle enheder. Af samme årsager bør fristerne også i videst muligt omfang følge en tilgang, som hænger sammen med kravene i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([2]), og i det mindste har samme virkning som disse.

(2) For at undgå at pålægge finansielle enheder en urimelig indberetningsbyrde på et tidspunkt, hvor de håndterer de IKT-relaterede hændelser, bør indholdet af den indledende underretning begrænses til de vigtigste oplysninger. For at kunne træffe passende tilsynsforanstaltninger har de kompetente myndigheder behov for at modtage oplysninger om større IKT-relaterede hændelser så hurtigt som muligt, efter at den finansielle enhed har klassificeret en IKT-relateret hændelse som »større«. Fristen for indgivelse af en indledende underretning, jf. artikel 19, stk. 4, litra a), i forordning (EU) 2022/2554, bør derfor være så kort som muligt efter klassificeringen af en IKT-relateret hændelse som »større«, samtidig med at der stadig gives mulighed for fleksibilitet, navnlig for forretningsmodeller for tjenester, der ikke er særligt tidskritiske, i tilfælde hvor finansielle enheder har brug for mere tid til at håndtere den IKT-relaterede hændelse, efter at de har fået kendskab til den.

(3) Efter at de kompetente myndigheder har modtaget den indledende underretning, bør de modtage mere udførlige oplysninger om den IKT-relaterede hændelse i den foreløbige rapport og alle relevante oplysninger i den endelige rapport. Oplysningerne i disse rapporter bør sætte de kompetente myndigheder i stand til yderligere at vurdere den IKT-relaterede hændelse og evaluere de tilsynsforanstaltninger, de måtte ønske at træffe.

(4) De indberetningsfrister, der er omhandlet i artikel 20, stk. 1, litra a), nr. ii), i forordning (EU) 2022/2554, bør derfor afveje behovet for, at de kompetente myndigheder hurtigt modtager oplysningerne, i forhold til behovet for at give finansielle enheder tilstrækkelig tid til at indhente fuldstændige og nøjagtige oplysninger.

(5) Idet der tages hensyn til kriterierne i artikel 20, stk. 1, litra a), i forordning (EU) 2022/2554, bør indberetningsfristerne ikke udgøre en uforholdsmæssig stor byrde for mikrovirksomheder og andre ikkevæsentlige finansielle enheder. Derudover bør indberetningsfristerne tage højde for weekender og helligdage for at undgå, at finansielle enheder pålægges en uforholdsmæssig stor byrde.

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

([2]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Da væsentlige cybertrusler skal indberettes på frivillig basis, bør indholdet af sådanne underretninger ikke udgøre en byrde for finansielle enheder og bør være mere begrænset end de oplysninger, der anmodes om i forbindelse med større IKT-relaterede hændelser.

(7) Denne forordning er baseret på det udkast til reguleringsmæssige tekniske standarder, som ESA'erne har forelagt for Kommissionen.

(8) De europæiske tilsynsmyndigheder har gennemført åbne offentlige høringer om det udkast til reguleringsmæssige tekniske standarder, som ligger til grund for denne forordning, analyseret de potentielle omkostninger og fordele samt anmodet om rådgivning fra interessentgruppen, som er nedsat i henhold til artikel 37 i Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([3]), (EU) nr. 1094/2010 ([4]) og (EU) nr. 1095/2010 ([5]).

(9) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([6]) og afgav en positiv udtalelse den 22. juli 2024. Behandling af personoplysninger inden for rammerne af nærværende forordning bør ske i overensstemmelse med de gældende databeskyttelsesprincipper og bestemmelserne i forordning (EU) 2018/1725 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Generelle oplysninger, der skal indgå i indledende underretninger, foreløbige og endelige rapporter om større IKT-relaterede hændelser

Finansielle enheder skal i den indledende underretning, den foreløbige rapport og den endelige rapport, jf. artikel 19, stk. 4, i forordning (EU) 2022/2554, forelægge følgende generelle oplysninger:

a) indberetningens art (indledende underretning, foreløbig rapport eller endelig rapport)

b) navnet på den finansielle enhed, dens LEI-kode og typen af finansiel enhed, jf. artikel 2, stk. 1, i forordning (EU) 2022/2554

c) navnet på og identifikationskoden for den enhed, der indgiver den indledende underretning, den foreløbige eller endelige rapport vedrørende den finansielle enhed

d) hvis det er relevant, navne på og LEI-koder for alle finansielle enheder, der er omfattet af den samlede indledende underretning, foreløbige eller endelige rapport

e) kontaktoplysninger for de personer, der har ansvar for at kommunikere med den kompetente myndighed om den større IKT-relaterede hændelse

f) hvis det er relevant, identifikation af modervirksomheden i den koncern, som den finansielle enhed tilhører

g) hvis der er tale om økonomiske virkninger, angives den valuta, som beløbene er baseret på.

