2025/847

7.5.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/847

ze dne 6. května 2025,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o reakce na narušení bezpečnosti evropských peněženek digitální identity

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES ([1]), a zejména na čl. 5e odst. 5 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Evropský rámec pro digitální identitu (dále jen „rámec“) stanovený v nařízení (EU) č. 910/2014 je klíčovým prvkem při vytváření bezpečného a interoperabilního ekosystému digitální identity v celé Unii. Základem rámce, jehož cílem je usnadnit přístup ke službám v členských státech a zároveň zajistit ochranu osobních údajů a soukromí, jsou evropské peněženky digitální identity (dále jen „peněženky“).

(2) Na činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([2]) a nařízení (EU) 2018/1725 ([3]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([4]). Pravidly pro posuzování a poskytování informací stanovenými tímto nařízením není dotčena povinnost podle nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725 oznamovat v příslušných případech porušení zabezpečení osobních údajů příslušnému dozorovému úřadu ani povinnost podle uvedených nařízení oznamovat v příslušných případech porušení zabezpečení osobních údajů subjektům údajů.

(3) Komise pravidelně posuzuje nové technologie, postupy, normy a technické specifikace. V zájmu zajištění nejvyšší úrovně harmonizace mezi členskými státy při vývoji a certifikaci peněženek se technické specifikace stanovené v tomto nařízení opírají o práci provedenou podle doporučení Komise (EU) 2021/946 ([5]), zejména pokud jde o architekturu a referenční rámec, který je jeho součástí. V souladu se 75. bodem odůvodnění nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([6]) by Komise měla toto nařízení přezkoumat a v případě potřeby aktualizovat, aby bylo v souladu s globálním vývojem a architekturou a referenčním rámcem a aby byly dodržovány osvědčené postupy na vnitřním trhu.

([1]) Úř. věst. L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

([3]) 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).

([4]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Doporučení Komise (EU) 2021/946 ze dne 3. června 2021 o společném souboru nástrojů Unie pro koordinovaný přístup k rámci pro evropskou digitální identitu (Úř. věst. L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu (Úř. věst. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) V případě narušení nebo ohrožení bezpečnosti řešení peněženek nebo mechanismů ověřování platnosti uvedených v čl. 5a odst. 8 nařízení (EU) č. 910/2014 nebo systému elektronické identifikace, v jehož rámci jsou řešení peněženky poskytována, musí následovat rychlé, koordinované a bezpečné reakce na taková narušení a ohrožení bezpečnosti ve všech členských státech, aby byli chráněni uživatelé a zachována důvěra v ekosystém digitální identity. Tím není dotčena směrnice Evropského parlamentu a Rady (EU) 2022/2555 ([7]) a nařízení Evropského parlamentu a Rady (EU) 2019/881 ([8]) a (EU) 2024/2847 ([9]), zejména pokud jde o řešení incidentů nebo zranitelností a jejich posuzování jako narušení bezpečnosti. Členské státy by proto měly zajistit včasné pozastavení poskytování a používání peněženek ovlivněných narušením nebo ohrožením bezpečnosti, nebo v příslušných případech jejich stažení.

(5) Aby byla zajištěna vhodná reakce na narušení nebo ohrožení bezpečnosti, měly by členské státy posoudit, zda narušení nebo ohrožení bezpečnosti řešení peněženky, mechanismů ověřování platnosti uvedených v čl. 5a odst. 8 nařízení (EU) č. 910/2014 nebo systému elektronické identifikace, v jehož rámci je poskytováno řešení peněženky, ovlivňuje spolehlivost tohoto řešení peněženky nebo jiných řešení peněženky. Toto posouzení by mělo být založeno na jednotných kritériích, jako je počet a kategorie dotčených uživatelů peněženky, fyzických osob a stran spoléhajících se na peněženku, povaha dotčených dat, doba trvání narušení nebo ohrožení bezpečnosti, omezená dostupnost služby a finanční ztráty a potenciální ohrožení osobních údajů. Tato kritéria by měla členským státům poskytnout flexibilitu a volnost přiměřeným způsobem určit, zda je ovlivněna spolehlivost řešení peněženky a zda je vhodné pozastavení nebo, je-li to odůvodněno závažností narušení nebo ohrožení, stažení řešení peněženky. Tato kritéria by neměla vést k automatickému stažení řešení peněženky nebo k automatickému pozastavení poskytování a používání řešení peněženky, ale členské státy by je měly řádně zvážit při rozhodování, zda je stažení nebo pozastavení poskytování a používání řešení peněženky nezbytné.

