2025/303

20.2.2025

NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2025/303

ze dne 31. října 2024,

kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2023/1114, pokud jde o regulační technické normy upřesňující informace, které mají některé finanční subjekty uvádět v oznámení o svém záměru poskytovat služby související s kryptoaktivy

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937 ([1]), a zejména na čl. 60 odst. 13 třetí pododstavec uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Aby mohly příslušné orgány posoudit, zda určité finanční subjekty, které mají v úmyslu poskytovat služby související s kryptoaktivy, splňují příslušné požadavky stanovené v hlavě V a v příslušných případech v hlavě VI nařízení (EU) 2023/1114, měly by být informace, které mají určité finanční subjekty oznamovat o svém záměru poskytovat služby související s kryptoaktivy, dostatečně podrobné a vyčerpávající, aniž by představovaly nepřiměřenou zátěž.

(2) V souladu s čl. 60 odst. 7 písm. a) nařízení (EU) 2023/1114 musí oznámení o záměru poskytovat služby související s kryptoaktivy obsahovat program činností. Aby bylo možné poskytnout úplný obraz o činnostech, které má oznamující subjekt v úmyslu vykonávat, měl by program činností zahrnovat popis organizační struktury oznamujícího subjektu, jeho strategii při poskytování služeb souvisejících s kryptoaktivy cílovým zákazníkům a jeho provozní kapacitu na tři roky od data oznámení. Pokud jde o strategii používanou k oslovení zákazníků, oznamující subjekt by měl popsat marketingové prostředky, které má v úmyslu použít, jako jsou internetové stránky, aplikace pro mobilní telefony, osobní setkání, tiskové zprávy nebo jakákoli forma fyzických či elektronických prostředků, včetně nástrojů kampaně v sociálních médiích, internetové reklamy nebo bannerů, znovuzacílení reklamy (retargetingu), smluv s vlivnými osobami (tzv. influencery), sponzorských smluv, telefonních hovorů, webinářů, pozvánek na akce, afilačních kampaní, technik gamifikace, výzev k vyplnění odpovědního formuláře nebo k absolvování školení, demo účtů nebo vzdělávacích materiálů.

(3) Aby mohly příslušné orgány posoudit odolnost oznamujícího subjektu vůči vnějším finančním otřesům, včetně otřesů spojených s hodnotou kryptoaktiv, měl by oznamující subjekt do svého oznámení zahrnout zátěžové scénáře simulující závažné, avšak věrohodné události v rámci svého předpokládaného účetního plánu.

(4) Aby se předešlo výpadkům provozu, které mohou mít pro oznamující subjekt a obecněji pro trhy kryptoaktiv závažné finanční a regulační důsledky a důsledky pro pověst, je zásadní zachovat provoz nebo alespoň základní funkce poskytovatelů služeb souvisejících s kryptoaktivy a minimalizovat prostoje v důsledku neočekávaných narušení, včetně kybernetických útoků a přírodních katastrof. Oznámení by proto mělo obsahovat podrobné informace o opatřeních oznamujícího subjektu k zajištění kontinuity a řádného poskytování služeb souvisejících s kryptoaktivy, včetně podrobného popisu jeho rizik a plánů zachování kontinuity činností.

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

(5) Aby bylo zajištěno, že oznamující subjekty při poskytování služeb souvisejících s kryptoaktivy náležitě přistupují k rizikům a praktikám týkajícím se praní peněz a financování terorismu, jsou zapotřebí účinné mechanismy, systémy a postupy, které jsou v souladu se směrnicí Evropského parlamentu a Rady (EU) 2015/849 ([2]). Oznamující subjekty by proto měly ve svém oznámení poskytnout podrobné informace o svých mechanismech, systémech a postupech zavedených za účelem předcházení rizikům spojeným s jejich podnikatelskou činností mimo jiné v souvislosti s bojem proti praní peněz a financování terorismu.

(6) Vzhledem k decentralizované a digitální povaze kryptoaktiv jsou kybernetická bezpečnostní rizika pro poskytovatele služeb souvisejících s kryptoaktivy značná a mají mnoho podob. Aby bylo zajištěno, že oznamující subjekt je schopen předcházet narušení bezpečnosti údajů a finančním ztrátám, které by mohly být způsobeny kybernetickými útoky, měly by informace o nasazených systémech IKT oznamujícího subjektu a souvisejících bezpečnostních opatřeních, jako je totožnost a zeměpisná poloha poskytovatelů, popis externě zadávaných činností nebo služeb IKT s jejich hlavními charakteristikami, kopie smluvních ujednání, jak je uvedeno v čl. 60 odst. 7 písm. c) nařízení (EU) 2023/1114, zahrnovat lidské zdroje určené k řešení kybernetických bezpečnostních rizik.

