Úřední věstník
Evropské unie

CS
Řada L

2024/2982

4.12.2024

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2024/2982

ze dne 28. listopadu 2024,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o protokoly a rozhraní, které mají být podporovány evropským rámcem pro digitální identitu

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. 5a odst. 23 uvedeného nařízení,

vzhledem k těmto důvodům:

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

(2) Na všechny činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([2]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([3]).

(3) Ustanovení čl. 5a odst. 23 nařízení (EU) č. 910/2014 pověřuje Komisi, aby v případě potřeby stanovila příslušné specifikace a postupy. Toho je dosaženo prostřednictvím čtyř prováděcích nařízení, která se zabývají protokoly a rozhraními: prováděcí nařízení Komise (EU) 2024/2982 ([4]), integritou a základními funkcemi: prováděcí nařízení Komise (EU) 2024/2979 ([5]), osobními identifikačními údaji a elektronickým potvrzením atributů: prováděcí nařízení Komise (EU) 2024/2977 ([6]), jakož i oznámeními Komisi: prováděcí nařízení Komise (EU) 2024/2980 ([7]). Toto nařízení stanoví příslušné požadavky na protokoly a rozhraní.

([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]) 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).

([4]) Prováděcí nařízení Komise (EU) 2024/2982 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o protokoly a rozhraní, které mají být podporovány evropským rámcem pro digitální identitu (Úř. věst. L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Prováděcí nařízení Komise (EU) 2024/2979 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o integritu a základní funkce evropských peněženek digitální identity (Úř. věst. L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Prováděcí nařízení Komise (EU) 2024/2977 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o osobní identifikační údaje a elektronická potvrzení atributů vydávané k evropským peněženkám digitální identity (Úř. věst. L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Prováděcí nařízení Komise (EU) 2024/2980 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o oznámení Komisi týkající se ekosystému evropských peněženek digitální identity (Úř. věst. L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Komise pravidelně posuzuje nové technologie, postupy, normy nebo technické specifikace. V zájmu zajištění co nejvyšší úrovně harmonizace mezi členskými státy při vývoji a certifikaci peněženek se technické specifikace stanovené v tomto nařízení opírají o práci provedenou na základě doporučení Komise (EU) 2021/946 ze dne 3. června 2021 o společném souboru nástrojů Unie pro koordinovaný přístup k evropskému rámci pro digitální identitu ([8]), a zejména o architekturu a referenční rámec. V souladu se 75. bodem odůvodnění nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([9]) by Komise měla toto prováděcí nařízení přezkoumat a v případě potřeby ho aktualizovat, aby bylo v souladu s globálním vývojem, architekturou a referenčním rámcem a aby byly dodržovány osvědčené postupy na vnitřním trhu.

(5) Aby byla zajištěna transparentnost a důvěryhodnost stran spoléhajících se na peněženku vůči uživatelům peněženky, měly by protokoly a rozhraní používané řešeními peněženky uživatelům peněženek poskytovat spolehlivý mechanismus pro autentizaci stran spoléhajících se na peněženku a jiných jednotek peněženky. Naopak poskytovatelé peněženek by měli poskytnout mechanismus pro autentizaci a ověření platnosti jednotek peněženky, aby spoléhající se strany mohly obdržet záruky ohledně důvěryhodnosti a pravosti jednotek peněženky. Dále by měla být technická infrastruktura peněženek navržena tak, aby zajišťovala, že se k oprávněným spoléhajícím se stranám přenese pouze minimální nezbytné množství údajů, přičemž by měla být mezi jednotlivými transakcemi zachována nepropojitelnost. S cílem usnadnit vydávání osobních identifikačních údajů a elektronických potvrzení atributů by měla všechna řešení peněženky podporovat minimální sadu protokolů a rozhraní.

(6) Aby byla zajištěna použitelnost řešení peněženky ve všech členských státech, měla by všechna řešení peněženky podporovat obecné technické specifikace, pokud jde o předkládání osobních identifikačních údajů a elektronických potvrzení atributů spoléhajícím se stranám prostřednictvím peněženek, a to jak na dálku, tak i v blízkosti. Kromě toho mohou jednotky peněženky podporovat další protokoly a rozhraní pro konkrétní případy použití.

(7) Aby byla zajištěna záměrná a standardní ochrana údajů, měly by být peněženky vybaveny několika funkcemi pro zvýšení ochrany soukromí s cílem zabránit poskytovatelům prostředků pro elektronickou identifikaci a elektronického potvrzování atributů kombinovat osobní údaje získané při poskytování jiných služeb s osobními údaji zpracovávanými za účelem poskytování služeb, které spadají do oblasti působnosti nařízení (EU) č. 910/2014. Jak je stanoveno v nařízení (EU) č. 910/2014, spoléhající se strany nesmějí od uživatelů požadovat žádné jiné údaje než ty, které jsou uvedeny pro zamýšlené použití peněženek během procesu registrace. Uživatelé peněženky by měli mít možnost kdykoli ověřit registrační údaje spoléhajících se stran. Jednotky peněženek by dále měly být schopny jako součást žádosti o atribut uživatelům zobrazovat registrační certifikáty stran spoléhajících se na peněženku, jsou-li k dispozici. Uživatelům peněženky by to mělo umožnit ověřit, že atributy požadované stranou spoléhající se na peněženku spadají do rozsahu jejich registrovaných atributů, a poskytnout záruku, že žádost je legitimní a důvěryhodná.

(8) V zájmu ochrany údajů uživatelů peněženek by poskytovatelé peněženek měli zajistit, aby jednotky peněženky před zpřístupněním jakýchkoli údajů ověřovaly žádosti od stran spoléhajících se na peněženku nebo od jiných jednotek peněženky. Ze stejného důvodu a v souladu s čl. 5a odst. 4 písm. d) bodem ii) nařízení (EU) č. 910/2014 by poskytovatelé peněženek měli zajistit, aby jednotky peněženky uživatelům peněženek umožňovaly podávat žádosti o výmaz údajů stranám spoléhajícím se na peněženku.

(9) Aby bylo možné rychle reagovat v případě jakýchkoli obav o ochranu údajů souvisejících s čl. 5a odst. 4 písm. d) bodem iii) nařízení (EU) č. 910/2014, měli by poskytovatelé peněženek zajistit, aby řešení peněženky poskytovala mechanismy pro nahlášení spoléhající se strany příslušnému vnitrostátnímu úřadu pro ochranu údajů. Poskytovatelům peněženek a úřadům pro ochranu údajů by měla být ponechána přiměřená flexibilita při vytváření vhodných mechanismů pro interakci s úřady pro ochranu údajů členských států.

(10) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([10]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 30. září 2024.

([8]) Úř. věst. L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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).

([10]) 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).

(11) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru uvedeného v článku 48 nařízení (EU) č. 910/2014,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Předmět a oblast působnosti

Toto nařízení stanoví pravidla pro protokoly a rozhraní řešení peněženek pro:

1) vydávání osobních identifikačních údajů a elektronických potvrzení atributů k jednotkám peněženky;

2) předkládání atributů osobních identifikačních údajů a elektronických potvrzení atributů stranám spoléhajícím se na peněženku a jiným jednotkám peněženky;

3) sdělování žádostí o výmaz údajů stranám spoléhajícím se na peněženku;

4) nahlašování stran spoléhajících se na peněženku dozorovým úřadům zřízeným podle článku 51 nařízení (EU) 2016/679;

které je třeba pravidelně aktualizovat, aby byly v souladu s vývojem technologií a norem a s prací prováděnou na základě doporučení (EU) 2021/946, a zejména s architekturou a referenčním rámcem.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

1) „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;

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

3) „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;

4) „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;

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

6) „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;

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

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

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) „přístupovým certifikátem strany spoléhající se na peněženku“ certifikát pro elektronické pečetě nebo podpisy ověřující pravost a platnost strany spoléhající se na peněženku vydaný poskytovatelem přístupových certifikátů strany spoléhající se na peněženku;

11) „poskytovatelem přístupových certifikátů strany spoléhající se na peněženku“ fyzická nebo právnická osoba pověřená členským státem vydáváním přístupových certifikátů strany spoléhající se na peněženku stranám spoléhajícím se na peněženku registrovaným v tomto členském státě;

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

13) „vloženými zásadami zpřístupňování informací“ soubor pravidel, který je součástí elektronického potvrzení atributů jeho poskytovatelem a ve kterém jsou uvedeny podmínky, jež musí strana spoléhající se na peněženku splnit, aby získala přístup k elektronickému potvrzení atributů;

14) „registračním certifikátem strany spoléhající se na peněženku“ datový objekt, který označuje atributy, které spoléhající se strana zaregistrovala s úmyslem je požadovat od uživatelů;

15) „poskytovatelem osobních identifikačních údajů“ fyzická nebo právnická osoba odpovědná za vydávání a zneplatnění osobních identifikačních údajů a za zajištění kryptografického provázání osobních identifikačních údajů uživatele s jednotkou peněženky;

16) „kryptografickou vazbou“ metoda propojení osobních identifikačních údajů nebo elektronických potvrzení atributů s jednotkami peněženky pomocí kryptografických prostředků.

Článek 3

Obecná ustanovení

Pokud jde o protokoly a rozhraní uvedené v článcích 4 a 5, poskytovatelé peněženek zajistí, aby jednotky peněženky:

1) při interakci se stranami spoléhajícími se na peněženku autentizovaly přístupové certifikáty stran spoléhajících se na peněženku a ověřovaly jejich platnost;

2) při interakci s jinými jednotkami peněženky autentizovaly potvrzení jiných jednotek peněženky a ověřovaly jejich platnost;

3) autentizovaly žádosti podané pomocí přístupových certifikátů stran spoléhajících na peněženku nebo případně pomocí potvrzení od jiných jednotek peněženky a ověřovaly jejich platnost;

4) případně autentizovaly a ověřovaly platnost registračního certifikátu strany spoléhající se na peněženku;

5) zobrazovaly uživatelům peněženky informace obsažené v certifikátech strany spoléhající se na peněženku nebo v potvrzeních jednotky peněženky;

6) případně uživatelům peněženky zobrazovaly atributy, které mají uživatelé peněženky předložit;

7) případně uživatelům peněženky zobrazovaly informace obsažené v registračním certifikátu strany spoléhající se na peněženku;

8) předkládaly potvrzení jednotky peněženky stranám spoléhajícím se na peněženku nebo jednotkám peněženky, které o to požádají;

9) nepředkládaly stranám spoléhajícím se na peněženku nebo jednotkám peněženky žádné požadované atributy, dokud nebudou splněny tyto požadavky:

   a) ověření, zda bezpečná kryptografická aplikace peněženky autentizovala totožnost uživatele peněženky;

   b) ověření, zda byly vložené zásady zpřístupnění zpracovány v rámci jednotky peněženky případně v souladu s článkem 11 prováděcího nařízení (EU) 2024/2979;

   c) ověření, zda uživatelé peněženky předložení schválili částečně nebo v plném rozsahu;

10) umožňovaly metody k zachování soukromí, které zajistí nepropojitelnost v případech, kdy při předkládání potvrzení nebo osobních identifikačních údajů mezi různými stranami spoléhajícími se na peněženku elektronická potvrzení atributů nevyžadují identifikaci uživatele peněženky.

Článek 4

Vydávání osobních identifikačních údajů a elektronických potvrzení atributů k jednotkám peněženky

1. Poskytovatelé peněženek zajistí, aby řešení peněženky podporovala protokoly a rozhraní pro vydávání osobních identifikačních údajů a elektronických potvrzení atributů k jednotkám peněženky.

2. Poskytovatelé peněženek zajistí, aby jednotky peněženky požadovaly vydání osobních identifikačních údajů a elektronických potvrzení atributů pouze od stran, které mají autentický a platný přístupový certifikát strany spoléhající se na peněženku, který potvrzuje jejich roli jako:

a) poskytovatele osobních identifikačních údajů;

b) poskytovatele kvalifikovaného elektronického potvrzení atributů;

c) poskytovatele elektronického potvrzení atributů vydaného subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem nebo

d) poskytovatele nekvalifikovaného elektronického potvrzení atributů.

3. V souvislosti s vydáváním osobních identifikačních údajů a elektronických potvrzení atributů k jednotce peněženky poskytovatelé peněženek zajistí, aby byly splněny tyto požadavky:

a) pokud uživatelé peněženky používají svou jednotku peněženky k požádání o vydání osobních identifikačních údajů nebo elektronických potvrzení atributů od poskytovatelů osobních identifikačních údajů nebo poskytovatelů elektronických potvrzení atributů umožňujících vydání osobních identifikačních údajů nebo elektronických potvrzení atributů ve více než jednom formátu, musí o ně jednotka peněženky požádat ve všech formátech uvedených v článku 8 prováděcího nařízení (EU) 2024/2979, kterým se stanoví prováděcí pravidla k nařízení č. 910/2014, pokud jde o integritu a základní funkce evropských peněženek digitální identity;

b) pokud uživatelé peněženky používají svou jednotku peněženky k interakci s poskytovateli osobních identifikačních údajů nebo elektronických potvrzení atributů, musí jednotky peněženky umožnit autentizaci a potvrzení platnosti komponentů jednotky peněženky tím, že těmto poskytovatelům na jejich žádost předloží potvrzení jednotky peněženky;

c) řešení peněženky podporují mechanismy, které poskytovatelům osobních identifikačních údajů umožňují ověřit vydání, doručení a aktivaci v souladu s požadavky na vysokou úroveň záruky stanovenými v prováděcím nařízení Komise (EU) 2015/1502 ([11]);

d) jednotky peněženky ověřují pravost a platnost osobních identifikačních údajů a elektronických potvrzení atributů.

Článek 5

Předkládání atributů stranám spoléhajícím se na peněženku

1. Poskytovatelé peněženek zajistí, aby řešení peněženky podporovala protokoly a rozhraní pro předkládání atributů stranám spoléhajícím se na peněženku, a to na dálku a případně v blízkosti, v souladu s normami uvedenými v příloze.

2. Poskytovatelé peněženek zajistí, aby jednotky peněženky na žádost uživatelů odpovídaly na úspěšně autentizované žádosti s ověřenou platností od stran spoléhajících se na peněženku uvedených v článku 3 v souladu s normami uvedenými v příloze.

3. Poskytovatelé peněženek zajistí, aby jednotky peněženky podporovaly prokazování vlastnictví soukromých klíčů odpovídajících veřejným klíčům používaným v kryptografických vazbách.

([11]) Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Úř. věst. L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

4. Poskytovatelé peněženek zajistí, aby řešení peněženky podporovala výběrové zpřístupňování atributů osobních identifikačních údajů a elektronických potvrzení atributů.

5. Odstavce 1 až 4 se použijí obdobně na interakce mezi dvěma jednotkami peněženky v blízkosti.

Článek 6

Sdělování žádostí o výmaz údajů

1. Poskytovatelé peněženek zajistí, aby jednotky peněženky podporovaly protokoly a rozhraní, které v souladu s článkem 17 nařízení (EU) 2016/679 umožní uživatelům peněženek požádat strany spoléhající se na peněženky, s nimiž prostřednictvím těchto jednotek peněženky komunikovali, o výmaz svých osobních údajů poskytnutých prostřednictvím těchto jednotek peněženky.

2. Protokoly a rozhraní uvedené v odstavci 1 umožňují uživatelům peněženky vybrat strany spoléhající se na peněženku, kterým mají být žádosti o výmaz údajů zaslány.

3. Jednotky peněženky zobrazují uživateli peněženky předchozí žádosti o výmaz údajů podané prostřednictvím těchto jednotek peněženky.

Článek 7

Nahlašování stran spoléhajících se na peněženku dozorovým úřadům zřízeným podle článku 51 nařízení (EU) 2016/679

1. Poskytovatelé peněženek zajistí, aby jednotky peněženky uživatelům peněženek umožňovaly snadno nahlásit strany spoléhající se na peněženky dozorovým úřadům zřízeným podle článku 51 nařízení (EU) 2016/679.

2. Poskytovatelé peněženek zavedou protokoly a rozhraní pro nahlašování stran spoléhajících se na peněženku v souladu s vnitrostátními procesními předpisy členských států.

3. Poskytovatelé peněženek zajistí, aby jednotky peněženky uživatelům peněženek umožňovaly tato nahlášení doložit, včetně přiložení příslušných informací k identifikaci stran spoléhajících se na peněženku a tvrzení uživatelů peněženek ve strojově čitelném formátu.

Článek 8

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 28. listopadu 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA

NORMY PODLE ČL. 5 ODST. 1 A 2

— ISO/IEC 18013-5:2021

— ISO/IEC TS 18013-7:2024