(6) Vzhledem k dopadu a obtížím způsobeným pozastavením používání řešení peněženky budou členské státy muset vyhodnotit, zda jsou zneplatnění potvrzení jednotek peněženky nebo jakákoli jiná dodatečná opatření nezbytná k přiměřené reakci na dané narušení nebo ohrožení bezpečnosti.

(7) Aby byli uživatelé peněženky informováni o stavu svých peněženek, musí jim být poskytnuty odpovídající informace o narušeních nebo ohroženích bezpečnosti ovlivňujících jejich peněženky. Vzhledem k tomu, že strany spoléhající se na peněženku registrované v Unii mohou být rovněž dotčeny narušeními a ohroženími bezpečnosti, je třeba sdílet příslušné informace o narušeních a ohroženích bezpečnosti i s nimi.

(8) V zájmu posílení transparentnosti a vybudování důvěry v ekosystém digitální identity by informace o narušeních nebo ohroženích bezpečnosti a o jejich důsledcích měly zahrnovat alespoň informace požadované podle tohoto nařízení. Informace o narušeních nebo ohroženích bezpečnosti sdílené s uživateli peněženky a stranami spoléhajícími se na peněženku by však měly být pečlivě uváženy, aby se předešlo jejich zneužití útočníky a minimalizovalo riziko takového zneužití.

([7]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti) (Úř. věst. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Aby měli uživatelé po nápravě narušení nebo ohrožení bezpečnosti opět přístup ke svým jednotkám peněženky, bude muset členský stát, který řešení peněženky poskytl, bez zbytečného odkladu obnovit poskytování a používání těchto řešení peněženky. Toho lze dosáhnout opětovným vytvořením jednotek peněženky, vydáním jednotek peněženky poskytovaných v rámci nové verze řešení peněženky nebo opětovným vydáním nových platných potvrzení jednotek peněženky. Dotčení uživatelé peněženky, strany spoléhající se na peněženku, jednotná kontaktní místa určená podle čl. 46c odst. 1 nařízení (EU) č. 910/2014 a Komise musí být patřičně informováni.

(10) Aby se zajistilo stažení peněženek, pokud narušení nebo ohrožení bezpečnosti nebylo napraveno do tří měsíců od pozastavení nebo pokud je to odůvodněno závažností narušení nebo ohrožení bezpečnosti, měl by členský stát zajistit, aby byla příslušná potvrzení jednotek peněženky zneplatněna a nemohla být vrácena do platného stavu ani být vydána či poskytnuta stávajícím jednotkám peněženky. V rámci dotčeného řešení peněženky by navíc neměly být poskytovány nové jednotky peněženky. Pro účely transparentnosti musí být uživatelé, spoléhající se strany, jednotná kontaktní místa určená podle čl. 46c odst. 1 nařízení (EU) č. 910/2014 a Komise o stažení informováni. To zahrnuje popis potenciálních dopadů na uživatele peněženky, zejména na správu vydaných potvrzení nebo na strany spoléhající se na peněženku.

(11) Tříměsíční lhůta, která následuje po pozastavení poskytování a používání řešení peněženky a během níž má být napraveno narušení nebo ohrožení bezpečnosti, které k tomuto pozastavení vedlo, by měla poskytnout termín, do kdy má být řešení peněženky staženo, nebylo-li provedeno vhodné nápravné opatření. Členské státy však mohou požadovat, aby narušení nebo ohrožení bezpečnosti bylo napraveno ve lhůtě kratší než tři měsíce, zejména, je-li to relevantní, s ohledem na rozsah, dobu trvání a důsledky daného narušení nebo ohrožení bezpečnosti. Pokud narušení nebo ohrožení bezpečnosti není napraveno nebo jej nelze napravit ve lhůtě stanovené členským státem, může členský stát požadovat, aby bylo řešení peněženky staženo před uplynutím tříměsíční lhůty. Členské státy by tuto lhůtu, během níž musí být napraveno narušení nebo ohrožení bezpečnosti, které vedlo k pozastavení poskytování a používání řešení peněženky, měly využít k přípravě na možné stažení tohoto řešení peněženky a z toho plynoucí komunikaci.

(12) Aby se snížila administrativní zátěž členských států, pokud jde o informace, které mají být v souladu s tímto nařízením poskytovány Komisi a ostatním členským státům, měly by členské státy využívat stávající nástroje pro oznamování, jako je systém CIRAS (*Cyber Incident Reporting and Analysis System*) pro hlášení a analýzu kybernetických incidentů provozovaný Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA). Pokud jde o alternativní kanály nebo prostředky, které se mají použít k informování uživatelů peněženky dotčených narušením nebo ohrožením bezpečnosti a stran spoléhajících se na peněženku, měly by členské státy zajistit, aby příslušné informace byly poskytovány jasným, srozumitelným a jednoduše dostupným způsobem. Kanály pro poskytování těchto informací dotčeným uživatelům peněženek a stranám spoléhajícím se na peněženku by měly zahrnovat vhodná řešení pro hromadné sdělování založené na internetových stránkách, sledování aktualizací internetových stránek v reálném čase a agregaci zpráv.

(13) V souladu s čl. 42 odst. 1 nařízení (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal své stanovisko dne 31. ledna 2025.

(14) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného článkem 48 nařízení (EU) č. 910/2014,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Předmět

Toto nařízení stanoví pravidla pro reakce na narušení bezpečnosti peněženek, mechanismů ověřování platnosti uvedených v čl. 5a odst. 8 nařízení (EU) č. 910/2014 a systému elektronické identifikace, v jehož rámci jsou peněženky poskytovány.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

1) „řešením peněženky“ kombinace softwaru, hardwaru, služeb, nastavení a konfigurací, včetně instancí peněženky, jedné nebo více bezpečných kryptografických aplikací peněženky a jednoho nebo více bezpečných kryptografických prostředků peněženky;

2) „uživatelem peněženky“ uživatel, který má jednotku peněženky pod kontrolou;

3) „stranou spoléhající se na peněženku“ spoléhající se strana, která má v úmyslu spoléhat se na jednotky peněženky při poskytování veřejných nebo soukromých služeb prostřednictvím digitální interakce;

4) „instancí peněženky“ aplikace nainstalovaná a nakonfigurovaná v zařízení nebo prostředí uživatele peněženky, která je součástí jednotky peněženky a kterou uživatel peněženky používá k interakci s jednotkou peněženky;

5) „bezpečnou kryptografickou aplikací peněženky“ aplikace, která spravuje kritická aktiva prostřednictvím propojení s kryptografickými a nekryptografickými funkcemi poskytovanými bezpečným kryptografickým prostředkem peněženky a jejich využívání;

6) „bezpečným kryptografickým prostředkem peněženky“ prostředek odolný proti neoprávněné manipulaci, který poskytuje prostředí propojené s bezpečnou kryptografickou aplikací peněženky a používané touto aplikací k ochraně kritických aktiv a poskytování kryptografických funkcí pro bezpečné provádění kritických operací;

7) „poskytovatelem peněženky“ fyzická nebo právnická osoba, která poskytuje řešení peněženky;

8) „jednotkou peněženky“ jedinečná konfigurace řešení peněženky, která zahrnuje instance peněženky, bezpečné kryptografické aplikace peněženky a bezpečné kryptografické prostředky peněženky, které poskytovatel peněženky poskytuje jednotlivému uživateli peněženky;

9) „kritickými aktivy“ aktiva v rámci jednotky peněženky nebo ve vztahu k ní, která jsou tak mimořádně důležitá, že ohrožení jejich dostupnosti, důvěrnosti nebo integrity by mělo velmi vážný a oslabující účinek na schopnost spoléhat se na jednotku peněženky;

10) „potvrzením jednotky peněženky“ datový objekt, který popisuje komponenty jednotky peněženky nebo umožňuje autentizaci a ověření platnosti těchto komponentů.