([3]) Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EUT L 331 af 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF (EUT L 331 af 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikel 2

Specifikke oplysninger, der skal indgå i indledende underretninger

Indledende underretninger, jf. artikel 19, stk. 4, litra a), i forordning (EU) 2022/2554, skal mindst indeholde følgende specifikke oplysninger:

a) den referencekode for hændelsen, som den finansielle enhed har tildelt

b) dato for detektion, tidspunkt for detektion og klassificering af hændelsen i henhold til artikel 8 i Kommissionens delegerede forordning (EU) 2024/1772 ([7])

c) en beskrivelse af den IKT-relaterede hændelse

d) de kriterier, der er fastsat i artikel 1-8 i delegeret forordning (EU) 2024/1772, på grundlag af hvilke den finansielle enhed klassificerede den IKT-relaterede hændelse som »større«

e) de medlemsstater, der er berørt af den IKT-relaterede hændelse

f) oplysninger om, hvordan den IKT-relaterede hændelse blev opdaget

g) hvis de foreligger, oplysninger om den IKT-relaterede hændelses oprindelse

h) oplysninger om, hvorvidt den finansielle enhed har aktiveret en plan for driftsstabiliteten

i) hvis det er relevant, oplysninger om omklassificeringen af den IKT-relaterede hændelse fra »større« til »mindre«

j) hvis de foreligger, eventuelle andre relevante oplysninger.

Artikel 3

Specifikke oplysninger, der skal indgå i foreløbige rapporter

Foreløbige rapporter, jf. artikel 19, stk. 4, litra b), i forordning (EU) 2022/2554, skal mindst indeholde følgende specifikke oplysninger:

a) den referencekode for hændelsen, som den kompetente myndighed har oplyst

b) dato og klokkeslæt, hvor den IKT-relaterede hændelses indtraf

c) hvis det er relevant, den dato og det tidspunkt, hvor den finansielle enhed genoprettede sine normale aktiviteter

d) oplysninger om, hvordan de kriterier, der er fastsat i artikel 1-8 i delegeret forordning (EU) 2024/1772, på grundlag af hvilke den finansielle enhed klassificerede den IKT-relaterede hændelse som »større«, er blevet opfyldt

e) typen af IKT-relateret hændelse

f) hvis det er relevant, de trusler og teknikker, som trusselsaktøren har anvendt

g) berørte funktionelle områder og forretningsprocesser

h) berørte infrastrukturkomponenter, der understøtter forretningsprocesser

i) virkninger for kundernes finansielle interesser

j) oplysninger om indberetning af IKT-relaterede hændelser til andre myndigheder

k) midlertidige tiltag eller foranstaltninger, som den finansielle enhed har indført eller planlagt for at foretage genopretning efter den IKT-relaterede hændelse

l) hvis det er relevant, oplysninger om kompromitteringsindikatorer.

([7]) Kommissionens delegerede forordning (EU) 2024/1772 af 13. marts 2024 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 for så vidt angår reguleringsmæssige tekniske standarder, der præciserer kriterierne for klassificering af IKT-relaterede hændelser og cybertrusler, fastsætter væsentlighedstærskler og præciserer de nærmere oplysninger om indberetninger af større hændelser (EUT L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Artikel 4

Specifikke oplysninger, der skal indgå i endelige rapporter

Endelige rapporter, jf. artikel 19, stk. 4, litra c), i forordning (EU) 2022/2554, skal mindst indeholde følgende specifikke oplysninger:

a) oplysninger om de grundlæggende årsager til den IKT-relaterede hændelse

b) datoer og tidspunkter, hvor den IKT-relaterede hændelse blev løst, og den eller de grundlæggende årsag(er) blev håndteret

c) oplysninger om afviklingen af den IKT-relaterede hændelse

d) hvis det er relevant, oplysninger, der er relevante for afviklingsmyndighederne

e) oplysninger om direkte og indirekte omkostninger og tab, som hidrører fra IKT-relaterede hændelser, og oplysninger om finansielle inddrivelser

f) hvis det er relevant, oplysninger om tilbagevendende IKT-relaterede hændelser.