(7) Oddělení kryptoaktiv a peněžních prostředků zákazníků chrání zákazníky před ztrátami poskytovatele služeb souvisejících s kryptoaktivy a před zneužitím jejich kryptoaktiv a peněžních prostředků. Článek 70 nařízení (EU) 2023/1114 proto vyžaduje, aby poskytovatelé služeb souvisejících s kryptoaktivy přijali odpovídající opatření k ochraně vlastnických práv zákazníků. Tento požadavek se vztahuje i na poskytovatele služeb souvisejících s kryptoaktivy, kteří neposkytují služby úschovy a správy.

(8) Aby mohly příslušné orgány posoudit přiměřenost provozních pravidel oznamujícího subjektu pro jeho obchodní platformy pro kryptoaktiva, měl by oznamující subjekt v popisu těchto pravidel specifikovat určité prvky. Oznamující subjekt by měl zejména rozvést aspekty provozních pravidel týkající se přijímání kryptoaktiv k obchodování, obchodování s nimi a jejich vypořádání. Pokud jde o přijímání kryptoaktiv k obchodování, oznamující subjekty by měly poskytnout podrobné informace o tom, jak přijatá kryptoaktiva splňují pravidla oznamujícího subjektu, o druzích kryptoaktiv, které oznamující subjekt nepřijme k obchodování na své obchodní platformě, a o důvodech jejich vyloučení a o poplatcích za přijetí k obchodování. Pokud jde o obchodování s kryptoaktivy, oznamující subjekt by měl specifikovat ustanovení provozních pravidel, která upravují provádění a rušení pokynů, řádné obchodování, transparentnost a vedení záznamů. V neposlední řadě by oznamující subjekt měl do popisu provozních pravidel zahrnout ustanovení, jimiž se řídí vypořádání transakcí s kryptoaktivy na obchodní platformě, včetně upřesnění, zda je vypořádání iniciováno s využitím technologie distribuovaného registru (DLT), časového rámce, v němž je provedení iniciováno, vymezení okamžiku, kdy je vypořádání konečné, všech ověření nutných k zajištění účinného vypořádání transakce a veškerých opatření k omezení selhání vypořádání.

(9) Aby mohly příslušné orgány posoudit přiměřenost oznamujícího subjektu při poskytování určitých služeb souvisejících s kryptoaktivy, jako je směna kryptoaktiv za peněžní prostředky nebo za jiná kryptoaktiva, provádění pokynů, poskytování poradenství týkajícího se kryptoaktiv nebo správa portfolia kryptoaktiv a služby převodu, měl by oznamující subjekt uvést podrobnosti o tom, jak budou tyto služby související s kryptoaktivy poskytovány, jakož i opatření zavedená k zajištění toho, aby oznamující subjekt dodržoval příslušná ustanovení nařízení (EU) 2023/1114, pokud jde o poskytování těchto služeb souvisejících s kryptoaktivy.

(10) Veškeré zpracování osobních údajů podle tohoto nařízení musí být v souladu s požadavky nařízení Evropského parlamentu a Rady (EU) 2016/679 ([3]).

([2]) Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES (Úř. věst. L 141, 5.6.2015, s. 73, ELI: http://data.europa.eu/eli/dir/2015/849/oj).

([3]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(11) Toto nařízení vychází z návrhů regulačních technických norem předložených Komisi Evropským orgánem pro cenné papíry a trhy (ESMA) a vypracovaných v úzké spolupráci s Evropským orgánem pro bankovnictví.

(12) Orgán ESMA uskutečnil k návrhům regulačních technických norem, z nichž toto nařízení vychází, otevřené veřejné konzultace, analyzoval potenciální související náklady a přínosy a požádal o stanovisko skupinu subjektů působících v oblasti cenných papírů a trhů zřízenou podle článku 37 nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ([4]).

(13) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([5]) byl konzultován evropský inspektor ochrany údajů, který sdělil formální připomínky dne 21. června 2024,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Program činností

1. Pro účely čl. 60 odst. 7 písm. a) nařízení (EU) 2023/1114 oznamující subjekt poskytne příslušnému orgánu program činností na tři roky následující po datu oznámení, včetně následujících informací:

a) v případě, že oznamující subjekt patří do skupiny ve smyslu čl. 2 bodu 11 směrnice Evropského parlamentu a Rady 2013/34/EU ([6]), vysvětlení, jak činnosti oznamujícího subjektu zapadají do strategie této skupiny a jak se vzájemně ovlivňují s činnostmi ostatních subjektů této skupiny, včetně přehledu současné a plánované organizace a struktury této skupiny;

b) vysvětlení, jak se očekává, že činnost subjektů ve skupině, včetně případů, kdy jsou ve skupině regulované subjekty, ovlivní činnost oznamujícího subjektu, včetně seznamu subjektů ve skupině a informací o těchto subjektech, včetně regulovaných subjektů, služeb poskytovaných těmito subjekty a jmen domén všech internetových stránek provozovaných těmito subjekty;

c) seznamu služeb souvisejících s kryptoaktivy, které má oznamující subjekt v úmyslu poskytovat, a druhů kryptoaktiv, kterých se tyto služby budou týkat;

d) dalších plánovaných činností, regulovaných v souladu s právem Unie nebo vnitrostátním právem nebo neregulovaných, včetně jakýchkoli jiných služeb, než jsou služby související s kryptoaktivy, které má oznamující subjekt v úmyslu poskytovat;

e) zda má oznamující subjekt v úmyslu veřejně nabízet kryptoaktiva nebo zda usiluje o přijetí kryptoaktiv k obchodování, a pokud ano, o jaký druh kryptoaktiv se jedná;

f) seznamu jurisdikcí v Unii i ve třetích zemích, v nichž oznamující subjekt plánuje poskytovat služby související s kryptoaktivy, včetně informací o cílovém počtu zákazníků podle zeměpisných oblastí;

g) typů potenciálních zákazníků, na které se služby související s kryptoaktivy poskytované oznamujícím subjektem zaměřují;

([4]) Nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro cenné papíry a trhy), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/77/ES (Úř. věst. L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([5]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([6]) Směrnice Evropského parlamentu a Rady 2013/34/EU ze dne 26. června 2013 o ročních účetních závěrkách, konsolidovaných účetních závěrkách a souvisejících zprávách některých forem podniků, o změně směrnice Evropského parlamentu a Rady 2006/43/ES a o zrušení směrnic Rady 78/660/EHS a 83/349/EHS (Úř. věst. L 182, 29.6.2013, s. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

h) popisu způsobu přístupu zákazníků ke službám souvisejícím s kryptoaktivy poskytovaným oznamujícím subjektem, včetně všech následujících údajů:

i) jmen domén všech internetových stránek nebo jiných aplikací založených na IKT, jejichž prostřednictvím bude oznamující subjekt poskytovat služby související s kryptoaktivy, a informací o jazycích, v nichž budou tyto internetové stránky nebo jiné aplikace založené na IKT dostupné, o druzích služeb souvisejících s kryptoaktivy, které budou prostřednictvím těchto internetových stránek nebo jiných aplikací založených na IKT přístupné, a v příslušných případech o tom, ze kterých členských států budou tyto internetové stránky nebo jiné aplikace založené na IKT přístupné;

ii) názvu jakékoli aplikace založené na IKT, která je zákazníkům k dispozici pro přístup ke službám souvisejícím s kryptoaktivy, jazyků, v nichž je tato aplikace založená na IKT dostupná, a služeb souvisejících s kryptoaktivy, které jsou prostřednictvím této aplikace založené na IKT dostupné;

i) plánovaných marketingových a propagačních aktivit a opatření pro poskytování služeb souvisejících s kryptoaktivy, včetně:

i) všech marketingových prostředků, které budou u jednotlivých služeb využívány;

ii) zamýšleného způsobu identifikace oznamujícího subjektu;

iii) informací o příslušné kategorii cílových zákazníků;

iv) druhů kryptoaktiv;

v) jazyků, které budou používány pro marketingové a propagační aktivity;

j) podrobného popisu lidských a finančních zdrojů a prostředků IKT přidělených na plánované služby související s kryptoaktivy a jejich zeměpisného umístění;

k) zásad oznamujícího subjektu v oblasti externího zajištění funkcí, služeb nebo činností a způsobu, jakým byly přizpůsobeny službám souvisejícím s kryptoaktivy, jakož i podrobného popisu plánovaných opatření oznamujícího subjektu v oblasti externího zajištění funkcí, služeb nebo činností, včetně opatření uvnitř skupiny, a způsobu, jakým oznamující subjekt zajistí dodržení ustanovení článku 73 nařízení (EU) 2023/1114, včetně informací o funkci nebo osobě odpovědné za externí zajištění funkcí, služeb nebo činností, lidských zdrojích a prostředcích IKT přidělených na kontrolu externě zajišťovaných funkcí, služeb nebo činností či souvisejících opatření a o posouzení rizik souvisejících s externím zajištěním funkcí služeb nebo činností;

l) seznamu subjektů, které budou poskytovat externě zajišťované služby pro poskytování služeb souvisejících s kryptoaktivy, jejich zeměpisného umístění a příslušných externě zajišťovaných služeb;

m) předpokládaného účetního plánu včetně zátěžových scénářů na individuální a v příslušných případech konsolidované skupinové a subkonsolidované úrovni v souladu se směrnicí 2013/34/EU, přičemž se zohlední i veškeré vnitroskupinové úvěry, které byly nebo mají být poskytnuty oznamujícím subjektem a oznamujícímu subjektu;

n) jakékoli směny kryptoaktiv za peněžní prostředky a dalších činností souvisejících s kryptoaktivy, které má oznamující subjekt v úmyslu provádět, a to i prostřednictvím decentralizovaných finančních aplikací, s nimiž hodlá být oznamující subjekt v interakci na vlastní účet.

2. Pokud má oznamující subjekt v úmyslu poskytovat službu přijímání a předávání pokynů ke kryptoaktivům jménem zákazníků, poskytne příslušnému orgánu kopii postupů a popis opatření zajišťujících soulad s článkem 80 nařízení (EU) 2023/1114.

3. Pokud má oznamující subjekt v úmyslu poskytovat službu umisťování kryptoaktiv, předloží příslušnému orgánu kopii postupů pro identifikaci, prevenci a řízení střetů zájmů a informování o nich a popis opatření zavedených za účelem dosažení souladu s článkem 79 nařízení (EU) 2023/1114 a s nařízením Komise v přenesené pravomoci, kterým se stanoví technické normy přijaté podle čl. 72 odst. 5 nařízení (EU) 2023/1114.

Článek 2

Plán zachování kontinuity činností

1. Pro účely čl. 60 odst. 7 písm. b) bodu iii) nařízení (EU) 2023/1114 oznamující subjekt předloží příslušnému orgánu podrobný popis svého plánu zachování kontinuity činností, včetně opatření, která mají být přijata k zajištění kontinuity a řádného poskytování jeho služeb souvisejících s kryptoaktivy.

2. Popis uvedený v odstavci 1 musí zahrnovat:

a) podrobnosti prokazující, že zavedený plán zachování kontinuity činností je odpovídající a že jsou zavedena opatření k udržování a pravidelnému testování tohoto plánu;

b) u zásadních nebo důležitých funkcí podporovaných poskytovateli služeb, kteří jsou třetími stranami, podrobnosti o tom, jak je zajištěna kontinuita činností v případě, že se kvalita poskytování těchto funkcí zhorší na nepřijatelnou úroveň nebo jí nebude dosaženo;

c) informace o tom, jak je zajištěna kontinuita činností v případě úmrtí klíčové osoby, a případně o politických rizicích v jurisdikcích poskytovatele služeb.

Článek 3

Odhalování a prevence praní peněz a financování terorismu

Pro účely čl. 60 odst. 7 písm. b) bodů i) a ii) nařízení (EU) 2023/1114 oznamující subjekt poskytne příslušnému orgánu informace o svých mechanismech vnitřní kontroly, zásadách a postupech k zajištění souladu s ustanoveními vnitrostátních právních předpisů, kterými se provádí směrnice (EU) 2015/849, a o rámci pro posuzování rizik s cílem řídit rizika související s praním peněz a financováním terorismu, včetně následujících informací:

a) posouzení inherentních a zbytkových rizik praní peněz a financování terorismu spojených s poskytováním služeb souvisejících s kryptoaktivy oznamujícím subjektem, včetně rizik souvisejících s:

   i) okruhem zákazníků oznamujícího subjektu;

   ii) poskytovanými službami;

   iii) používanými distribučními kanály;

   iv) zeměpisnými oblastmi působnosti;

b) opatření, která oznamující subjekt zavedl nebo zavede k předcházení zjištěným rizikům a k dodržování platných požadavků proti praní peněz a financování terorismu, včetně procesu posuzování rizik oznamujícího subjektu, zásad a postupů k zajištění dodržování požadavků na hloubkovou kontrolu zákazníka a zásad a postupů pro odhalování a hlášení podezřelých transakcí nebo činností;

c) podrobných informací o tom, jak jsou mechanismy vnitřní kontroly, zásady a postupy přiměřené a úměrné rozsahu, povaze a inherentnímu riziku praní peněz a financování terorismu, včetně rozsahu poskytovaných služeb souvisejících s kryptoaktivy, složitosti obchodního modelu a způsobu, jakým oznamující subjekt zajišťuje soulad se směrnicí Evropského parlamentu a Rady (EU) 2015/849 a nařízením Evropského parlamentu a Rady (EU) 2023/1113 ([7]);

d) totožnosti osoby odpovědné za zajištění souladu oznamujícího subjektu s požadavky na boj proti praní peněz a financování terorismu, včetně důkazů o dovednostech a odbornosti této osoby;

e) opatření, lidských a finančních zdrojů vynaložených na základě ročních údajů k zajištění toho, aby byli pracovníci oznamujícího subjektu náležitě vyškoleni v otázkách boje proti praní peněz a financování terorismu a v oblasti specifických rizik souvisejících s kryptoaktivy;

([7]) Nařízení Evropského parlamentu a Rady (EU) 2023/1113 ze dne 31. května 2023 o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv a o změně směrnice (EU) 2015/849 (Úř. věst. L 150, 9.6.2023, s. 1, ELI: http://data.europa.eu/eli/reg/2023/1113/oj).

f) kopie zásad, postupů a systémů oznamujícího subjektu pro boj proti praní peněz a terorismu;

g) souhrnného dokumentu popisujícího změny, které byly provedeny v postupech a systémech oznamujícího subjektu v oblasti boje proti praní peněz a terorismu v důsledku plánovaných služeb souvisejících s kryptoaktivy;

h) četnosti hodnocení přiměřenosti a účinnosti mechanismů, systémů a postupů vnitřní kontroly, včetně identifikace osoby nebo funkce odpovědné za toto hodnocení.

Článek 4

Systémy IKT a související bezpečnostní opatření

Pro účely čl. 60 odst. 7 písm. c) nařízení (EU) 2023/1114 oznamující subjekt poskytne příslušnému orgánu tyto informace:

a) technickou dokumentaci systémů IKT, případně infrastruktury DLT, na které se spoléhá, a bezpečnostní opatření, včetně popisu opatření a nasazených prostředků IKT a lidských zdrojů zavedených za účelem dosažení souladu s nařízením Evropského parlamentu a Rady (EU) 2022/2554 ([8]) včetně následujících informací:

   i) popisu toho, jak oznamující subjekt zajišťuje řádný, komplexní a dobře zdokumentovaný rámec řízení rizik v oblasti IKT jako součást svého celkového systému řízení rizik, včetně podrobného popisu systémů, protokolů a nástrojů IKT a toho, jak postupy, zásady a systémy oznamujícího subjektu zajistí bezpečnost, integritu, dostupnost, hodnověrnost a důvěrnost údajů v souladu s nařízeními (EU) 2022/2554 a (EU) 2016/679;

   ii) identifikace služeb IKT podporujících zásadní nebo důležité funkce, které oznamující subjekt vyvinul nebo udržuje, jakož i služeb poskytovaných poskytovateli služeb, kteří jsou třetími stranami, popisu těchto smluvních ujednání a způsobu, jakým jsou tato ujednání v souladu s článkem 73 nařízení (EU) 2023/1114 a kapitolou V nařízení (EU) 2022/2554;

   iii) popisu postupů, zásad, opatření a systémů oznamujícího subjektu pro řízení bezpečnosti a incidentů;

b) pokud je k dispozici, popis auditu kybernetické bezpečnosti provedeného auditorem kybernetické bezpečnosti, který je třetí stranou a má dostatečné zkušenosti v souladu s nařízením Komise v přenesené pravomoci, kterým se stanoví technické normy podle čl. 26 odst. 11 čtvrtého pododstavce nařízení (EU) 2022/2554, zahrnujícího v ideálním případě tyto audity nebo testy provedené externími nezávislými stranami:

   i) opatření v oblasti organizační kybernetické bezpečnosti, fyzické bezpečnosti a životního cyklu bezpečného vývoje softwaru;

   ii) posouzení zranitelnosti a posouzení zabezpečení sítě;

   iii) přezkumy konfigurace aktiv v oblasti IKT podporujících zásadní a důležité funkce, jak jsou definovány v čl. 3 bodě 22 nařízení (EU) 2022/2554;

   iv) penetrační testy aktiv v oblasti IKT podporujících zásadní a důležité funkce, jak jsou definovány v čl. 3 bodě 17 nařízení (EU) 2022/2554, v souladu se všemi následujícími přístupy k auditním testům:

      1) černou skříňkou: auditor nemá k dispozici žádné jiné informace než IP adresy a adresy URL spojené s auditovaným cílem. Této fázi zpravidla předchází zjišťování informací a identifikace cíle dotazováním na služby systému doménových jmen (DNS), skenováním otevřených portů, zjišťováním přítomnosti filtračních zařízení;

([8]) Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

2) fází šedé skříňky: auditoři mají znalosti standardního uživatele informačního systému (legitimní ověření, „standardní“ pracovní stanice). Identifikátory mohou patřit různým uživatelským profilům, aby bylo možné testovat různé úrovně oprávnění;

3) fází bílé skříňky: auditoři mají před zahájením analýzy co nejvíce technických informací (architektura, zdrojový kód, telefonní kontakty, identifikátory atd.) a také přístup k technickým kontaktům souvisejícím s cílem;

v) pokud oznamující subjekt používá a/nebo vyvíjí inteligentní smlouvy, přezkum jejich zdrojového kódu z hlediska kybernetické bezpečnosti;

c) popis případně provedených auditů systémů IKT, včetně použité infrastruktury DLT a bezpečnostních opatření;

d) popis příslušných informací uvedených v písmenech a) a b) v obecně srozumitelném jazyce.

Článek 5

Oddělení a úschova kryptoaktiv a peněžních prostředků zákazníků

1. Pro účely čl. 60 odst. 7 písm. d) nařízení (EU) 2023/1114 oznamující subjekt, který má v úmyslu držet kryptoaktiva patřící zákazníkům nebo prostředky přístupu k těmto kryptoaktivům nebo peněžní prostředky zákazníků jiné než elektronické peněžní tokeny, poskytne příslušnému orgánu podrobný popis svých postupů pro oddělení kryptoaktiv a peněžních prostředků zákazníků, včetně následujících informací:

a) jak oznamující subjekt zajistí následující:

i) aby peněžní prostředky zákazníků nepoužíval na svůj vlastní účet;

ii) aby kryptoaktiva patřící zákazníkům nepoužíval na svůj vlastní účet;

iii) aby byla kryptoaktiva zákazníků uložena v jiných peněženkách než v peněženkách patřících oznamujícímu subjektu;

b) podrobného popisu systému schvalování kryptografických klíčů a zabezpečení kryptografických klíčů včetně peněženek s více podpisy;

c) jak oznamující subjekt odděluje kryptoaktiva zákazníků, včetně jejich oddělení od kryptoaktiv jiných zákazníků, pokud jsou peněženky obsahující kryptoaktiva více než jednoho zákazníka vedeny na souhrnných účtech;

d) popisu postupu, který zajistí, aby peněžní prostředky zákazníků jiné než elektronické peněžní tokeny byly uloženy u centrální banky nebo u úvěrové instituce do konce pracovního dne následujícího po dni, kdy byly obdrženy, a aby byly vedeny na účtu samostatně identifikovatelném od jakýchkoli účtů používaných k uložení peněžních prostředků patřících oznamujícímu subjektu;

e) v případě, že oznamující subjekt nemá v úmyslu ukládat peněžní prostředky u příslušné centrální banky, jaké faktory oznamující subjekt zohledňuje při výběru úvěrových institucí, u nichž ukládá peněžní prostředky zákazníků, včetně zásad diverzifikace oznamujícího subjektu, jsou-li k dispozici, a četnosti přezkumu výběru úvěrových institucí, u nichž ukládá peněžní prostředky zákazníků;

f) jak oznamující subjekt zajistí, aby byli zákazníci jasně, stručně a v obecně srozumitelném jazyce informováni o klíčových aspektech systémů, zásad a postupů oznamujícího subjektu, aby byl dodržen čl. 70 odst. 1, 2 a 3 nařízení (EU) 2023/1114.

2. V souladu s čl. 70 odst. 5 nařízení (EU) 2023/1114 poskytují poskytovatelé služeb souvisejících s kryptoaktivy, kteří jsou institucemi elektronických peněz nebo úvěrovými institucemi, pouze informace uvedené v odstavci 1 tohoto článku.

Článek 6

Zásady úschovy a správy

Pro účely čl. 60 odst. 7 písm. e) nařízení (EU) 2023/1114 oznamující subjekt poskytne příslušnému orgánu tyto informace:

a) popis opatření souvisejících s typem úschovy nabízené zákazníkům, kopii standardní smlouvy oznamujícího subjektu o úschově a správě kryptoaktiv jménem zákazníků podle čl. 75 odst. 1 nařízení (EU) 2023/1114 a kopii shrnutí zásad úschovy zpřístupněného zákazníkům v souladu s čl. 75 odst. 3 třetím pododstavcem uvedeného nařízení;

b) zásady úschovy a správy oznamujícího subjektu, včetně popisu identifikovaných zdrojů provozních rizik a rizik v oblasti IKT pro úschovu a kontrolu kryptoaktiv nebo prostředků přístupu ke kryptoaktivům zákazníků, spolu s následujícími informacemi:

   i) zásadami a postupy a popisem opatření pro dosažení souladu s čl. 75 odst. 8 nařízení (EU) 2023/1114;

   ii) zásadami a postupy a popisem systémů a kontrolních mechanismů pro řízení provozních rizik a rizik v oblasti IKT, včetně případů, kdy je úschova a správa kryptoaktiv jménem zákazníků svěřena třetí straně;

   iii) zásadami a postupy týkajícími se systémů pro zajištění výkonu práv spojených s kryptoaktivy ze strany zákazníků a jejich popis;

   iv) zásadami a postupy týkajícími se systémů zajišťujících vrácení kryptoaktiv nebo prostředků přístupu zákazníkům a jejich popis;

c) informace o způsobu identifikace kryptoaktiv a způsobu přístupu ke kryptoaktivům zákazníků;

d) informace o opatřeních k minimalizaci rizika ztráty kryptoaktiv nebo prostředků přístupu ke kryptoaktivům;

e) pokud poskytovatel služeb souvisejících s kryptoaktivy pověřil úschovou a správou kryptoaktiv jménem zákazníků třetí stranu:

   i) informace o totožnosti třetí strany poskytující službu úschovy a správy kryptoaktiv a o jejím statusu v souladu s článkem 59 nebo článkem 60 nařízení (EU) 2023/1114;

   ii) popis všech funkcí souvisejících s úschovou a správou kryptoaktiv, jejichž výkonem poskytovatel služeb souvisejících s kryptoaktivy pověřil jiné osoby, případně seznam všech pověřených a dále pověřených osob a případný střet zájmů, který by z takového pověření mohl vyplynout;

   iii) popis způsobu, jakým má oznamující subjekt v úmyslu dohlížet na tato pověření nebo další pověření.