Článek 3

Zjištění narušení nebo ohrožení bezpečnosti

1. Aniž je dotčena směrnice (EU) 2022/2555 a nařízení (EU) 2019/881 a (EU) 2024/2847, členské státy řádně uváží kritéria stanovená v příloze I tohoto nařízení, aby posoudily, zda narušení nebo ohrožení bezpečnosti řešení peněženky, mechanismů ověřování platnosti uvedených v čl. 5a odst. 8 nařízení (EU) č. 910/2014 nebo systému elektronické identifikace, v jehož rámci je řešení peněženky poskytováno, ovlivňují jejich spolehlivost nebo spolehlivost jiných řešení peněženky.

2. Pokud členský stát na základě posouzení uvedeného v odstavci 1 zjistí, že narušení nebo ohrožení bezpečnosti ovlivňuje spolehlivost řešení peněženky, a pozastaví poskytování a používání tohoto řešení peněženky, přijme opatření stanovená v článcích 4 a 5. Pokud členský stát stáhne řešení peněženky, přijme opatření stanovená v článcích 8 a 9.

3. Pokud se členský stát dozví o informacích týkajících se možného narušení nebo ohrožení bezpečnosti, které by mohlo ovlivnit spolehlivost jednoho nebo více řešení peněženky poskytovaných jiným členským státem, sdělí tuto skutečnost bez zbytečného odkladu Komisi a jednotným kontaktním místům dotčených členských států určeným podle čl. 46c odst. 1 nařízení (EU) č. 910/2014. Toto sdělení zahrnuje informace stanovené v čl. 5 odst. 2.

4. Členský stát, který obdrží informace poskytnuté podle odstavce 3, přijme bez zbytečného odkladu opatření stanovená v odstavcích 1 a 2.

Článek 4

Pozastavení poskytování a používání peněženek a další nápravná opatření

1. Členské státy zajistí, aby v rámci pozastaveného řešení peněženky nebyly poskytovány, používány ani aktivovány žádné jednotky peněženky.

2. Členské státy zhodnotí, zda je zneplatnění potvrzení jednotek peněženky u jednotek peněženky dotčených pozastavením řešení peněženky nebo jakékoli jiné dodatečné nápravné opatření nezbytné k odpovídající reakci na narušení nebo ohrožení bezpečnosti.

3. Opatření stanovená v odstavcích 1 a 2 musí být přijata bez zbytečného odkladu a v každém případě nejpozději do 24 hodin po pozastavení poskytování a používání řešení peněženky, které je narušením nebo ohrožením bezpečnosti dotčeno.

4. Opatření stanovená v odstavcích 1 a 2 nesmí dotčeným uživatelům peněženky bránit ve výkonu práva na přenositelnost údajů stanoveného v čl. 5a odst. 4 písm. g) nařízení (EU) č. 910/2014. Podmínkou však je, že toto právo mohou uživatelé peněženky vykonávat, aniž by byla snížena bezpečnost kritických aktiv dotčených jednotek peněženky, zejména s ohledem na důvody pozastavení a potřebu zajistit účinnou ochranu těchto aktiv před zneužitím.

Článek 5

Informace o pozastaveních a nápravných opatřeních

1. Jasné, srozumitelné a jednoduše dostupné informace o pozastavení poskytování a používání řešení peněženky se bez zbytečného odkladu a nejpozději do 24 hodin po pozastavení poskytování a používání řešení peněženky poskytnou:

a) jednotným kontaktním místům určeným podle čl. 46c odst. 1 nařízení (EU) č. 910/2014;

b) Komisi;

c) dotčeným uživatelům peněženky;

d) stranám spoléhajícím se na peněženku registrovaným v souladu s článkem 5b nařízení (EU) č. 910/2014.

2. Informace poskytnuté v souladu s odstavcem 1 zahrnují alespoň:

a) název poskytovatele řešení peněženky, jehož poskytování a používání bylo pozastaveno;

b) název a referenční identifikátor tohoto řešení peněženky, jak jsou uvedeny v seznamu certifikovaných peněženek vypracovaném podle článku 5d nařízení (EU) č. 910/2014, a v příslušných případech dotčené verze;

c) datum a čas, kdy bylo narušení nebo ohrožení bezpečnosti zjištěno;

d) jsou-li známy, datum a čas, kdy nastaly účinky narušení nebo ohrožení bezpečnosti, a to na základě síťových nebo systémových protokolů nebo jiných zdrojů dat;

e) datum a čas, kdy bylo řešení peněženky pozastaveno;

f) kontaktní údaje zahrnující alespoň e-mailovou adresu a telefonní číslo oznamujícího členského státu a pokud se liší, poskytovatele peněženky uvedeného v písmenu (a);

g) popis narušení nebo ohrožení bezpečnosti;

h) popis ohrožených údajů, v příslušných případech včetně kategorií osobních údajů definovaných v čl. 9 odst. 1 a článku 10 nařízení (EU) 2016/679;

i) je-li to možné, odhad přibližného počtu dotčených uživatelů peněženky a dalších dotčených fyzických osob;

j) popis potenciálních dopadů na strany spoléhající se na peněženku nebo na uživatele peněženky a v druhém uvedeném případě, je-li to relevantní, nástin opatření, která mohou uživatelé peněženky přijmout ke zmírnění těchto potenciálních dopadů;

k) popis přijatých nebo plánovaných opatření k nápravě narušení nebo ohrožení bezpečnosti spolu s harmonogramem a lhůtou pro tuto nápravu;

l) je-li to relevantní a vhodné, popis přijatých nebo plánovaných opatření pro převedení dotčených uživatelů peněženky na alternativní služby nebo řešení peněženky.

Článek 6

Obnovení poskytování a používání peněženek

Je-li to nezbytné k zajištění obnovy poskytování, aktivace a používání řešení peněženky, členské státy bez zbytečného odkladu:

1) obnoví poskytování a používání jednotek peněženky poskytovaných v rámci tohoto řešení peněženky vydáním jednotky peněženky poskytované v rámci nové verze řešení peněženky všem dotčeným uživatelům;

2) vydají nová potvrzení jednotek peněženky novým jednotkám peněženky nebo v příslušných případech dříve vydaným jednotkám peněženky, pokud tyto jednotky peněženky splňují bezpečnostní požadavky zavedené po nápravě narušení nebo ohrožení bezpečnosti;

3) zruší případná opatření provedená podle článku 4, která brání poskytování nových jednotek peněženky v rámci dotčeného řešení peněženky, pokud se tato opatření týkala výhradně narušení nebo ohrožení bezpečnosti, které je nyní napraveno.

Článek 7

Informace o obnovení

Pokud členský stát obnoví řešení peněženky, zajistí, aby:

1) informace o této skutečnosti byly bez zbytečného odkladu poskytnuty všem stranám, které obdržely informace o pozastavení poskytování a používání daného řešení peněženky v souladu s čl. 5 odst. 1;

2) informace poskytnuté podle bodu 1 zahrnovaly alespoň prvky uvedené v čl. 5 odst. 2 písm. (a), (b) a (f) až (h) a tyto prvky:

   a) datum a čas, kdy bylo narušení nebo ohrožení bezpečnosti napraveno;

   b) datum a čas obnovení dotčeného řešení peněženky a v příslušných případech dotčených jednotek peněženky poskytovaných v rámci tohoto řešení peněženky;

   c) popis opatření přijatých k nápravě narušení nebo ohrožení bezpečnosti;

   d) popis potenciálních zbytkových dopadů na strany spoléhající se na peněženku nebo na uživatele peněženky a v druhém uvedeném případě, je-li to relevantní, nástin opatření, která mohou uživatelé peněženky přijmout ke zmírnění těchto potenciálních zbytkových dopadů.