Artikel 5

Frister for den indledende underretning og for de foreløbige og endelige rapporter

1. Finansielle enheder skal indgive den indledende underretning og de foreløbige og endelige rapporter, jf. artikel 19, stk. 4, litra a), b) og c), i forordning (EU) 2022/2554, inden for følgende frister:

a) for den indledende underretning: så tidligt som muligt, men under alle omstændigheder senest fire timer efter klassificeringen af den IKT-relaterede hændelse som en større IKT-relateret hændelse og senest 24 timer efter det tidspunkt, hvor den finansielle enhed er fået kendskab til den IKT-relaterede hændelse

b) for den foreløbige rapport: senest 72 timer efter indgivelsen af den indledende underretning, selv hvis status eller håndtering af hændelsen ikke har ændret sig, jf. artikel 19, stk. 4, litra b), i forordning (EU) 2022/2554. Finansielle enheder skal indgive en ajourført foreløbig rapport uden unødigt ophold og under alle omstændigheder, når de normale aktiviteter er blevet genoprettet.

c) for den endelige rapport: senest en måned efter enten indgivelsen af den foreløbige rapport eller, hvis det er relevant, efter den seneste ajourførte foreløbige rapport.

2. Hvis den finansielle enhed ikke har klassificeret en IKT-relateret hændelse som »større« inden for 24 timer fra det tidspunkt, hvor den finansielle enhed har fået kendskab til den IKT-relaterede hændelse, men klassificerer den pågældende IKT-relaterede hændelse som »større« på et senere tidspunkt, skal den finansielle enhed indgive den indledende underretning inden for fire timer efter klassificeringen af den IKT-relaterede hændelse som en større hændelse.

3. Finansielle enheder, der ikke er i stand til at indgive den indledende underretning, den foreløbige rapport eller den endelige rapport inden for de i stk. 1 fastsatte frister, skal underrette den kompetente myndighed herom uden unødigt ophold, men senest inden for de respektive frister for indgivelse af underretningen eller rapporten, og redegøre for årsagerne til forsinkelsen.

4. Hvis fristen for indgivelse af en indledende underretning, foreløbig rapport eller endelig rapport falder på en weekenddag eller en helligdag i den indberettende finansielle enheds medlemsstat, kan den finansielle enhed indgive den indledende underretning, foreløbige eller endelige rapport senest kl. 12.00 på den følgende arbejdsdag.

5. Stk. 4 finder ikke anvendelse på indgivelse af en indledende underretning eller en foreløbig rapport, som foretages af kreditinstitutter, centrale modparter, operatører af markedspladser og andre finansielle enheder, der er identificeret som væsentlige eller vigtige enheder i henhold til artikel 3 i direktiv (EU) 2022/2555.

6. De kompetente myndigheder kan beslutte, at stk. 4 ikke skal finde anvendelse på indgivelse af en indledende underretning eller en foreløbig rapport fra andre finansielle enheder end dem, der er omhandlet i stk. 5, som er væsentlige eller har systemisk karakter for den finansielle sektor på nationalt plan eller EU-plan. De kompetente myndigheder skal underrette de identificerede finansielle enheder om deres beslutning. Den kompetente myndigheds beslutning finder kun anvendelse på hændelser, der indberettes efter den dato, hvor den kompetente myndighed underrettede de identificerede finansielle enheder om beslutningen.

Artikel 6

Indholdet af den frivillige underretning om væsentlige cybertrusler

Indholdet af den frivillige underretning om væsentlige cybertrusler, jf. artikel 19, stk. 2, i forordning (EU) 2022/2554, skal omfatte følgende:

a) generelle oplysninger om den indberettende finansielle enhed, jf. artikel 1

b) dato og klokkeslæt for detektion af den væsentlige cybertrussel og eventuelle andre relevante tidsstempler, som vedrører den væsentlige cybertrussel

c) en beskrivelse af den væsentlige cybertrussel

d) oplysninger om den væsentlige cybertrussels potentielle virkninger for den finansielle enhed, dens kunder eller finansielle modparter

e) de klassificeringskriterier, der ville have udløst en indberetning af en større hændelse, jf. artikel 1-8 i delegeret forordning (EU) 2024/1772, hvis cybertruslen var blevet til virkelighed

f) oplysninger om status for den væsentlige cybertrussel og eventuelle ændringer i trusselsaktiviteten

g) hvis det er relevant, en beskrivelse af de tiltag, som den finansielle enhed har iværksat for at forhindre, at de væsentlige cybertrusler bliver til virkelighed

h) oplysninger om enhver underretning om den væsentlige cybertrussel til andre finansielle enheder eller myndigheder

i) hvis det er relevant, oplysninger om kompromitteringsindikatorer

j) hvis de foreligger, eventuelle andre relevante oplysninger.

Artikel 7

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 23. oktober 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand