Úřední věstník
Evropské unie

CS
Řada L

2025/2160

28.10.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/2160

ze dne 27. října 2025,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy, specifikace a postupy pro řízení rizik spojených s poskytováním nekvalifikovaných služeb vytvářejících důvěru

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. 19a odst. 2 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru hrají v digitálním prostředí důležitou roli tím, že poskytují služby vytvářející důvěru, které usnadňují bezpečné elektronické transakce. Nařízení (EU) č. 910/2014 klade na nekvalifikované poskytovatele služeb vytvářejících důvěru méně regulačních požadavků než na kvalifikované poskytovatele služeb vytvářejících důvěru. Požadavky týkající se bezpečnosti a povinnosti zajistit hloubkovou kontrolu operací a služeb, jejich transparentnost a odpovědnost za ně se však vztahují na všechny poskytovatele služeb vytvářejících důvěru.

(2) Nekvalifikované poskytovatele služeb vytvářejících důvěru lze považovat za důležité nebo základní subjekty v souladu s článkem 3 směrnice Evropského parlamentu a Rady (EU) 2022/2555 ([2]). Proto se na ně vztahuje prováděcí nařízení Komise (EU) 2024/2690 ([3]), kterým se stanoví technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik. Rozsah požadavků stanovených v čl. 19a odst. 1 písm. a) nařízení (EU) č. 910/2014 se však týká postupů řízení rizik týkajících se právních, obchodních, provozních a jiných přímých či nepřímých rizik spojených s poskytováním nekvalifikovaných služeb vytvářejících důvěru. S cílem doplnit rámec řízení rizik stanovený v prováděcím nařízení (EU) 2024/2690 a umožnit soudržný přístup k řízení všech příslušných druhů rizik by měly být stanoveny specifikace a postupy týkající se řízení těchto rizik nekvalifikovanými poskytovateli služeb vytvářejících důvěru. Pokyny poskytované Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) nebo příslušnými vnitrostátními orgány podle směrnice (EU) 2022/2555 mohou nekvalifikovaným poskytovatelům služeb vytvářejících důvěru pomoci při navrhování a provádění vhodných politik řízení rizik.

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

([2]) 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).

([3]) Prováděcí nařízení Komise (EU) 2024/2690 ze dne 17. října 2024, kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru (Úř. věst. L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

(3) Předpoklad shody stanovený v čl. 19a odst. 2 nařízení (EU) č. 910/2014 by se měl uplatnit pouze v případě, že nekvalifikovaní poskytovatelé služeb vytvářejících důvěru splňují požadavky stanovené v tomto nařízení. Referenční normy uvedené v příloze by měly odrážet zavedené postupy a měly by být v příslušných odvětvích obecně uznávány. S cílem zajistit, aby nekvalifikovaní poskytovatelé služeb vytvářejících důvěru řídili právní, obchodní, provozní a jiná přímá či nepřímá rizika spojená s poskytováním nekvalifikovaných služeb vytvářejících důvěru v souladu s čl. 19a odst. 1 nařízení (EU) č. 910/2014, by nekvalifikovaní poskytovatelé služeb vytvářejících důvěru měli splňovat odkazované prvky norem, jak jsou uvedeny v příloze, a požadavky na řízení rizik stanovené v tomto nařízení pro předpoklad shody.

(4) Pokud nekvalifikovaný poskytovatel služeb vytvářejících důvěru dodržuje požadavky stanovené v tomto prováděcím nařízení, měly by orgány dohledu předpokládat shodu s příslušnými požadavky nařízení (EU) č. 910/2014. Nekvalifikovaný poskytovatel služeb vytvářejících důvěru však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