Článek 8

Stažení peněženek

1. Není-li narušení nebo ohrožení bezpečnosti, které vedlo k pozastavení poskytování a používání řešení peněženky, napraveno do tří měsíců od data pozastavení poskytování a používání tohoto řešení peněženky, členský stát, který toto řešení peněženky poskytuje, zajistí, aby bylo dotčené řešení peněženky staženo a zrušena jeho platnost, a to bez zbytečného odkladu a v každém případě do 72 hodin po uplynutí tříměsíční lhůty.

2. Když členský stát stáhne řešení peněženky, zajistí, aby:

a) potvrzení jednotek peněženky pro jednotku peněženky dotčeného řešení peněženky byla zneplatněna;

b) potvrzení jednotky peněženky se nemohla vrátit zpět do platného stavu;

c) pro stávající jednotky peněženky poskytované v rámci dotčeného řešení peněženky nebylo možné vydat žádná nová potvrzení jednotky peněženky;

d) v rámci dotčeného řešení peněženky nebylo možné poskytnout žádnou novou jednotku peněženky.

3. Opatření stanovená v odstavcích 1 a 2 nesmí dotčeným uživatelům peněženky bránit ve výkonu práva na přenositelnost údajů stanoveného v čl. 5a odst. 4 písm. g) nařízení (EU) č. 910/2014. Podmínkou však je, že toto právo mohou uživatelé peněženky vykonávat, aniž by byla snížena bezpečnost kritických aktiv dotčených jednotek peněženky, zejména s ohledem na důvody stažení a potřebu zajistit účinnou ochranu těchto aktiv před zneužitím.

Článek 9

Informace o stažení

1. Jasné, srozumitelné a jednoduše dostupné informace o stažení řešení peněženky se bez zbytečného odkladu a nejpozději do 24 hodin po stažení řešení peněženky poskytnou:

a) jednotným kontaktním místům určeným podle čl. 46c odst. 1 nařízení (EU) č. 910/2014;

b) Komisi;

c) dotčeným uživatelům peněženky;

d) stranám spoléhajícím se na peněženku registrovaným v souladu s článkem 5b nařízení (EU) č. 910/2014.

2. Informace poskytnuté v souladu s odstavcem 1 zahrnují alespoň:

a) název poskytovatele řešení peněženky, které bylo staženo;

b) název a referenční identifikátor tohoto řešení peněženky, jak jsou uvedeny v seznamu certifikovaných peněženek vypracovaném podle článku 5d nařízení (EU) č. 910/2014, a v příslušných případech dotčené verze;

c) datum a čas, kdy bylo zjištěno narušení nebo ohrožení bezpečnosti, které z důvodu své závažnosti nebo proto, že nebylo napraveno do tří měsíců, vedlo ke stažení dotčeného řešení peněženky;

d) jsou-li známy, datum a čas, kdy nastaly účinky narušení nebo ohrožení bezpečnosti, a to na základě síťových nebo systémových protokolů nebo jiných zdrojů dat;

e) datum a čas, kdy bylo staženo řešení peněženky a účinně zneplatněna potvrzení jednotky peněženky u jednotek peněženky poskytnutých v rámci daného řešení peněženky;

f) informaci, zda je stažení důsledkem závažnosti narušení nebo ohrožení bezpečnosti nebo je důsledkem nenapravení narušení nebo ohrožení bezpečnosti;

g) kontaktní údaje zahrnující alespoň e-mailovou adresu a telefonní číslo oznamujícího členského státu a pokud se liší, poskytovatele peněženky uvedeného v písmenu (a);

h) popis narušení nebo ohrožení bezpečnosti;

i) popis ohrožených údajů, v příslušných případech včetně kategorií osobních údajů stanovených v čl. 9 odst. 1 a článku 10 nařízení (EU) 2016/679;

j) je-li to možné, odhad přibližného počtu dotčených uživatelů peněženky a dalších dotčených fyzických osob;

k) popis potenciálních dopadů na strany spoléhající se na peněženku nebo na uživatele peněženky a v druhém uvedeném případě, je-li to relevantní, nástin opatření, která mohou uživatelé peněženky přijmout ke zmírnění těchto potenciálních dopadů;

l) popis přijatých nebo plánovaných opatření pro převedení dotčených uživatelů peněženky na alternativní řešení peněženky nebo, je-li to relevantní a vhodné, alternativní služby.

