EUROPA-
KOMMISSIONEN

Bruxelles, den 13.3.2024
C(2024) 1519 final

KOMMISSIONENS DELEGEREDE FORORDNING (EU) …/…

af 13.3.2024

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

(EØS-relevant tekst)

BEGRUNDELSE

1. BAGGRUND FOR DEN DELEGEREDE RETSAKT

Et af målene i forordning (EU) 2022/2554 om digital operationel modstandsdygtighed i den finansielle sektor (DORA) er at harmonisere og strømline ordningen for indberetning af IKT-relaterede hændelser for finansielle enheder i EU. Med henblik herpå indføres der ved DORA konsekvente krav til finansielle enheder om styring, klassificering og indberetning af IKT-relaterede hændelser.

I den forbindelse giver artikel 18, stk. 3, i DORA de europæiske tilsynsmyndigheder (ESA'er) beføjelse til gennem Det Fælles Udvalg og i samråd med ECB og ENISA at udarbejde fælles udkast til reguleringsmæssige tekniske standarder, der indeholder en yderligere præcisering af følgende:

a) de kriterier vedrørende klassificering og fastlæggelse af virkningerne af IKT-relaterede hændelser, der er fastsat i artikel 18, stk. 1, i DORA, herunder væsentlighedstærskler til bestemmelse af større IKT-relaterede hændelser eller, alt efter hvad der er relevant, større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som er omfattet af indberetningspligten i artikel 19, stk. 1, i DORA

b) de kriterier, som de kompetente myndigheder skal anvende med henblik på at vurdere relevansen af større IKT-relaterede hændelser eller, alt efter hvad der er relevant, af større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, for de relevante myndigheder i andre medlemsstater, og de nærmere oplysninger i rapporterne om større IKT-relaterede hændelser eller, alt efter hvad der er relevant, større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som skal udveksles med andre kompetente myndigheder i henhold til artikel 19, stk. 6 og 7, i DORA, og

c) de kriterier, der skal anvendes til at klassificere cybertrusler som væsentlige, herunder høje væsentlighedstærskler til bestemmelse af væsentlige cybertrusler.

Denne delegerede forordning svarer til nævnte mandat og blev forelagt Kommissionen den 17. januar 2024.

ENISA og ECB har derfor været en del af det fælles ESA-underudvalg om digital operationel modstandsdygtighed (JC SC DOR).

2. HØRINGER FORUD FOR RETSAKTENS VEDTAGELSE

Som led i udarbejdelsen af de standarder, der er fastsat i dette udkast til delegeret forordning, offentliggjorde ESA'erne udkastet til reguleringsmæssige tekniske standarder den 19. juni 2023 for en høringsperiode på tre måneder, som sluttede den 11. september 2023. ESA'erne modtog 105 besvarelser fra forskellige markedsdeltagere i den finansielle sektor. ESA'ernes endelige rapport indeholder et fuldstændigt overblik over interessenternes besvarelserne[1].

[1] De europæiske tilsynsmyndigheder (2024), "Final report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554".

Respondenterne i den offentlige høring fremlagde bemærkninger om alle aspekter af det foreslåede udkast til reguleringsmæssige tekniske standarder. De vigtigste punkter, der blev rejst, er følgende:

- **Metoden til klassificering af større hændelser**: Mange respondenter i den offentlige høring mente, at klassificeringsmetoden er for kompleks, og at indberetningsprocessen er en udfordring for de finansielle enheder i forbindelse med styring af hændelserne. Nogle af disse respondenter foreslog også ændringer i vægtningen af forskellige kriterier, der passer bedre til deres respektive sektor (f.eks. at flytte kriteriet "berørte kunder, finansielle modparter og transaktioner", så det bliver et sekundært kriterium, at opgradere kriteriet "varighed og tjenestens nedetid" til et primært kriterium osv.). Flere respondenter foreslog også, at klassifikationsmetoden i de reguleringsmæssige tekniske standarder bør have et mere direkte fokus på virkningerne af den pågældende hændelse.
- **Klassificeringskriterierne og deres væsentlighedstærskler**: Klassificeringskriterierne i de reguleringsmæssige tekniske standarder omfatter "Berørte kunder, finansielle modparter og transaktioner", "Indvirkning på omdømmet", "Varighed og tjenestens nedetid", "Geografisk udbredelse", "Datatab", "Berørte kritiske tjenester" og "Økonomiske virkninger". Interessenterne opfordrede generelt til yderligere præciseringer (f.eks. af hvordan tærsklerne beregnes) og opfordrede ofte til at hæve væsentlighedstærsklerne.
- **Tilbagevendende hændelser**: Flere respondenter udtrykte bekymring over den operationelle byrde, som analyse af hændelser med henblik på lighedsøgninger vil medføre, herunder den betydelige brug af interne ressourcer og vanskelighederne med at vurdere dataene. Nogle af dem nævnte også proportionalitetsproblemer, da dette krav vil påvirke mindre enheder i uforholdsmæssigt høj grad.
- **Proportionalitetsprincippet**: Interessenterne understregede også betydningen af at sikre proportionalitet. Desuden ydede ESA's fælles rådgivende udvalg om proportionalitet også ad hoc-rådgivning om, hvordan proportionaliteten i udkastet til reguleringsmæssige tekniske standarder kan styrkes.

På grundlag af de modtagne bemærkninger indførte ESA'erne ændringer af udkastet til reguleringsmæssige tekniske standarder. Disse ændringer vedrører klassifikationsmetoden, præciseringen af visse klassificeringskriterier og deres væsentlighedstærskler og tilgangen vedrørende tilbagevendende hændelser:

- Med hensyn til klassificeringsmetoden har ESA'erne ændret udkastet til reguleringsmæssige tekniske standarder, således at de finansielle enheder klassificerer hændelser som større, hvis kriteriet "Berørte kritiske tjenester" er opfyldt, og i) der konstateres ondsindet uautoriseret adgang til net- og informationssystemer som en del af kriteriet om "Datatab", eller ii) væsentlighedstærsklerne for to andre kriterier er opfyldt.
- Med hensyn til klassificeringskriterierne og tærsklerne herfor har ESA'erne, samtidig med at der opretholdes en harmoniseret metode til klassificering af hændelser for alle finansielle enheder, der er omfattet af DORA's anvendelsesområde, præciseret de forskellige aspekter af klassificeringen i kriterierne og indført ændringer af tærsklerne for kriterierne "Berørte kunder, finansielle modparter og transaktioner" og "Datatab" for at indføre yderligere proportionalitet, behandle sektorspecifikke spørgsmål, der er rejst, og registrere relevante cyberhændelser.

- For at imødekomme betænkeligheder vedrørende indberetningsbyrden for finansielle enheder har ESA'erne endelig ændret metoden til klassificering af tilbagevendende hændelser, som nu har fokus på hændelser, der er indtruffet mindst to gange, som har den samme åbenlyse grundlæggende årsag, og som kumulativt ville have opfyldt kriterierne for klassificering af hændelser. Vurderingen af tilbagevenden skal foretages hver måned.

3. JURIDISKE ASPEKTER AF DEN DELEGEREDE RETSAKT

I kapitel I fastsættes kriterierne for klassificering af hændelser, som berører kunder, finansielle modparter og transaktioner (artikel 1), indvirkning på omdømmet (artikel 2), varighed og tjenestens nedetid (artikel 3), geografisk udbredelse (artikel 4), datatab (artikel 5), de berørte tjenesters kritiske betydning (artikel 6) og økonomiske virkninger (artikel 7).

I kapitel II fastsættes betingelserne for klassificering af en hændelse som større og for, hvordan tilbagevendende hændelser håndteres (artikel 8), og de dermed forbundne væsentlighedstærskler (artikel 9).

Kapitel III omfatter væsentlige cybertrusler og fastsætter væsentlighedstærskler til bestemmelse af, hvornår en cybertrussel er væsentlig (artikel 10).

I kapitel IV fastsættes regler vedrørende bestemmelse af, om en større hændelse er relevant for kompetente myndigheder i andre medlemsstater (artikel 11), og hvordan oplysninger om større hændelser skal deles med andre kompetente myndigheder (artikel 12).

Kapitel V indeholder de afsluttende bestemmelser om ikrafttræden (artikel 13).

KOMMISSIONENS DELEGEREDE FORORDNING (EU) …/…

af 13.3.2024

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

(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[2], særlig artikel 18, stk. 4, tredje afsnit, og

ud fra følgende betragtninger:

(1) Forordning (EU) 2022/2554 har til formål at harmonisere og strømline kravene til indberetning af IKT-relaterede hændelser og til operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, som berører kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere og e-pengeinstitutter ("hændelser"). I betragtning af at indberetningskravene omfatter 20 forskellige typer finansielle enheder, bør klassificeringskriterierne og væsentlighedstærsklerne til bestemmelse af større hændelser og væsentlige cybertrusler beskrives på en enkel, harmoniseret og konsekvent måde, der tager hensyn til de særlige forhold, der gør sig gældende for alle relevante finansielle enheders tjenester og aktiviteter.

(2) For at sikre proportionalitet bør klassificeringskriterierne og væsentlighedstærsklerne afspejle størrelsen og den overordnede risikoprofil samt karakteren, omfanget og kompleksiteten af alle finansielle enheders tjenester. Desuden bør kriterierne og væsentlighedstærsklerne udformes således, at de anvendes konsekvent på alle finansielle enheder, uanset deres størrelse og risikoprofil, og at de ikke udgør en uforholdsmæssigt stor indberetningsbyrde for mindre finansielle enheder. For at håndtere situationer, hvor et betydeligt antal kunder er berørt af en hændelse, der som sådan ikke overstiger den gældende tærskel, bør der dog fastsættes en absolut tærskel, der primært er rettet mod større finansielle enheder.

(3) I forbindelse med rammer for indberetning af hændelser, som har eksisteret før forordning (EU) 2022/2554 trådte i kraft, bør der sikres kontinuitet for finansielle enheder. Klassificeringskriterierne og væsentlighedstærsklerne bør derfor tilpasses og inspireres af EBA's retningslinjer for indberetning af større hændelser i henhold til

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

Europa-Parlamentets og Rådets direktiv (EU) 2015/2366[3], retningslinjerne for periodiske oplysninger og underretning om væsentlige ændringer, som transaktionsregistre skal indgive til ESMA, ECB's/FTM's ramme for indberetning af cyberhændelser og anden relevant vejledning. Klassificeringskriterierne og tærsklerne bør også være egnede til de finansielle enheder, der ikke har været underlagt krav om indberetning af hændelser forud for forordning (EU) 2022/2554.

(4) Med hensyn til klassificeringskriteriet "Berørt beløb på og antal af berørte transaktioner" er begrebet transaktioner bredt og dækker forskellige aktiviteter og tjenesteydelser på tværs af de sektorspecifikke retsakter, der finder anvendelse på finansielle enheder. Med henblik på dette klassificeringskriterium bør det ligeledes omfatte betalingstransaktioner og alle former for udveksling af finansielle instrumenter, kryptoaktiver, råvarer eller andre aktiver, også i form af margen, sikkerhedsstillelse eller pant, både mod kontanter og andre aktiver. Alle transaktioner, der involverer aktiver, hvis værdi kan udtrykkes i et pengebeløb, bør tages i betragtning til klassificeringsformål.

(5) Klassificeringskriterierne bør sikre, at der tages højde for alle relevante typer større hændelser. Mange klassificeringskriterier tager ikke nødvendigvis højde for cyberangreb i forbindelse med indtrængen i netværk eller informationssystemer. De er imidlertid vigtige, da enhver form for indtrængen i net- og informationssystemer kan skade den finansielle enhed. Klassificeringskriterierne "berørte kritiske tjenester" og "datatab" bør derfor præciseres på en sådan måde, at de tager højde for disse typer af større hændelser, navnlig uautoriseret indtrængen, som kan få alvorlige konsekvenser, heriblandt brud på datasikkerheden og datalækager, og det til trods for, at virkningerne ikke viser sig med det samme.

(6) Eftersom kreditinstitutter både er omfattet af rammen for klassificering af hændelser i henhold til artikel 18 i forordning (EU) 2022/2554 og rammen for operationel risiko i henhold til Kommissionens delegerede forordning (EU) 2018/959[4], bør metoden til vurdering af de økonomiske virkninger af en hændelse, baseret på beregningen af omkostninger og tab, i videst muligt omfang være konsekvent på tværs af begge rammer for at undgå at indføre uforenelige eller modstridende krav.

(7) Kriteriet vedrørende den geografiske udbredelse af en hændelse, der er fastsat i artikel 18, stk. 1, litra c), i forordning (EU) 2022/2554, bør fokusere på hændelsens grænseoverskridende virkninger, da de andre kriterier i nævnte artikel vil tage højde for en hændelses virkninger for en finansiel enheds aktiviteter inden for en enkelt jurisdiktion.

(8) Eftersom klassificeringskriterierne er indbyrdes afhængige og forbundet med hinanden, bør metoden til identifikation af større hændelser, der skal indberettes i henhold til artikel 19, stk. 1, i forordning (EU) 2022/2554, baseres på en kombination af kriterier, hvor nogle kriterier, der er tæt knyttet til definitionerne af en IKT-relateret

---

[3] Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, og om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

[4] Kommissionens delegerede forordning (EU) 2018/959 af 14. marts 2018 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 for så vidt angår reguleringsmæssige tekniske standarder vedrørende præciseringen af den vurderingsmetode, som de kompetente myndigheder skal anvende, når institutter gives tilladelse til at anvende avancerede målemetoder for operationel risiko (EUT L 169 af 6.7.2018, s. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

hændelse og en større IKT-relateret hændelse, jf. artikel 3, stk. 8 og 10, i forordning (EU) 2022/2554, bør spille en mere fremtrædende rolle i klassificeringen af større hændelser end andre kriterier.

(9) Med henblik på at sikre, at de indberetninger og underretninger om større hændelser, som de kompetente myndigheder modtager i henhold til artikel 19, stk. 1, i forordning (EU) 2022/2554, er relevante både til tilsynsformål og med henblik på forhindring af afsmitning på tværs af den finansielle sektor, bør væsentlighedstærsklerne gøre det muligt at tage højde for større hændelser ved bl.a. at fokusere på virkninger for enhedsspecifikke kritiske tjenester, de specifikke absolutte og relative tærskler for kunder, finansielle modparter eller transaktioner, som er indikator på væsentlige virkninger for den finansielle enhed, og virkningernes betydning i andre medlemsstater.

(10) Hændelser, der påvirker IKT-tjenester eller net- og informationssystemer, der understøtter kritiske eller vigtige funktioner, eller finansielle tjenester, der kræver tilladelse, eller ondsindet uautoriseret adgang til net- og informationssystemer, der understøtter kritiske eller vigtige funktioner, bør betragtes som hændelser, der påvirker kritiske tjenester i de finansielle enheder. Ondsindet, uautoriseret adgang til net- og informationssystemer, der understøtter finansielle enheders kritiske eller vigtige funktioner, udgør alvorlige risici for den finansielle enhed og bør, da de kan påvirke andre finansielle enheder, altid betragtes som større hændelser, der skal indberettes.

(11) Tilbagevendende hændelser, der er indbyrdes forbundet gennem en lignende åbenlys grundlæggende årsag, som hver for sig ikke er større hændelser, kan være tegn på væsentlige mangler og svagheder i den finansielle enheds hændelses- og risikostyringsprocedurer. Tilbagevendende hændelser bør derfor samlet set betragtes som større, hvis de forekommer gentagne gange over en vis periode.

(12) I betragtning af at cybertrusler kan have en negativ indvirkning på den finansielle enhed og den finansielle sektor, bør de væsentlige cybertrusler, som finansielle enheder kan indberette, fungere som indikator for sandsynligheden for, at de opstår og den potentielle indvirknings kritiske betydning. For at sikre en klar og konsekvent vurdering af cybertruslernes betydning bør klassificeringen af en cybertrussel som væsentlig derfor afhænge af sandsynligheden for, at klassificeringskriterierne for større hændelser og tærsklen herfor ville være opfyldt, hvis truslen var opstået, af typen af cybertrussel og af de oplysninger, der er til rådighed for den finansielle enhed.

(13) I betragtning af at kompetente myndigheder i andre medlemsstater skal underrettes om hændelser, der påvirker finansielle enheder og kunder i deres jurisdiktion, bør vurderingen af indvirkningen i en anden jurisdiktion i overensstemmelse med artikel 19, stk. 7, i forordning (EU) 2022/2554 baseres på den grundlæggende årsag til hændelsen, på potentiel afsmitning gennem tredjepartsudbydere og på finansielle markedsinfrastrukturer samt på hændelsens indvirkning på vigtige grupper af kunder eller finansielle modparter.

(14) De indberetnings- og underretningsprocesser, der er omhandlet i artikel 19, stk. 6 og 7, i forordning (EU) 2022/2554, bør gøre det muligt for de respektive modtagere at vurdere indvirkningen af hændelserne. De indberettede oplysninger bør derfor omfatte alle detaljer i de hændelsesindberetninger, som den finansielle enhed indsender til den kompetente myndighed.

(15) Hvis en hændelse udgør et brud på persondatasikkerheden i henhold til forordning (EU) 2016/679 og direktiv 2002/58, bør nærværende forordning ikke berøre

indberetnings- og underretningspligten i forbindelse med brud på persondatasikkerheden som fastsat i disse EU-retsakter. De kompetente myndigheder bør samarbejde og udveksle oplysninger om alle relevante spørgsmål med de myndigheder, der er omhandlet i forordning (EU) 2016/679 og direktiv 2002/58/EF.

(16) Denne forordning er baseret på det udkast til reguleringsmæssige tekniske standarder, som de europæiske tilsynsmyndigheder har forelagt Kommissionen i samråd med Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og Den Europæiske Centralbank (ECB).

(17) Det Fælles Udvalg af Europæiske Tilsynsmyndigheder, jf. artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010[5], artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010[6] og artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010[7], har afholdt åbne offentlige høringer om det udkast til reguleringsmæssige tekniske standarder, som ligger til grund for denne forordning, analyseret de potentielle omkostninger og fordele ved de foreslåede standarder og anmodet om rådgivning fra interessentgruppen for banker, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1093/2010, interessentgruppen for forsikrings- og genforsikringsordninger og interessentgruppen for arbejdsmarkedspensionsordninger, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1094/2010, og interessentgruppen for værdipapirer og markeder, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1095/2010.

(18) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725[8] og afgav en udtalelse den 24. januar 2024 —

VEDTAGET DENNE FORORDNING:

Kapitel I
Klassificeringskriterier

Artikel 1
Kunder, finansielle modparter og transaktioner

1. Antallet af kunder, der er berørt af hændelsen som omhandlet i artikel 18, stk. 1, litra a), i forordning (EU) 2022/2554, skal afspejle antallet af alle berørte kunder, uanset

---

5 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).

6 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).

7 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).

8 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).

om de er fysiske eller juridiske personer, der er eller ikke var i stand til at gøre brug af den tjeneste, som den finansielle enhed leverede under hændelsen, eller som blev negativt påvirket af hændelsen. Dette antal skal også omfatte tredjeparter, der på udtrykkelig vis er omfattet af den kontraktlige ordning mellem den finansielle enhed og kunden som modtagere af den berørte tjeneste.

2. Antallet af finansielle modparter, der er berørt af hændelsen, jf. artikel 18, stk. 1, litra a), i forordning (EU) 2022/2554, skal afspejle antallet af alle berørte finansielle modparter, der har indgået en kontraktlig ordning med den finansielle enhed.

3. I forbindelse med relevansen af de kunder og finansielle modparter, der er berørt af hændelsen som omhandlet i artikel 18, stk. 1, litra a), i forordning (EU) 2022/2554, tager den finansielle enhed hensyn til, i hvilket omfang indvirkningen på en kunde eller en finansiel modpart vil påvirke gennemførelsen af den finansielle enheds forretningsmål, samt hændelsens potentielle indvirkning på markedets effektivitet.

4. I forhold til beløbet på eller antallet af transaktioner, der er berørt af hændelsen som omhandlet i artikel 18, stk. 1, litra a), i forordning (EU) 2022/2554, tager den finansielle enhed hensyn til alle berørte transaktioner, der involverer et pengebeløb, hvor mindst én del af transaktionen gennemføres i Unionen.

5. Hvis det faktiske antal berørte kunder eller finansielle modparter eller det faktiske antal eller beløb på de berørte transaktioner ikke kan fastslås, skal den finansielle enhed estimere disse antal eller beløb på grundlag af tilgængelige data fra sammenlignelige referenceperioder.

Artikel 2
Indvirkning på omdømmet

1. Med henblik på at fastslå hændelsens indvirkning på omdømmet som omhandlet i artikel 18, stk. 1, litra a), i forordning (EU) 2022/2554 tager de finansielle enheder hensyn til, at der er sket en indvirkning på omdømmet, hvis mindst et af følgende kriterier er opfyldt:

   a) hændelsen er blevet afspejlet i medierne

   b) hændelsen har resulteret i gentagne klager fra forskellige kunder eller finansielle modparter vedrørende tjenester med direkte kundekontakt eller kritiske forretningsforbindelser

   c) den finansielle enhed vil ikke være i stand til eller vil sandsynligvis ikke være i stand til at opfylde forskriftsmæssige krav som følge af hændelsen

   d) den finansielle enhed vil eller vil sandsynligvis miste kunder eller finansielle modparter, hvilket vil få en væsentlig indvirkning på dens forretningsaktiviteter som følge af hændelsen.

2. Ved vurderingen af hændelsens indvirkning på omdømmet tager de finansielle enheder hensyn til den grad af synlighed, som hændelsen har opnået eller sandsynligvis vil opnå i forhold til hvert af de kriterier, der er anført i stk. 1.

Artikel 3
Varighed og tjenestens nedetid

1. Finansielle enheder måler varigheden af en hændelse som omhandlet i artikel 18, stk. 1, litra b), i forordning (EU) 2022/2554 fra det tidspunkt, hvor hændelsen indtræffer, til det tidspunkt, hvor den afhjælpes.

   Hvis finansielle enheder ikke er i stand til at fastslå det tidspunkt, hvor hændelsen indtraf, skal de måle hændelsens varighed fra det tidspunkt, hvor den blev detekteret. Hvis finansielle enheder bliver opmærksomme på, at hændelsen indtraf, inden den blev opdaget, måler de varigheden fra det tidspunkt, hvor hændelsen registreres i netværk eller systemlogfiler eller andre datakilder.

   Hvis finansielle enheder endnu ikke ved, hvornår hændelsen vil blive afhjulpet, eller ikke er i stand til at verificere registreringer i logfiler eller andre datakilder, anvender de estimater.

2. Finansielle enheder måler tjenestens nedetid i forbindelse med en hændelse som omhandlet i artikel 18, stk. 1, litra b), i forordning (EU) 2022/2554 fra det tidspunkt, hvor tjenesten helt eller delvist ikke er tilgængelig for kunder, finansielle modparter eller andre interne eller eksterne brugere, til det tidspunkt, hvor normale aktiviteter eller operationer er blevet genoprettet til det serviceniveau, der blev leveret før hændelsen. Hvis tjenestens nedetid forårsager en forsinkelse i leveringen af tjenesten, efter at de normale aktiviteter eller operationer er blevet genoprettet, måles nedetiden fra hændelsens start til det tidspunkt, hvor den forsinkede tjeneste leveres fuldt ud.

   Hvis finansielle enheder ikke er i stand til at fastslå det tidspunkt, hvor tjenestens nedetid startede, skal de måle tjenestens nedetid fra det tidspunkt, hvor den blev detekteret.

Artikel 4
Geografisk udbredelse

Med henblik på at bestemme den geografiske udbredelse inden for de områder, der er berørt af hændelsen som omhandlet i artikel 18, stk. 1, litra c), i forordning (EU) 2022/2554, vurderer finansielle enheder, om hændelsen har eller har haft en indvirkning i andre medlemsstater, og navnlig betydningen af indvirkningen på følgende:

a) kunder og finansielle modparter i andre medlemsstater

b) filialer eller andre finansielle enheder i koncernen, der udøver aktiviteter i andre medlemsstater

c) finansielle markedsinfrastrukturer eller tredjepartsudbydere, som kan påvirke finansielle enheder i andre medlemsstater, som de leverer tjenesteydelser til, i det omfang sådanne oplysninger er tilgængelige.

Artikel 5
Datatab

Med henblik på at bestemme de datatab, som hændelsen medfører som omhandlet i artikel 18, stk. 1, litra d), i forordning (EU) 2022/2554, tager de finansielle enheder hensyn til følgende:

a) for så vidt angår tilgængeligheden af data, om hændelsen har gjort dataene om efterspørgsel fra den finansielle enhed, dens kunder eller dens modparter midlertidigt eller permanent utilgængelige eller ubrugelige

b) med hensyn til autenticiteten af data, om hændelsen har bragt datakildens pålidelighed i fare

c) for så vidt angår integriteten af data, om hændelsen har ført til en ikkegodkendt ændring af data, der har gjort dem unøjagtige eller ufuldstændige

d) med hensyn til fortroligheden af data, om hændelsen har resulteret i, at data er blevet tilgået af eller videregivet til en uautoriseret part eller et uautoriseret system.

Artikel 6
De berørte tjenesters kritiske betydning

Med henblik på at bestemme de berørte tjenesters kritiske betydning som omhandlet i artikel 18, stk. 1, litra e), i forordning (EU) 2022/2554, vurderer finansielle enheder, hvorvidt hændelsen:

a) påvirker eller har påvirket IKT-tjenester eller net- og informationssystemer, der understøtter kritiske eller vigtige funktioner i den finansielle enhed

b) påvirker eller har påvirket finansielle tjenesteydelser, der leveres af den finansielle enhed, og som kræver godkendelse eller registrering, eller som er underlagt kompetente myndigheders tilsyn

c) udgør eller har udgjort en vellykket, ondsindet og uautoriseret adgang til den finansielle enheds net- og informationssystemer.

Artikel 7
Økonomiske virkninger

1. Med henblik på at fastsætte de økonomiske virkninger af hændelsen som omhandlet i artikel 18, stk. 1, litra f), i forordning (EU) 2022/2554 tager de finansielle enheder, uden at indregne finansielle inddrivelser, hensyn til følgende typer af direkte og indirekte omkostninger og tab, som de har afholdt og lidt som følge af hændelsen:

   a) eksproprierede midler eller finansielle aktiver, som de hæfter for, herunder aktiver, der er gået tabt som følge af tyveri

   b) omkostninger ved udskiftning eller flytning af software, hardware eller infrastruktur

   c) personaleomkostninger, herunder omkostninger ved udskiftning eller flytning af personale, ansættelse af ekstra personale, aflønning af overarbejde og genopretning af mistede eller forringede kvalifikationer

   d) gebyrer som følge af manglende overholdelse af kontraktlige forpligtelser

   e) omkostninger ved klageadgang og kompensation til kunder

   f) tab som følge af mistede indtægter

   g) omkostninger forbundet med effektiviteten af den interne og eksterne kommunikation

   h) rådgivningsomkostninger, herunder omkostninger i forbindelse med juridisk rådgivning, kriminaltekniske tjenester og oprydningstjenester.

2. Omkostninger og tab som omhandlet i stk. 1 omfatter ikke omkostninger, der er nødvendige for den daglige drift af virksomheden, navnlig følgende:

a) omkostninger ved generel vedligeholdelse af infrastruktur, udstyr, hardware og software samt udgifter til ajourføring af personalets kvalifikationer

b) interne eller eksterne omkostninger i forbindelse med at styrke virksomheden efter hændelsen, herunder opgraderinger, forbedringer og risikovurderingsinitiativer

c) forsikringspræmier.

3. Finansielle enheder beregner de beløb, som udgøres af omkostninger og tab, på grundlag af data, der er tilgængelige på indberetningstidspunktet. Hvis de faktiske omkostninger og tab ikke kan opgøres, estimerer finansielle enheder disse beløb.

4. Ved vurderingen af hændelsens økonomiske virkninger sammenlægger de finansielle enheder de omkostninger og tab, der er omhandlet i stk. 1.

Kapitel II
Større hændelser og væsentlighedstærskler

Artikel 8
Større hændelser

1. En hændelse betragtes som en større hændelse med henblik på artikel 19, stk. 1, i forordning (EU) 2022/2554, hvis den har påvirket kritiske tjenester som omhandlet i artikel 6, og hvis en af følgende betingelser er opfyldt:

a) væsentlighedstærsklen i artikel 9, stk. 5, litra b), er nået

b) to eller flere af de andre væsentlighedstærskler, der er omhandlet i artikel 9, stk. 1-6, er nået.

2. Tilbagevendende hændelser, der hver for sig ikke betragtes som en større hændelse i overensstemmelse med stk. 1, betragtes som én større hændelse, hvis de opfylder alle følgende betingelser:

a) de har fundet sted mindst to gange inden for seks måneder

b) de har den samme åbenlyse grundlæggende årsag som omhandlet i artikel 20, litra b), i forordning (EU) 2022/2554

c) de opfylder samlet set kriterierne for at blive betragtet som en større hændelse, jf. stk. 1.

Finansielle enheder vurderer forekomsten af tilbagevendende hændelser en gang om måneden.

Dette stykke finder ikke anvendelse på mikrovirksomheder og finansielle enheder, der er opført i artikel 16, stk. 1, i forordning (EU) 2022/2554.

Artikel 9
Væsentlighedstærskler til bestemmelse af større hændelser

1. Væsentlighedstærsklen for kriteriet "kunder, finansielle modparter og transaktioner" er nået, hvis en af følgende betingelser er opfyldt:

a) antallet af berørte kunder er højere end 10 % af alle kunder, der benytter den berørte tjeneste

b) antallet af berørte kunder, der anvender den berørte tjeneste, er højere end 100 000

c) antallet af berørte finansielle modparter er højere end 30 % af alle finansielle modparter, der udøver aktiviteter i forbindelse med leveringen af den berørte tjeneste

d) antallet af berørte transaktioner er højere end 10 % af det daglige gennemsnitlige antal transaktioner, der gennemføres af den finansielle enhed i forbindelse med den berørte tjeneste

e) beløbet på berørte transaktioner er højere end 10 % af den daglige gennemsnitlige værdi af transaktioner, der gennemføres af den finansielle enhed i forbindelse med den berørte tjeneste

f) kunder eller finansielle modparter, der er blevet identificeret som relevante i overensstemmelse med artikel 1, stk. 3, er blevet berørt.

Hvis det faktiske antal berørte kunder eller finansielle modparter eller det faktiske antal eller beløb på de berørte transaktioner ikke kan fastslås, skal den finansielle enhed estimere disse antal eller beløb på grundlag af tilgængelige data fra sammenlignelige referenceperioder.

2. Væsentlighedstærsklen for kriteriet "indvirkning på omdømmet" er nået, hvis en af betingelserne i artikel 2, litra a)-d), er opfyldt.

3. Væsentlighedstærsklen for kriteriet "varighed og tjenestens nedetid" er nået, hvis en af følgende betingelser er opfyldt:

a) hændelsen varer længere end 24 timer

b) tjenestens nedetid er længere end 2 timer for IKT-tjenester, der understøtter kritiske eller vigtige funktioner.

4. Væsentlighedstærsklen for kriteriet "geografisk udbredelse" er nået, hvis hændelsen har en indvirkning i to eller flere medlemsstater i overensstemmelse med artikel 4.

5. Væsentlighedstærsklen for kriteriet "datatab" er nået, hvis en af følgende betingelser er opfyldt:

a) enhver indvirkning som omhandlet i artikel 5 på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data har eller vil få en negativ indvirkning på gennemførelsen af den finansielle enheds forretningsmål eller på dens evne til at opfylde forskriftsmæssige krav

b) enhver vellykket, ondsindet og uautoriseret adgang, der ikke er omfattet af litra a), til net- og informationssystemer, i tilfælde hvor en sådan adgang kan medføre tab af data.

6. Væsentlighedstærsklen for kriteriet "økonomisk virkning" er nået, hvis den finansielle enheds omkostninger og tab som følge af hændelsen har overskredet eller sandsynligvis vil overstige 100 000 EUR.

Kapitel III
Væsentlige cybertrusler

Artikel 10

Høje væsentlighedstærskler til bestemmelse af væsentlige cybertrusler

Med henblik på artikel 18, stk. 2, i forordning (EU) 2022/2554 anses en cybertrussel for at være væsentlig, hvis alle følgende betingelser er opfyldt:

a) cybertruslen kan, hvis den finder sted, påvirke eller have påvirket den finansielle enheds kritiske eller vigtige funktioner eller kan påvirke andre finansielle enheder, tredjepartsudbydere, kunder eller finansielle modparter på grundlag af oplysninger, der er tilgængelige for den finansielle enhed

b) der er stor sandsynlighed for, at cybertruslen finder sted i den finansielle enhed eller i andre finansielle enheder, idet der som minimum tages hensyn til følgende elementer:

   i) relevante risici forbundet med den cybertrussel, der er omhandlet i litra a), herunder potentielle sårbarheder i den finansielle enheds systemer, der kan udnyttes

   ii) trusselsaktørernes kapaciteter og hensigt, i det omfang den finansielle enhed har kendskab hertil

   iii) truslens vedholdenhed og eventuel indhentet viden om hændelser, der har påvirket den finansielle enhed eller dens tredjepartsudbyder, kunder eller finansielle modparter

c) cybertruslen kan, hvis den finder sted, opfylde eller nå et eller en af følgende:

   i) kriteriet vedrørende tjenesters kritiske betydning som fastsat i artikel 18, stk. 1, litra e), i forordning (EU) 2022/2554, jf. nærværende forordnings artikel 6

   ii) væsentlighedstærsklen som fastsat i artikel 9, stk. 1

   iii) væsentlighedstærsklen som fastsat i artikel 9, stk. 4.

Hvis den finansielle enhed afhængigt af typen af cybertrussel og tilgængelige oplysninger konkluderer, at væsentlighedstærsklerne i artikel 9, stk. 2, 3, 5 og 6, kan nås, kan disse tærskler også tages i betragtning.

Kapitel IV
Større hændelsers relevans for kompetente myndigheder i andre medlemsstater og nærmere oplysninger om indberetninger, der skal deles med andre kompetente myndigheder

Artikel 11

Større hændelsers relevans for kompetente myndigheder i andre medlemsstater

Vurderingen af, om den større hændelse er relevant for kompetente myndigheder i andre medlemsstater som omhandlet i artikel 19, stk. 7, i forordning (EU) 2022/2554, baseres på, om hændelsen har en grundlæggende årsag, der hidrører fra en anden medlemsstat, eller om hændelsen har eller har haft en betydelig indvirkning i en anden medlemsstat i forbindelse med et af følgende:

a) kunder eller finansielle modparter

b) en filial i den finansielle enhed eller en anden finansiel enhed i koncernen

c) en finansiel markedsinfrastruktur eller en tredjepartsudbyder, der kan påvirke finansielle enheder, som de leverer tjenester til.

Artikel 12
Nærmere oplysninger om større hændelser, der skal deles med andre kompetente myndigheder

De nærmere oplysninger om større hændelser, som de kompetente myndigheder skal indberette til andre kompetente myndigheder i overensstemmelse med artikel 19, stk. 6, i forordning (EU) 2022/2554, og de underretninger, som EBA, ESMA eller EIOPA og ECB skal indgive til de relevante kompetente myndigheder i andre medlemsstater i overensstemmelse med nævnte forordnings artikel 19, stk. 7, skal uden nogen form for anonymisering indeholde samme niveau af oplysninger som de underretninger og indberetninger af større hændelser, der modtages fra finansielle enheder i overensstemmelse med artikel 19, stk. 4, i forordning (EU) 2022/2554.

Kapitel V
Afsluttende bestemmelser

Artikel 13
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 13.3.2024.

På Kommissionens vegne
Formand
Ursula VON DER LEYEN