Článek 7

Provozní pravidla obchodní platformy a odhalování zneužití trhu

1. Pro účely čl. 60 odst. 7 písm. f) nařízení (EU) 2023/1114 oznamující subjekt, který má v úmyslu provozovat obchodní platformu pro kryptoaktiva, poskytne příslušnému orgánu tyto informace:

a) pravidla pro přijímání kryptoaktiv k obchodování;

b) schvalovací proces pro přijetí kryptoaktiv k obchodování, včetně hloubkové kontroly zákazníka prováděné v souladu se směrnicí (EU) 2015/849;

c) seznam všech kategorií kryptoaktiv, která nebudou přijata k obchodování, a důvody jejich vyloučení;

d) zásady, postupy a poplatky týkající se přijetí k obchodování, případně spolu s popisem členství, slev a souvisejících podmínek;

e) pravidla pro provádění pokynů, včetně postupů pro zrušení provedených pokynů a pro sdělování těchto informací účastníkům trhu;

f) metody zavedené k posouzení vhodnosti kryptoaktiv v souladu s čl. 76 odst. 2 nařízení (EU) 2023/1114;

g) systémy, postupy a opatření zavedené za účelem dosažení souladu s čl. 76 odst. 7 nařízení (EU) 2023/1114;

h) způsob uveřejnění všech kupních a prodejních cen, intenzitu obchodních zájmů na uvedených cenách, které jsou pro kryptoaktiva sdělovány prostřednictvím jejich obchodní platformy, a cenu, objem a čas transakcí provedených v souvislosti s kryptoaktivy obchodovanými na jejich obchodní platformě v souladu s čl. 76 odst. 9 a 10 nařízení (EU) 2023/1114;

i) struktury poplatků a odůvodnění, jak jsou tyto struktury v souladu s čl. 76 odst. 13 nařízení (EU) 2023/1114;

j) systémy, postupy a opatření zavedené za účelem uchovávání údajů ohledně všech pokynů pro potřebu příslušného orgánu, nebo mechanismus, který zajistí, aby měl příslušný orgán přístup k evidenci pokynů a jakémukoli jinému obchodnímu systému;

k) pokud jde o vypořádání transakcí:

   i) zda je konečné vypořádání transakcí iniciováno v distribuovaném registru nebo mimo něj;

   ii) časový rámec, v němž je iniciováno konečné vypořádání transakcí s kryptoaktivy;

   iii) způsob ověření dostupnosti peněžních prostředků a kryptoaktiv;

   iv) způsob potvrzení příslušných údajů o transakcích;

   v) předpokládaná opatření k omezení selhání vypořádání;

   vi) okamžik, kdy je vypořádání konečné, a okamžik, kdy je iniciováno konečné vypořádání po provedení transakce.

l) postupy a systémy zavedené za účelem odhalování a předcházení zneužívání trhu, včetně informací o sdělování možných případů zneužívání trhu příslušnému orgánu.

2. Oznamující subjekty, které mají v úmyslu provozovat obchodní platformu pro kryptoaktiva, poskytnou příslušnému orgánu kopii provozních pravidel obchodní platformy a veškerých postupů pro odhalování a předcházení zneužívání trhu.

Článek 8

Směna kryptoaktiv za peněžní prostředky nebo jiná kryptoaktiva

Pro účely čl. 60 odst. 7 písm. g) nařízení (EU) 2023/1114 oznamující subjekt, který má v úmyslu směňovat kryptoaktiva za peněžní prostředky nebo za jiná kryptoaktiva, poskytne příslušnému orgánu tyto informace:

a) popis obchodní politiky stanovené v souladu s čl. 77 odst. 1 nařízení (EU) 2023/1114;

b) metodiku pro stanovení ceny kryptoaktiv, která oznamující subjekt navrhuje ke směně za peněžní prostředky nebo za jiná kryptoaktiva v souladu s čl. 77 odst. 2 nařízení (EU) 2023/1114, včetně toho, jak objem kryptoaktiv a volatilita trhů kryptoaktiv ovlivňují mechanismus stanovení ceny.

Článek 9

Zásady provádění pokynů

Pro účely čl. 60 odst. 7 písm. h) nařízení (EU) 2023/1114 oznamující subjekt, který má v úmyslu provádět pokyny ke kryptoaktivům jménem zákazníků, poskytne příslušnému orgánu své zásady provádění pokynů, včetně následujících informací:

a) ujednání, která zajišťují, že zákazník před provedením pokynu udělil souhlas se zásadami provádění pokynů;

b) seznamu obchodních platforem pro kryptoaktiva, na které se oznamující subjekt bude spoléhat při provádění pokynů, a kritérií pro posuzování míst provádění pokynů zahrnutých do zásad provádění pokynů v souladu s čl. 78 odst. 6 nařízení (EU) 2023/1114;

c) které obchodní platformy má oznamující subjekt v úmyslu využívat pro jednotlivé druhy kryptoaktiv a potvrzení, že oznamující subjekt neobdrží žádnou formu odměny, slevy nebo nepeněžní výhody za směrování přijatých pokynů na konkrétní obchodní platformu pro kryptoaktiva;