Článek 10

Informační systém

Členské státy zasílají informace uvedené v článcích 3, 5, 7 a 9 Komisi a jednotným kontaktním místům členských států určeným podle čl. 46c odst. 1 nařízení (EU) č. 910/2014 prostřednictvím systému CIRAS provozovaného agenturou ENISA nebo rovnocenného systému, na němž se členské státy a Komise dohodnou.

Článek 11

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 s výjimkou článku 10, který se použije ode dne 7. května 2026.

V Bruselu dne 6. května 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA

Kritéria pro posouzení narušení nebo ohrožení bezpečnosti

1. Členské státy při posuzování narušení nebo ohrožení bezpečnosti vycházejí z těchto kritérií:

a) narušení nebo ohrožení způsobilo nebo může způsobit smrt fyzické osoby nebo značnou újmu na zdraví fyzické osoby;

b) došlo nebo může dojít k úspěšnému podezřelému zlovolnému nebo neoprávněnému přístupu k síti a informačním systémům poskytovatele peněženky, poskytovatele mechanismů ověřování platnosti uvedených v čl. 5a odst. 8 nařízení (EU) č. 910/2014 nebo poskytovatele systému elektronické identifikace, v jehož rámci je poskytováno řešení peněženky (dále jen „dotčené subjekty“), a to způsobem, který může způsobit závažné narušení provozu, přičemž uvedené systémy jsou kritickými součástmi dotčeného řešení peněženky, dotčených mechanismů ověřování platnosti uvedených v čl. 5a odst. 8 nařízení (EU) č. 910/2014 nebo dotčeného systému elektronické identifikace, v jehož rámci je poskytováno řešení peněženky;

c) řešení peněženky, mechanismus ověřování platnosti uvedený v čl. 5a odst. 8 nařízení (EU) č. 910/2014 nebo systém elektronické identifikace, v jehož rámci je poskytováno řešení peněženky, či jejich část:

— jsou nebo dle prognózy budou zcela nedostupné uživatelům peněženky nebo stranám spoléhajícím se na peněženku po dobu delší než 12 po sobě jdoucích hodin,

— jsou nebo dle prognózy budou nedostupné uživatelům peněženky nebo stranám spoléhajícím se na peněženku po dobu delší než 16 hodin, počítáno na základě kalendářního týdne;

d) existuje podezření, že omezená dostupnost řešení peněženky nebo služeb poskytovaných dotčenými subjekty, pokud jde o řešení peněženky, má nebo dle prognózy bude mít dopad na více než 1 % uživatelů peněženky nebo stran spoléhajících se na peněženku;

e) existuje možnost narušení nebo došlo k narušení fyzického přístupu omezeného na důvěryhodné pracovníky dotčených subjektů či ochrany takového fyzického přístupu, a to k jednomu nebo více místům, kde se nacházejí sítě a informační systémy podporující řešení peněženky, poskytování mechanismů ověřování platnosti uvedených v čl. 5a odst. 8 nařízení (EU) č. 910/2014 spojených s řešením peněženky nebo systém elektronické identifikace, v jehož rámci je řešení peněženky poskytováno;

f) došlo nebo může dojít k ohrožení soukromí, integrity, důvěrnosti nebo autenticity dat uchovávaných, předávaných nebo zpracovávaných v řešení peněženky, přičemž toto ohrožení se vyznačuje jednou nebo více z těchto charakteristik:

— má dopad na více než 1 % uživatelů peněženky v rámci dotčeného řešení peněženky nebo na více než 100 000 těchto uživatelů peněženky, podle toho, který počet je menší,

— je výsledkem úspěšné podezřelé zlovolné činnosti;

— je nebo pravděpodobně je důsledkem jedné nebo více známých zranitelností, včetně zranitelností, s nimiž je nakládáno v souladu s prováděcím nařízením Komise (EU) 2024/2981 ([1]),

