Europeiska unionens
officiella tidning

SV
L-serien

2025/299

13.2.2025

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2025/299

av den 31 oktober 2024

om komplettering av Europaparlamentets och rådets förordning (EU) 2023/1114 om marknader för kryptotillgångar vad gäller tekniska tillsynsstandarder för kontinuitet och regelbundenhet vid utförande av kryptotillgångstjänster

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA DELEGERADE FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2023/1114 av den 31 maj 2023 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937 ([1]), särskilt artikel 68.10 tredje stycket, och

av följande skäl:

(1) I artiklarna 11 och 12 i Europaparlamentets och rådets förordning (EU) 2022/2554 ([2]) föreskrivs krav avseende åtgärder och återställande, strategier och förfaranden för säkerhetskopiering och förfaranden och metoder för återskapande och återställning avseende finansiella enheters, inbegripet kryptotillgångstjänsteleverantörers, IKT-system. I kommissionens delegerade förordning (EU) 2024/1774 ([3]) ges en närmare beskrivning av komponenterna i IKT-kontinuitetspolicyn, testningen av IKT-kontinuitetsplaner, och komponenterna i finansiella enheters, inbegripet kryptotillgångstjänsteleverantörers, IKT-åtgärds- och IKT-återställningsplaner. Denna förordning kompletterar de bestämmelserna i förordning (EU) 2022/2554 och i delegerade förordning (EU) 2024/1774 när det gäller kontinuitet och regelbundenhet vid utförande av kryptotillgångstjänster.

(2) Leverantörerna av kryptotillgångstjänster får när de tillhandahåller sina tjänster använda en distribuerad liggare som de inte har någon kontroll över, inbegripet en tillståndslös distribuerad liggare. I ett sådant fall kan det hända att de inte kan säkerställa regelbundenheten och kontinuiteten i sina tjänster när störningar orsakas av problem som är förbundna med driften av sådana distribuerade liggare. För att minska marknadsvolatiliteten som kan ha en negativ inverkan på kunder som påverkas av sådana störningar bör leverantörerna av kryptotillgångstjänster i sin kontinuitetspolicy inkludera åtgärder för snabb kommunikation med kunder och andra externa intressenter. Sådan kommunikation bör omfatta viktig och aktuell information till kunder om sådana störningar, inbegripet pågående statusuppdateringar, till dess att störningarna har åtgärdats och tjänsterna återupptas. Om informationen om statusen för den tillståndsfria distribuerade liggare som är ansvarig för ett avbrott i tjänsten inte är lätt tillgänglig för leverantören av kryptotillgångstjänster, bör leverantören av kryptotillgångstjänster efter bästa förmåga meddela uppdateringar till kunder och andra intressenter, inbegripet behöriga myndigheter, för att säkerställa att kunderna och intressenterna har så omfattande information som möjligt om sådana störningar.

([1]) EUT L 150, 9.6.2023, s. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

([2]) 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).

([3]) Kommissionens delegerade förordning (EU) 2024/1774 av den 13 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar verktyg, metoder, processer och strategier för IKT-riskhantering och den förenklade IKT-riskhanteringsramen (EUT L, 2024/1774, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1774/oj).

(3) För att undvika en oproportionerlig administrativ börda för små och medelstora företag och nystartade företag bör leverantörerna av kryptotillgångstjänster i sin kontinuitetspolicy beakta omfattningen, arten och urvalet av de tjänster som de tillhandahåller. Detta innebär att leverantörerna av kryptotillgångstjänster bör fastställa sina specifika kontinuitetskrav på grundval av en robust självbedömning, baserat på ett antal kriterier som gör det möjligt att genomföra en kontinuitetspolicy som står i proportion till deras tjänsters inverkan på marknaden. Självbedömningen bör också ta hänsyn till andra omständigheter utöver de som förtecknas i bilagan som kan ha inverkan på leverantören av kryptotillgångstjänster.

(4) Denna förordning grundar sig på det förslag till tekniska tillsynsstandarder som Europeiska värdepappers- och marknadsmyndigheten (Esma) har överlämnat till kommissionen.

(5) Europeiska värdepappers- och marknadsmyndigheten har anordnat öppna offentliga samråd om det förslag till tekniska tillsynsstandarder som denna förordning bygger på, analyserat de potentiella kostnaderna och fördelarna därav och begärt råd från den intressentgrupp för värdepapper och marknader som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordning (EU) nr 1095/2010 ([4]).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Definitioner

I denna förordning gäller följande definitioner:

a) *kritisk eller viktig funktion*: en kritisk eller viktig funktion enligt definitionen i artikel 3.22 i förordning (EU) 2022/2554.

b) *tillståndsfri distribuerad liggare*: en specifik typ av distribuerad liggare där ingen enhet kontrollerar den distribuerade liggaren och DLT-nätnoder kan inrättas av varje person som uppfyller de tekniska kraven och protokollen i den distribuerade liggaren.

Artikel 2

Organisatoriska kontinuitetsarrangemang

1. Den kontinuitetspolicy som avses i artikel 68.7 i förordning (EU) 2023/1114 ska omfatta planer, förfaranden och åtgärder.

2. Kryptotillgångstjänsteleverantörernas ledningsorgan ska, vid fullgörandet av de uppgifter som avses i artikel 68.6 i förordning (EU) 2023/1114, fastställa och godkänna de planer, förfaranden och åtgärder som ingår i kontinuitetsplanen. Kryptotillgångstjänsteleverantörernas ledningsorgan ska ansvara för genomförandet av kontinuitetspolicyn och för att se över dess effektivitet minst en gång om året.

3. Leverantörerna av kryptotillgångstjänster ska säkerställa att varje ändring av kontinuitetspolicyn överförs till all relevant intern personal via effektiva kommunikationskanaler.

([4]) 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).

Artikel 3

Kontinuitetspolicy

1. Den kontinuitetspolicy som avses i artikel 68.7 i förordning (EU) 2023/1114 ska säkerställa att leverantörerna av kryptotillgångstjänster på ett korrekt sätt hanterar störande incidenter eller prestandaproblem som rör de system som är kritiska för driften av deras affärsfunktioner, och den ska lagras på ett varaktigt medium.

2. Leverantörerna av kryptotillgångstjänster ska i kontinuitetspolicyn ta med allt av följande:

a) En specificering av kontinuitetspolicyns omfattning, inbegripet dess begränsningar och undantag, som ska omfattas av kontinuitetsplanerna, kontinuitetsförfarandena och kontinuitetsåtgärderna.

b) En beskrivning av kriterierna för att aktivera kontinuitetsplanerna, inbegripet eskaleringsförfaranden upp till ledningsorganets nivå.

c) Bestämmelser om kryptotillgångstjänsteleverantörens styrning och organisation, inbegripet personalens roller och ansvarsområden, för att säkerställa att det finns tillräckliga resurser för att ett effektivt genomförande av policyn.

d) Bestämmelser som säkerställer överensstämmelse mellan kontinuitetsplanerna och IKT-kontinuitetsplanerna och de åtgärds- och återställningsplaner avseende IKT som avses i artiklarna 24 och 26 i delegerad förordning (EU) 2024/1774.

Artikel 4

Kontinuitetsplaner

1. Vid genomförandet av den kontinuitetspolicy som avses i artikel 68.7 i förordning (EU) 2023/1114 ska leverantörerna av kryptotillgångstjänster upprätta kontinuitetsplaner. Kontinuitetsplanerna ska ange de förfaranden som är nödvändiga för att skydda och, vid behov, återupprätta

a) Kunduppgifternas konfidentialitet, integritet och tillgänglighet,

b) Tillgängligheten hos kryptotillgångstjänsteleverantörers affärsfunktioner, stödprocesser och informationstillgångar.

2. Kontinuitetsplanerna ska innehålla följande:

a) Ett antal möjliga negativa scenarier som rör driften av kritiska eller viktiga funktioner, t.ex. att affärsfunktioner, personal, arbetsutrymmen, externa leverantörer eller datacentraler blir otillgängliga eller att kritiska data och dokument går förlorade eller ändras.

b) De förfaranden och riktlinjer som ska följas vid en störande incident, inbegripet

   i) de åtgärder som är nödvändiga för att återställa kritiska eller viktiga funktioner,

   ii) de tidsfrister inom vilka dessa kritiska eller viktiga funktioner ska återställas,

   iii) målen för återställningspunkten,

   iv) längsta tid för att återuppta tjänsterna,

c) förfaranden och policyer för att flytta de affärsfunktioner som används för att tillhandahålla kryptotillgångstjänster till en backup-enhet,

d) säkerhetskopiering av kritiska affärsuppgifter, inbegripet aktuell information om de kontakter som krävs för att säkerställa kommunikation inom leverantören av kryptotillgångstjänster, och mellan leverantören av kryptotillgångstjänster och dess kunder,

e) förfaranden för snabb kommunikation med kunder och andra externa intressenter, inbegripet behöriga myndigheter.

3. I händelse av en störning som inbegriper en tillståndsfri distribuerad liggare som leverantören av kryptotillgångstjänster använder när den tillhandahåller sina tjänster ska den kommunikation som avses i punkt 2 e innehålla följande information:

a) När tjänsterna förväntas återupptas.

b) Orsakerna till och inverkan av den störande incidenten.

c) Alla risker avseende kunders medel och kryptotillgångar som innehas för deras räkning.

d) Åtgärder som kryptotillgångstjänsten avser att vidta som svar på en störning av en tillståndslös distribuerad liggare.

Om denna information inte är lätt tillgänglig för leverantören av kryptotillgångstjänster, ska leverantören av kryptotillgångstjänster efter bästa förmåga meddela uppdateringar av informationen i första stycket till kunder och intressenter, inbegripet behöriga myndigheter.

4. Kontinuitetsplanerna ska innehålla förfaranden för hantering av störningar av utkontrakterade kritiska eller viktiga funktioner, inbegripet när dessa kritiska eller viktiga funktioner blir otillgängliga.

Artikel 5

Periodisk testning av kontinuitetsplanerna

1. Leverantörerna av kryptotillgångstjänster ska på grundval av realistiska scenarier testa driften av de kontinuitetsplaner som avses i artikel 4. Sådan testning ska verifiera förmågan hos leverantören av kryptotillgångstjänster att återhämta sig från störande incidenter och återuppta tjänsterna i enlighet med artikel 4.2 b.

2. Leverantörerna av kryptotillgångstjänster ska årligen testa kontinuitetsplanerna med beaktande av följande:

a) Resultaten av de tester som avses i punkt 1.

b) Den senaste hotunderrättelsen.

c) Lärdomar från tidigare händelser.

d) I förekommande fall, eventuella ändringar av återställningsmålen, inbegripet målen om återställningstid och målen för återhämtningspunkten enligt artikel 4.2 b.

e) Förändringar i affärsfunktionerna.

3. Leverantörerna av kryptotillgångstjänster ska dokumentera resultaten av testningen skriftligen och lämna in dem till sitt ledningsorgan och till de operativa enheter som deltar i kontinuitetsplanerna.

4. Leverantörerna av kryptotillgångstjänster ska säkerställa att testningen av kontinuitetsplanerna inte stör det normala utförandet av deras tjänster.

Artikel 6

Komplexitet och riskövervägande

1. Vid fastställandet av kontinuitetspolicyn, inbegripet planerna, förfarandena och åtgärderna, ska leverantörerna av kryptotillgångstjänster ta hänsyn till delar av ökad komplexitet eller ökad risk, inbegripet följande:

a) Typen och urvalet av kryptotillgångstjänster som erbjuds.

b) I vilken utsträckning kryptotillgångstjänsteleverantörernas tjänster är beroende av tillståndslösa distribuerade liggare.

c) Den potentiella inverkan av eventuella störningar på kontinuiteten i leverantörens verksamhet och tillgången till dess tjänster.

2. Vid tillämpning av punkt 1 ska leverantörerna av kryptotillgångstjänster årligen göra en självbedömning av omfattningen, arten och urvalet av sina tjänster. Leverantörerna av kryptotillgångstjänster ska basera den självbedömningen på de kriterier som anges i bilagan och alla andra kriterier som leverantören av kryptotillgångstjänster anser vara relevanta.

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 31 oktober 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA

KRITERIER FÖR KRYPTOTILLGÅNGSTJÄNSTELEVERANTÖRERS SJÄLVBEDÖMNING

a) Arten av leverantör av kryptotillgångstjänster, på grundval av följande element:

   i) Den klass-benämning som anges i bilaga IV till förordning (EU) 2023/1114.

   ii) Den genomsnittliga likviditetsnivån, eller marknadsdjupet, hos de kryptotillgångar som är tillgängliga för handel på en handelsplattform för kryptotillgångar, i förekommande fall.

   iii) Vilken roll leverantören av kryptotillgångstjänster har i det finansiella systemet, inbegripet om den driver en handelsplattform för kryptotillgångar och om de kryptotillgångar som handlas på dennas plattform handlas på andra plattformar för kryptotillgångar.

b) Omfattningen, genom att bedöma vilken inverkan leverantören av kryptotillgångstjänster har på marknadens korrekta funktion på grundval av följande element, i förekommande fall:

   i) Huruvida leverantör av kryptotillgångstjänster klassificeras som ”betydande” i enlighet med artikel 85 i förordning (EU) 2023/1114.

   ii) Antal länder i vilka leverantören av kryptotillgångstjänster bedriver verksamhet.

   iii) Antal kunder.

   iv) Antal aktiva användare.

   v) Värdet på de kryptotillgångar som förvaras.

   vi) Volymen av transaktioner på en handelsplattform för kryptotillgångar.

   vii) Antal överföringar av kryptotillgångar för kunders räkning,

   viii) Antal ordrar som utförs för kunders räkning,

c) Komplexiteten, genom att bedöma följande element, i förekommande fall:

   i) Kryptotillgångstjänsteleverantörens struktur i fråga om ägande och styrning, och dess organisatoriska, driftmässiga, tekniska, fysiska och geografiska närvaro.

   ii) Omfattningen hos kryptotillgångstjänsteleverantörens utkontraktering, och särskilt huruvida kritiska eller viktiga driftsmässiga funktioner har utkontrakterats.

   iii) Antal och typ av distribuerade liggare som används vid utförandet av tjänsterna.

   iv) Antal DLT-nätnoder som leverantören av kryptotillgångstjänster driver i en eller flera distribuerade liggare.

   v) Antal och typ av smarta kontrakt som ingås och upprätthålls av leverantören av kryptotillgångstjänster.

   vi) Hur kundernas privata krypteringsnycklar och andra medel för åtkomst kryptotillgångar säkras under förvaring.

   vii) Användning av mjuk- och hårdvarubaserade depåbaserade plånböcker eller plånböcker som säkrar krypteringsnycklar genom användning av flera förvaltare.

Vid tillämpningen av punkterna b iii–viii ska leverantörerna av kryptotillgångstjänster för självbedömningen använda det dagliga genomsnittet under en ett-årig referensperiod.