(5) Aby bylo zajištěno, že identifikovaná rizika jsou náležitě řešena, měly by politiky řízení rizik, kterými se nekvalifikovaní poskytovatelé služeb vytvářejících důvěru řídí, zahrnovat postupy pro dokumentaci a hodnocení rizik, jakož i pro identifikaci, výběr a provádění vhodných opatření k ošetření rizik. Provádění opatření k ošetření rizik by mělo být průběžně monitorováno. Pokud jde o informace, které nekvalifikovaní poskytovatelé služeb vytvářejících důvěru zaznamenávají a uchovávají v rámci svých opatření k ošetření rizik, měli by nekvalifikovaní poskytovatelé služeb vytvářejících důvěru zajistit integritu a důvěrnost těchto údajů. Kromě toho by nekvalifikovaní poskytovatelé služeb vytvářejících důvěru měli v zájmu zvýšení transparentnosti a podpory činností dohledu zveřejňovat metody ověřování totožnosti, které používají. Vzhledem k tomu, že ne všechna identifikovaná rizika mohou být plně vyřešena jejich vyloučením, zmírněním nebo převedením na jiné subjekty, měla by být veškerá zbytková rizika schválena řídicími orgány nekvalifikovaných poskytovatelů služeb vytvářejících důvěru. Kritéria pro přijetí zbytkových rizik by měla být srozumitelně odůvodněna.

(6) Komise pravidelně posuzuje nové technologie, postupy, normy nebo technické specifikace. V souladu se 75. bodem odůvodnění nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([4]) by Komise měla toto prováděcí nařízení přezkoumávat a v případě potřeby ho aktualizovat, aby bylo v souladu s globálním vývojem, novými technologiemi, postupy, normami či technickými specifikacemi a aby byly dodržovány osvědčené postupy na vnitřním trhu.

(7) Na činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([5]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([6]).

(8) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([7]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 8. srpna 2025 ([8]).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

([8]) Formální připomínky EIOÚ k návrhu prováděcího nařízení, pokud jde o specifikace a postupy pro řízení rizik spojených s poskytováním nekvalifikovaných služeb vytvářejících důvěru | evropský inspektor ochrany údajů.

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

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Referenční normy

Referenční normy podle čl. 19a odst. 2 nařízení (EU) č. 910/2014 jsou uvedeny v příloze tohoto nařízení.

Článek 2

Politiky řízení rizik

1. Politiky řízení rizik uvedené v čl. 19a odst. 1 nařízení (EU) č. 910/2014 jasně identifikují služby vytvářející důvěru, na něž se vztahují, jsou specifické pro dané služby vytvářející důvěru a jsou schváleny řídicím orgánem nekvalifikovaného poskytovatele služeb vytvářejících důvěru.

2. Politiky řízení rizik zahrnují alespoň všechny tyto prvky:

a) celkovou míru tolerance rizika v souladu s kritičností a požadovanou úrovní bezpečnosti služeb vytvářejících důvěru s ohledem na nejnovější technologický vývoj;

b) příslušná kritéria rizik, mimo jiné včetně pravděpodobnosti, dopadu a úrovně rizika, s přihlédnutím k operativním informacím o kybernetických hrozbách a zranitelnostem;

c) přístup k identifikaci a dokumentaci rizik spojených s poskytováním služeb vytvářejících důvěru, přičemž se zohlední celý rozsah informačního systému používaného nekvalifikovaným poskytovatelem služeb vytvářejících důvěru, včetně rizik spojených se složkami systému a se všemi aktivními nebo pasivními stranami zapojenými do uplatňování systému nebo do poskytování služeb vytvářejících důvěru;

d) proces hodnocení identifikovaných rizik na základě kritérií rizik uvedených v písmeni b);

e) proces identifikace, stanovení priorit a průběžného sledování provádění vhodných opatření k ošetření rizik;

f) proces průběžného sledování provádění politik řízení rizik.

3. Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru stanoví vhodné postupy a uchovávají dokumenty, aby zajistili provádění požadavků stanovených v příslušných právních předpisech.

4. Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru stanoví vhodné dokumentované postupy, které zajišťují sledování legislativních a regulačních změn na unijní a vnitrostátní úrovni, které mohou mít dopad na poskytování služeb vytvářejících důvěru.

Článek 3

Identifikace, dokumentace a hodnocení rizik

Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru identifikují, dokumentují a vyhodnocují všechna rizika uvedená v čl. 19a odst. 1 nařízení (EU) č. 910/2014 v souladu s politikami řízení rizik uvedenými v článku 2, a zejména:

a) identifikují rizika ve vztahu ke třetím stranám;

b) identifikují potenciální jediný bod selhání při poskytování služeb vytvářejících důvěru;

c) vyhodnocují identifikovaná rizika na základě kritérií rizik uvedených v čl. 2 odst. 2 písm. b).

Článek 4

Opatření k ošetření rizik

1. V souladu s politikami uvedenými v článku 2 nekvalifikovaní poskytovatelé služeb vytvářejících důvěru plánují, dokumentují a provádějí opatření k ošetření rizik a plní zejména tyto úkoly:

a) identifikují vhodná opatření k ošetření rizik a stanovují priority těchto opatření;

b) vybírají, schvalují a dokumentují vybraná opatření k ošetření rizik, včetně jejich bezpečnostních požadavků a provozních postupů, v plánu ošetření rizik a určují, kdo je odpovědný za provedení opatření k ošetření rizik a kdy mají být provedena;

c) průběžně sledují provádění opatření k ošetření rizik.

2. Plán ošetření rizik stanovený v odst. 1 písm. b) srozumitelně odůvodní přijetí zbytkových rizik.

3. V rámci opatření k ošetření rizik uvedených v odstavci 1 nekvalifikovaní poskytovatelé služeb vytvářejících důvěru rovněž:

a) v příslušných případech ověřují totožnost uživatelů služby vytvářející důvěru přímo nebo prostřednictvím třetí strany a zveřejňují informace o použitých metodách ověřování totožnosti;

b) pro účely poskytnutí důkazů v soudním řízení a zajištění kontinuity služeb zaznamenávají a bezpečně uchovávají po dobu nezbytnou v souladu s právními předpisy Unie nebo vnitrostátními právními předpisy, a to i po ukončení činnosti nekvalifikovaného poskytovatele služeb vytvářejících důvěru, tyto informace:

   — veškeré relevantní informace shromážděné v rámci procesu registrace a onboardingu uživatelů služeb vytvářejících důvěru, v příslušných případech včetně ověření totožnosti uživatelů,

   — v příslušných případech autentizační údaje přidělené uživateli služby vytvářející důvěru a

   — jakoukoli změnu statusu certifikátů veřejného klíče nebo jiného kryptografického materiálu používaného při poskytování služby vytvářející důvěru;

c) v příslušných případech zajišťují, aby autentizační údaje přidělené uživateli služby vytvářející důvěru byly jedinečné.

4. Při identifikaci, výběru, schvalování a stanovení priorit vhodných opatření k ošetření rizik nekvalifikovaní poskytovatelé služeb vytvářejících důvěru zohledňují tyto prvky:

a) výsledky hodnocení rizik uvedeného v článku 3;

b) účinnost opatření k ošetření rizik;

c) posouzení shody;

d) významné incidenty;

e) náklady na provádění ve vztahu k očekávanému přínosu;

f) příslušnou vhodnou klasifikaci aktiv;

g) analýzu obchodního dopadu rizik identifikovaných v souladu s článkem 3.

5. Řídicí orgány nekvalifikovaných poskytovatelů služeb vytvářejících důvěru schvalují zbytková rizika, která zůstávají po provedení opatření k ošetření rizik, jak je stanoveno v plánu ošetření rizik.

6. Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru přezkoumávají, dokumentují a v příslušných případech aktualizují výsledky hodnocení rizik a plán ošetření rizik v plánovaných intervalech – a alespoň jednou ročně – a v případě, že dojde k významným změnám infrastruktury, operací nebo rizik či k významným incidentům.

7. Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru zajistí dostupnost, integritu a důvěrnost informací uvedených v odst. 3 písm. b).

Článek 5

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 27. října 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA

Seznam referenčních norem pro nekvalifikované poskytovatele služeb vytvářejících důvěru

Platí požadavky podle těchto bodů normy ETSI EN 319 401 V3.1.1 (2024-06): „Elektronické podpisy a důvěryhodné infrastruktury (ESI) – Obecné požadavky politiky pro poskytovatele důvěryhodných služeb“:

5. Posouzení rizik;
6. Politiky a postupy;
7.1 Vnitřní organizace;
7.2 Lidské zdroje;
7.3 Správa aktiv;
7.4 Kontrola přístupu;
7.6 Fyzická a environmentální bezpečnost.