d) jak se při provádění pokynů zohledňuje cena, náklady, rychlost, pravděpodobnost provedení a vypořádání, objem, povaha, podmínky úschovy kryptoaktiv nebo jakékoli jiné relevantní faktory, které jsou zvažovány v rámci všech nezbytných kroků k dosažení nejlepšího možného výsledku pro zákazníka;

e) případně opatření pro informování zákazníků o tom, že oznamující subjekt bude provádět pokyny mimo obchodní platformu, a způsobu, jakým oznamující subjekt získá předchozí výslovný souhlas zákazníka před provedením těchto pokynů;

f) jak je zákazník upozorněn na to, že jakékoli konkrétní instrukce zákazníka mohou oznamujícímu subjektu zabránit v tom, aby v souladu s opatřeními, která oznamující subjekt zavedl a uplatňuje ve svých zásadách provádění pokynů, podnikl nezbytné kroky za účelem dosahování nejlepšího možného výsledku při provádění daných pokynů, pokud jde o prvky, jichž se tyto instrukce týkají;

g) procesu výběru obchodních míst, používaných strategií provádění pokynů, opatření používaných k analyzování dosažené kvality provedení pokynů a způsobu, jakým oznamující subjekt sleduje a ověřuje, zda byly pro zákazníky dosaženy nejlepší možné výsledky;

h) opatření k zabránění zneužití jakýchkoli informací týkajících se pokynů zákazníků zaměstnanci oznamujícího subjektu;

i) ujednání a postupů, jak oznamující subjekt sdělí zákazníkům informace o svých zásadách provádění pokynů a jak jim oznámí veškeré podstatné změny těchto zásad;

j) opatření k prokázání souladu s článkem 78 nařízení (EU) 2023/1114 příslušnému orgánu na jeho žádost.

Článek 10

Poskytování poradenství týkajícího se kryptoaktiv nebo správy portfolia kryptoaktiv

Pro účely čl. 60 odst. 7 písm. i) nařízení (EU) 2023/1114 oznamující subjekt, který má v úmyslu poskytovat poradenství týkající se kryptoaktiv nebo správu portfolia kryptoaktiv, poskytne příslušnému orgánu tyto informace:

a) podrobný popis opatření zavedených oznamujícím subjektem k zajištění souladu s čl. 81 odst. 7 nařízení (EU) 2023/1114, včetně následujících informací:

   i) mechanismů pro účinnou kontrolu, hodnocení a udržování znalostí a odbornosti fyzických osob poskytujících poradenství týkající se kryptoaktiv nebo spravujících portfolia kryptoaktiv;

   ii) opatření zajišťujících, že fyzické osoby podílející se na poskytování poradenství nebo správy portfolia znají, chápou a uplatňují vnitřní zásady a postupy oznamujícího subjektu zavedené za účelem dosažení souladu s nařízením (EU) 2023/1114, zejména s čl. 81 odst. 1 uvedeného nařízení a se směrnicí (EU) 2015/849;

iii) objemu lidských a finančních zdrojů, které oznamující subjekt plánuje každoročně vynaložit na odborný rozvoj a odbornou přípravu zaměstnanců poskytujících poradenství týkající se kryptoaktiv nebo spravujících portfolia kryptoaktiv;

b) mechanismy pro kontrolu, posouzení a udržování nezbytných znalostí a odbornosti fyzických osob poskytujících poradenství jménem oznamujícího subjektu podle kritérií pro toto posouzení používaných ve vnitrostátních právních předpisech, aby bylo možné posoudit vhodnost, jak je uvedeno v čl. 81 odst. 1 nařízení (EU) 2023/1114.

Článek 11

Služby převodu

Pro účely čl. 60 odst. 7 písm. k) nařízení (EU) 2023/1114 oznamující subjekt, který má v úmyslu poskytovat služby převodu kryptoaktiv jménem zákazníků, poskytne příslušnému orgánu tyto informace:

a) podrobnosti o druzích kryptoaktiv, pro které má oznamující subjekt v úmyslu poskytovat služby převodu;

b) podrobný popis opatření zavedených oznamujícím subjektem za účelem splnění požadavků článku 82 nařízení (EU) 2023/1114, včetně podrobných informací o opatřeních oznamujícího subjektu a nasazených prostředcích IKT a lidských zdrojích pro rychlé, účinné a důkladné řešení rizik během poskytování služeb převodu kryptoaktiv jménem zákazníků, s přihlédnutím k možným provozním selháním a kybernetickým bezpečnostním rizikům;

c) popis pojistné smlouvy oznamujícího subjektu, pokud je k dispozici, včetně informací o pojistném krytí škod na kryptoaktivech zákazníků, které mohou vzniknout v důsledku kybernetických bezpečnostních rizik;

d) opatření k zajištění toho, aby byli zákazníci o opatřeních uvedených v písmenu b) náležitě informováni.

Článek 12

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 31. října 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN