EUROPEISKA
KOMMISSIONEN

Bryssel den 23.10.2024
C(2024) 6901 final

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…

av den 23.10.2024

om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska tillsynsstandarder som specificerar innehåll och tidsfrister för den första anmälan av, delrapporten och slutrapporten om allvarliga IKT-relaterade incidenter samt innehållet i den frivilliga anmälan av betydande cyberhot

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL DEN DELEGERADE AKTEN

Ett av målen med förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (*Doraförordningen*) är att harmonisera och effektivisera systemet för rapportering av IKT-relaterade incidenter för finansiella entiteter i EU.

Enligt artikel 20 i Doraförordningen ska de europeiska tillsynsmyndigheterna, genom den gemensamma kommittén och i samråd med Europeiska centralbanken och Europeiska unionens cybersäkerhetsbyrå (Enisa), utarbeta

- förslag till tekniska tillsynsstandarder för att fastställa innehållet i rapporterna om IKT-relaterade incidenter och anmälan av betydande cyberhot samt inom vilka tidsfrister finansiella entiteter bör rapportera dessa incidenter till behöriga myndigheter.

Enligt artikel 20 i Doraförordningen ska de europeiska tillsynsmyndigheterna dessutom säkerställa att kraven i denna förordning är proportionella och överensstämmer med incidentrapporteringen enligt direktiv (EU) 2022/2555 (NIS 2-direktivet).

2. SAMRÅD SOM FÖREGÅTT ANTAGANDET AV AKTEN

Som ett led i utarbetandet av standarderna i denna förordning offentliggjorde de europeiska tillsynsmyndigheterna den 8 december 2023 förslaget till tekniska tillsynsstandarder för en samrådsperiod på tre månader som avslutades den 4 mars 2024. De europeiska tillsynsmyndigheterna mottog 109 svar från en mängd olika marknadsaktörer inom finanssektorn. Svaren från berörda parter sammanfattas i de europeiska tillsynsmyndigheternas slutrapport.

De europeiska tillsynsmyndigheterna instämde i merparten av de synpunkter och underliggande argument som framfördes och har infört ändringar i de tekniska tillsynsstandarderna. Ändringarna gäller tidsfristerna för första anmälan, delrapporten och slutrapporten, rapportering under veckoslut och helgdagar, aggregerad rapportering och rationalisering av innehållet i rapporteringsmallen.

När det gäller tidsfristerna för rapportering har de europeiska tillsynsmyndigheterna förlängt tidsfristen för delrapporten med upp till 24 timmar och för slutrapporten med minst 72 timmar genom att den börjar löpa från och med inlämnandet av den föregående anmälan/rapporten, i stället för från och med tidpunkten då incidenten klassificerats, vilket var fallet i det ursprungliga förslag till tekniska tillsynsstandarder som lades fram för samråd.

När det gäller rapportering under veckoslut och helgdagar har de europeiska tillsynsmyndigheterna begränsat vilka incidenter som måste rapporteras, avskaffat skyldigheten för mindre finansiella entiteter att göra en första anmälan och förlängt tidsfristen för anmälningar och rapporter till kl. 12.00 den första arbetsdagen i stället för inom 1 timme, vilket var fallet i det ursprungliga förslag till tekniska tillsynsstandarder som lades fram för samråd.

De europeiska tillsynsmyndigheterna har slutligen infört aggregerad rapportering på nationell nivå för finansiella entiteter som står under tillsyn av en enda behörig myndighet, förutsatt att vissa villkor är uppfyllda.

3. DEN DELEGERADE AKTENS RÄTTSLIGA ASPEKTER

I artikel 1 fastställs formatet för den typ av information som de finansiella entiteterna ska lämna.

I artikel 2 fastställs den allmänna information som de finansiella entiteterna måste lämna i samband med en första anmälan av allvarliga IKT-relaterade incidenter samt i del- och slutrapporter.

I artikel 3 definieras den information som de finansiella entiteterna måste lämna om den allvarliga IKT-relaterade incidenten i sin första anmälan.

I artikel 4 definieras den information som de finansiella entiteterna måste lämna om den allvarliga IKT-relaterade incidenten i sin delrapport.

I artikel 5 definieras den information som de finansiella entiteterna måste lämna om den allvarliga IKT-relaterade incidenten i sin slutrapport.

I artikel 6 fastställs tidsfristerna för inlämning av den första anmälan, den delrapport och de slutrapporter som avses i artikel 19.4 i förordning (EU) 2022/2554.

I artikel 7 fastställs innehållet i den frivilliga anmälan om betydande cyberhot.

Artikel 8 innehåller slutbestämmelserna om ikraftträdande.

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…

av den 23.10.2024

om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska tillsynsstandarder som specificerar innehåll och tidsfrister för den första anmälan av, delrapporten och slutrapporten om allvarliga IKT-relaterade incidenter samt innehållet i den frivilliga anmälan av betydande cyberhot

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011[1], särskilt artikel 20 tredje stycket, och

av följande skäl:

(1) För att harmonisera och förenkla de anmälnings- och rapporteringskrav för allvarliga IKT-relaterade incidenter som avses i artikel 19.4 i förordning (EU) 2022/2554 bör tidsfristerna för rapportering av allvarliga IKT-relaterade incidenter vara konsekventa för alla typer av finansiella entiteter. Tidsfristerna bör av detta skäl även i största möjliga utsträckning överensstämma med, och åtminstone ha samma verkan som, kraven i Europaparlamentets och rådets direktiv (EU) 2022/2555[2].

(2) För att inte lägga en orimlig rapporteringsbörda på de finansiella entiteterna i ett läge då de måste hantera den IKT-relaterade incidenten bör den första anmälan bara innehålla den viktigaste informationen. För att kunna vidta lämpliga tillsynsåtgärder måste behöriga myndigheter få information om allvarliga IKT-relaterade incidenter så snart som möjligt efter det att den finansiella entiteten har klassificerat en IKT-relaterad incident som allvarlig. Tidsfristen för den första anmälan som avses i artikel 19.4 a i förordning (EU) 2022/2554 bör följaktligen vara så kort som möjligt efter det att en IKT-relaterad incident har klassificerats som allvarlig, men samtidigt ge utrymme för flexibilitet, i synnerhet för affärsmodeller som inte är särskilt tidskritiska, för det fall att finansiella entiteter behöver mer tid att hantera den IKT-relaterade incidenten sedan de blivit medvetna om den.

---

[1] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[2] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80), ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(3) Efter att ha mottagit den första anmälan bör behöriga myndigheter få mer detaljerad information om den IKT-relaterade incidenten i delrapporten och all relevant information i slutrapporten. Informationen i dessa rapporter bör göra det möjligt för behöriga myndigheter att göra ytterligare bedömningar av den IKT-relaterade incidenten och ta ställning till vilka tillsynsåtgärder de kan vilja vidta.

(4) De tidsfrister för rapportering som avses i artikel 20 första stycket a ii i förordning (EU) 2022/2554 bör därför väga behöriga myndigheters behov av att snabbt få information mot behovet av att ge de finansiella entiteterna tillräckligt med tid att inhämta information som är fullständig och korrekt.

(5) Med beaktande av kriterierna i artikel 20 första stycket a i förordning (EU) 2022/2554 bör tidsfristerna för rapportering inte utgöra en oproportionerligt stor börda för mikroföretag och andra finansiella entiteter som inte är betydande. För att undvika en oproportionerligt stor börda för finansiella entiteter bör tidsfristerna för rapportering dessutom ta hänsyn till veckoslut och helgdagar.

(6) Eftersom betydande cyberhot anmäls på frivillig basis bör innehållet i sådana anmälningar inte vara betungande för finansiella entiteter utan mer begränsat än den information som krävs för allvarliga IKT-relaterade incidenter.

(7) Denna förordning grundar sig på det förslag till tekniska tillsynsstandarder som de europeiska tillsynsmyndigheterna har överlämnat till kommissionen.

(8) De europeiska tillsynsmyndigheterna har genomfört öppna offentliga samråd om det förslag till tekniska tillsynsstandarder som den här förordningen baseras på, analyserat potentiella kostnader och fördelar, samt begärt ett yttrande från de intressentgrupper som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordningar (EU) nr 1093/2010, 1094/2010 och 1095/2010[3].

(9) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725[4] och avgav ett yttrande den 22 juli 2024. All behandling av personuppgifter inom ramen för denna förordning bör utföras i enlighet med tillämpliga dataskyddsprinciper och bestämmelser i förordning (EG) 2018/1725.

---

[3] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj), Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj) och Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84, ELI:). http://data.europa.eu/eli/reg/2010/1095/oj).

[4] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Allmän information som ska lämnas i den första anmälan och i del- och slutrapporter om allvarliga IKT-relaterade incidenter

Finansiella entiteter ska i den första anmälan, den delrapport och den slutrapport som avses i artikel 19.4 i förordning (EU) 2022/2554 inkludera följande allmänna information:

(a) Typen av rapportering (första anmälan, delrapport eller slutrapport).

(b) Den finansiella entitetens namn, LEI-kod och typ enligt artikel 2.1 i förordning (EU) 2022/2554.

(c) Namn och id-kod för den entitet som lämnar in den första anmälan, delrapporten eller slutrapporten för den finansiella entiteten.

(d) I tillämpliga fall, namn och LEI-koder för alla finansiella entiteter som omfattas av en aggregerad första anmälan eller del- eller slutrapport.

(e) Kontaktuppgifter för de personer som ansvarar för kommunikationen med den behöriga myndigheten om den allvarliga IKT-relaterade incidenten.

(f) I tillämpliga fall, uppgift om moderföretaget i den koncern som den finansiella entiteten tillhör.

(g) I fall med ekonomiska följder, den valuta i vilken beloppen anges.

Artikel 2

Särskild information som ska lämnas i en första anmälan

En första anmälan enligt artikel 19.4 a i förordning (EU) 2022/2554 ska innehålla åtminstone följande specifika uppgifter:

(a) Den referenskod för incidenten som tilldelats av den finansiella entiteten.

(b) Datum och klockslag för upptäckt samt klassificering av incidenten i enlighet med artikel 8 i kommissionens delegerade förordning (EU) 2024/1772[5].

(c) En beskrivning av den IKT-relaterade incidenten.

(d) De kriterier i artiklarna 1–8 i delegerad förordning (EU) 2024/1772 på grundval av vilka den finansiella entiteten klassificerade den IKT-relaterade incidenten som allvarlig.

(e) De medlemsstater som påverkas av den IKT-relaterade incidenten.

(f) Information om hur den IKT-relaterade incidenten upptäcktes.

(g) Om tillgänglig, information om ursprunget till den IKT-relaterade incidenten.

(h) Information om huruvida den finansiella entiteten har aktiverat en kontinuitetsplan.

[5] Kommissionens delegerade förordning (EU) 2024/1772 av den 13 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar kriterierna för klassificering av IKT-relaterade incidenter och cyberhot, fastställande av väsentlighetströsklar och närmare uppgifter om rapporter om allvarliga incidenter (EUT L 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(i) I tillämpliga fall, information om att den IKT-relaterade incidenten omklassificerats från allvarlig till inte allvarlig.

(j) Om tillgänglig, annan relevant information.

Artikel 3
Särskild information som ska lämnas i en delrapport

En delrapport enligt artikel 19.4 b i förordning (EU) 2022/2554 ska innehålla åtminstone följande specifika uppgifter:

(a) I tillämpliga fall, den referenskod för incidenten som lämnats av den behöriga myndigheten.

(b) Datum och klockslag för den IKT-relaterade incidenten.

(c) I tillämpliga fall, datum och klockslag då den finansiella entiteten kunde återuppta normal verksamhet.

(d) Information om uppfyllandet av de kriterier i artiklarna 1–8 i delegerad förordning (EU) 2024/1772 på grundval av vilka den finansiella entiteten klassificerade den IKT-relaterade incidenten som allvarlig.

(e) Typen av IKT-relaterad incident.

(f) I tillämpliga fall, de hot och den teknik som används av den fientliga aktören.

(g) Berörda funktionsområden och affärsprocesser.

(h) Berörda infrastrukturkomponenter som stöder affärsprocesser.

(i) Inverkan på kundernas ekonomiska intressen.

(j) Information om rapporteringen av den IKT-relaterade incidenten till andra myndigheter.

(k) Tillfälliga åtgärder som den finansiella entiteten har vidtagit eller planerar att vidta för att återhämta sig från den IKT-relaterade incidenten.

(l) I tillämpliga fall, information om angreppsindikatorer.

Artikel 4
Särskild information som ska lämnas i en slutrapport

En slutrapport enligt artikel 19.4 c i förordning (EU) 2022/2554 ska innehålla åtminstone följande specifika uppgifter:

(a) Information om bakomliggande orsaker till den IKT-relaterade incidenten.

(b) Datum och klockslag då den IKT-relaterade incidenten åtgärdades och de bakomliggande orsakerna hanterades.

(c) Information om hur den IKT-relaterade incidenten åtgärdades.

(d) I tillämpliga fall, information som är relevant för resolutionsmyndigheter.

(e) Information om direkta och indirekta kostnader och förluster till följd av den IKT-relaterade incidenten samt information om finansiella återkrav.

(f) I tillämpliga fall, information om återkommande IKT-relaterade incidenter.

Artikel 5

Tidsfrister för en första anmälan och för del- och slutrapporter

1. Finansiella entiteter ska lämna in den första anmälan och de del- och slutrapporter som avses i artikel 19.4 a, b och c i förordning (EU) 2022/2554 inom följande tidsfrister:

   (a) För den första rapporten: Så tidigt som möjligt, men under alla omständigheter, inom fyra timmar från det att den IKT-relaterade incidenten klassificerats som en allvarlig IKT-relaterad incident och senast 24 timmar efter det att den finansiella entiteten har blivit medveten om den IKT-relaterade incidenten.

   (b) För delrapporten: Senast inom 72 timmar från det att den första anmälan lämnades in, även om statusen för incidenten eller hanteringen av den inte har förändrats på det sätt som avses i artikel 19.4 b i förordning (EU) 2022/2554. Finansiella entiteter ska utan onödigt dröjsmål och under alla omständigheter så snart normal verksamhet har återupptagits lämna in en uppdaterad delrapport.

   (c) För slutrapporten: Senast en månad efter antingen inlämnandet av delrapporten eller, i tillämpliga fall, efter den senaste uppdaterade delrapporten.

2. Om den finansiella entiteten inte inom 24 timmar från den tidpunkt då den blev medveten om den IKT-relaterade incidenten har klassificerat den som allvarlig, men i ett senare skede klassificerar den som allvarlig, ska den finansiella entiteten lämna in en första anmälan inom fyra timmar från det att den IKT-relaterade incidenten klassificerades som en allvarlig incident.

3. Finansiella entiteter som inte kan lämna in en första anmälan, delrapport eller slutrapport inom de tidsfrister som anges i punkt 1 ska informera den behöriga myndigheten om detta utan onödigt dröjsmål, men inte senare än respektive tidsfrister för inlämnande av anmälan eller rapporten, samt redogöra för skälen till förseningen.

4. Om tidsfristen för inlämnande av en första anmälan, delrapport eller slutrapport löper ut under ett veckoslut eller på en helgdag i den rapporterande finansiella entitetens medlemsstat får den finansiella entiteten lämna in en första anmälan, delrapport eller slutrapport senast kl. 12.00 närmast påföljande arbetsdag.

5. Punkt 4 ska inte tillämpas på inlämning av en första anmälan eller delrapport från kreditinstitut, centrala motparter, operatörer av handelsplatser och andra finansiella entiteter som bedömts som väsentliga eller viktiga entiteter i enlighet med artikel 3 i direktiv (EU) 2022/2555.

6. Behöriga myndigheter får besluta att punkt 4 inte ska gälla inlämnandet av en första anmälan eller en delrapport av andra finansiella entiteter än de som avses i punkt 5 och som är betydande eller systemviktiga för den finansiella sektorn på nationell nivå eller unionsnivå. Behöriga myndigheter ska meddela identifierade finansiella entiteter sitt beslut. Den behöriga myndighetens beslut ska endast gälla incidenter som rapporteras efter det datum då den behöriga myndigheten meddelade identifierade finansiella entiteter sitt beslut.

Artikel 6
Innehåll i den frivilliga anmälan av betydande cyberhot

Innehållet i den frivilliga anmälan av betydande cyberhot som avses i artikel 19.2 i förordning (EU) 2022/2554 ska omfatta följande:

(a) Allmän information om den anmälande finansiella entiteten enligt artikel 1.

(b) Datum och klockslag då det betydande cyberhotet upptäcktes och andra relevanta tidsstämplar som har anknytning till det betydande cyberhotet.

(c) En beskrivning av det betydande cyberhotet.

(d) Information om det betydande cyberhotets potentiella inverkan på den finansiella entiteten, dess kunder eller finansiella motparter.

(e) De klassificeringskriterier som skulle ha föranlett en rapport om allvarliga incidenter enligt artiklarna 1–8 i delegerad förordning (EU) 2024/1772 om cyberhotet hade materialiserats.

(f) Information om det betydande cyberhotets status och om eventuella förändringar i hotaktivitet.

(g) I tillämpliga fall, en beskrivning av de åtgärder som den finansiella entiteten har vidtagit för att förhindra att de betydande cyberhoten materialiseras.

(h) Information om alla underrättelser om det betydande cyberhotet till andra finansiella entiteter eller myndigheter.

(i) I tillämpliga fall, information om angreppsindikatorer.

(j) Om tillgänglig, annan relevant information.

Artikel 7
Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 23.10.2024

På kommissionens vägnar
Ordförande
Ursula VON DER LEYEN