— pravděpodobně ovlivní osobní údaje způsobem, který bude mít pravděpodobně za následek riziko pro práva a svobody dotčených fyzických osob, zejména v případě porušení zabezpečení osobních údajů ve smyslu čl. 9 odst. 1 a článku 10 nařízení (EU) 2016/679;

([1]) Prováděcí nařízení Komise (EU) 2024/2981 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o certifikaci evropských peněženek digitální identity (Úř. věst. L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— pravděpodobně bude mít dopad na elektronické komunikace osob,

— pravděpodobně bude mít za následek vysoké riziko pro práva a svobody fyzických osob,

— pravděpodobně bude mít dopad na zranitelné fyzické osoby;

g) certifikace řešení peněženky byla zrušena nebo se předpokládá, že bude zrušena;

h) narušení nebo ohrožení způsobilo nebo může způsobit dotčenému subjektu přímou finanční ztrátu, přičemž tato ztráta přesahuje 500 000 EUR nebo v příslušných případech 5 % celkového ročního obratu dotčeného subjektu za předchozí účetní období, podle toho, která částka je nižší.

2. Členské státy neberou v úvahu plánované důsledky údržby prováděné dotčenými subjekty nebo jejich jménem, pokud tato údržba:

a) byla předem oznámena potenciálně dotčeným uživatelům peněženky, stranám spoléhajícím se na peněženku a příslušným orgánům dohledu;

b) nesplňuje žádné z kritérií stanovených v bodě 1 této přílohy.

3. Pokud jde o bod 1 písm. (c), doba trvání incidentu ovlivňujícího dostupnost se měří od okamžiku, kdy je narušeno řádné poskytování ovlivněné služby, až do okamžiku, kdy je služba obnovena a znovu v provozu. Pokud dotčený subjekt není schopen určit okamžik, kdy narušení začalo, měří se doba trvání incidentu od okamžiku, kdy byl incident zjištěn, nebo od okamžiku, kdy byl incident zaznamenán v síťových nebo systémových protokolech nebo jiných zdrojích dat, podle toho, co nastalo dříve. Úplná nedostupnost služby se měří od okamžiku, kdy je služba uživatelům zcela nedostupná, do okamžiku, kdy byly běžné činnosti nebo provoz obnoveny na úroveň služby poskytovanou před incidentem. Pokud dotčený subjekt není schopen určit, kdy úplná nedostupnost služby začala, měří se nedostupnost od okamžiku, kdy ji tento subjekt zjistil.

4. Pokud jde o bod 1 písm. (d), má se za to, že k omezené dostupnosti služby dochází zejména tehdy, je-li služba výrazně pomalejší než průměrná doba odezvy nebo nejsou-li k dispozici všechny funkce služby. Pokud je to možné, použijí se pro posouzení zpoždění v době odezvy objektivní kritéria založená na průměrných dobách odezvy služeb.

5. K určení přímých finančních ztrát v důsledku narušení nebo ohrožení uvedených v bodě 1 písm. (h) dotčené subjekty vezmou v úvahu všechny finanční ztráty, které jim v důsledku incidentu vznikly, jako jsou náklady na náhradu nebo přemístění softwaru, hardwaru nebo infrastruktury, náklady na zaměstnance, včetně nákladů spojených s náhradou nebo přeložením zaměstnanců, náborem dalších zaměstnanců, odměn za přesčasy a obnovy pozbytých nebo zhoršených dovedností, poplatky v důsledku nedodržení smluvních závazků, náklady na nápravu a kompenzace zákazníkům, ztráty v důsledku ušlých příjmů, náklady spojené s interní a externí komunikací a náklady na poradenství, včetně nákladů spojených s právním poradenstvím, forenzními službami a službami souvisejícími se zajišťováním nápravy. Náklady nezbytné pro každodenní provoz podniku, jako jsou náklady na obecnou údržbu infrastruktury, vybavení, hardwaru a softwaru, vylepšování, iniciativy v oblasti posuzování rizik a pojistné se nepovažují za finanční ztráty v důsledku incidentu. Dotčené subjekty vypočtou částky finančních ztrát na základě dostupných údajů, a pokud nelze určit skutečnou výši finančních ztrát, tyto částky odhadnou.