2025/2532

17.12.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/2532

ze dne 16. prosince 2025,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy a specifikace pro kvalifikované služby elektronické archivace

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. 45j odst. 2 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nařízením Evropského parlamentu a Rady (EU) 2024/1183 ([2]) byl do nařízení (EU) č. 910/2014 zařazen seznam nových služeb vytvářejících důvěru a kvalifikovaných služeb vytvářejících důvěru, včetně kvalifikované služby elektronické archivace. Komise má stanovit seznam referenčních norem a v případě potřeby stanovit specifikace pro uvedené služby.

(2) Elektronická archivace je služba pro přijímání, uchovávání, zpřístupnění a výmaz elektronických dat a elektronických dokumentů s cílem zajistit jejich trvanlivost a čitelnost, jakož i zachovat jejich integritu, důvěrnost a důkaz původu po celou dobu uchovávání. Kvalifikované služby elektronické archivace hrají v digitálním podnikatelském prostředí klíčovou roli, neboť podporují přechod od tradičních postupů založených na papírových dokumentech k rovnocenným elektronickým postupům. Aby bylo zajištěno, že si elektronická data a elektronické dokumenty uchovají předpoklad své integrity a původu po celou dobu uchovávání kvalifikovaným poskytovatelem služeb vytvářejících důvěru, a aby bylo dosaženo vysoké úrovně transparentnosti a důvěry mezi všemi účastníky zapojenými do životního cyklu informací, je nezbytné stanovit společný soubor specifikací pro kvalifikované služby elektronické archivace.

(3) Aby se zvýšila důkazní síla, bezpečnost a důvěryhodnost kvalifikovaných služeb elektronické archivace, měly by se v případech, kdy se k vytváření, podepisování, pečetění nebo potvrzení data a času, například pokud jde o archivaci důkazů, důkazní záznamy, záznamy o událostech, záznamy o správném provedení postupů nebo zprávy potvrzující archivaci, používají elektronické podpisy, elektronické pečetě nebo elektronická časová razítka, používat kvalifikované služby vytvářející důvěru.

(4) Předpoklad shody stanovený v čl. 45j odst. 2 nařízení (EU) č. 910/2014 by se měl uplatnit pouze v případě, že kvalifikované služby elektronické archivace splňují požadavky stanovené v tomto nařízení. Referenční normy pro kvalifikované služby elektronické archivace by měly odrážet zavedené postupy a měly by být široce uznávány v příslušných odvětvích. Měly by být upraveny tak, aby zahrnovaly další opatření zajišťující bezpečnost a důvěryhodnost kvalifikovaných služeb elektronické archivace.

(5) Pokud poskytovatel služeb vytvářejících důvěru splňuje požadavky stanovené v tomto nařízení, měly by orgány dohledu předpokládat shodu s příslušnými požadavky nařízení (EU) č. 910/2014 a tento předpoklad řádně zohlednit při udělování nebo potvrzování kvalifikovaného statusu služby vytvářející důvěru. Kvalifikovaný poskytovatel služeb vytvářejících důvěru však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

(6) Aby byla zachována integrita a důkaz původu elektronických dat a elektronických dokumentů obsahujících jeden nebo více kvalifikovaných elektronických podpisů nebo pečetí, měly by kvalifikované služby elektronické archivace používat postupy a technologie schopné prodloužit důvěryhodnost těchto elektronických podpisů a pečetí i po uplynutí doby technické platnosti, přinejmenším po celou dobu uchovávání.

([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) 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).

(7) Komise pravidelně posuzuje nové technologie, postupy, normy nebo technické specifikace. V souladu se 75. bodem odůvodnění nařízení (EU) 2024/1183 by Komise měla toto 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.

(8) Na činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([3]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([4]).

(9) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([5]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 21. října 2025 ([6]).

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

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Elektronická archivace dokumentů opatřených kvalifikovaným elektronickým podpisem nebo kvalifikovanou elektronickou pečetí

1. Při archivaci elektronických dat nebo elektronických dokumentů, které obsahují kvalifikované elektronické podpisy nebo kvalifikované elektronické pečetě, poskytovatelé kvalifikovaných služeb elektronické archivace zajistí, aby byla zachována důvěryhodnost těchto kvalifikovaných elektronických podpisů nebo kvalifikovaných elektronických pečetí i po uplynutí doby jejich technické platnosti a aby byla zachována integrita a přesnost původu kvalifikovaných elektronických podpisů a pečetí, a to alespoň do konce zákonné nebo smluvní doby uchovávání.

2. Pro účely odstavce 1 mohou poskytovatelé kvalifikovaných služeb elektronické archivace využívat kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů nebo kvalifikovanou službu uchovávání kvalifikovaných elektronických pečetí.

Článek 2

Referenční normy a specifikace pro poskytování kvalifikovaných služeb elektronické archivace

Referenční normy a specifikace uvedené v čl. 45j odst. 2 nařízení (EU) č. 910/2014 jsou stanoveny v příloze tohoto nařízení.

([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).

([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]) 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]) Formální připomínky EIOÚ k návrhu prováděcího nařízení, kterým se stanoví prováděcí pravidla k nařízení (EU) č. 910/2014, pokud jde o referenční normy a specifikace kvalifikované služby elektronické archivace.

Článek 3

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 16. prosince 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA

Seznam referenčních norem a specifikací pro kvalifikované služby elektronické archivace

Norma CEN/TS 18170:2025 („CEN/TS 18170“) se použije s těmito úpravami:

a) Normativní odkazy (bod 2)

— ETSI EN 319 401 V3.1.1 (2024-06), „*Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers*“ (Elektronické podpisy a infrastruktury (ESI); Obecné politické požadavky na poskytovatele služeb vytvářejících důvěru).

— ETSI EN 319 421 V1.3.1 (2025-07), „*Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*“ (Elektronické podpisy a infrastruktury (ESI); Politické a bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru vydávající certifikáty; Část 1: Obecné požadavky).

— ISO 14721:2025, „*Space Data System Practices — Reference model for an open archival information system (OAIS)*“ (Postupy pro systém přenosu dat z kosmického prostoru – Referenční model pro otevřený archivační informační systém (OAIS)).

— ACM-ECCG, Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“ zveřejněné Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA).

— Prováděcí nařízení Komise (EU) 2024/482 ([1]).

— Prováděcí nařízení Komise (EU) 2024/3144 ([2]).

— ISO/IEC 15408:2022 (části 1 až 5), „*Information security, cybersecurity and privacy protection – Evaluation criteria for IT security*“ (Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT).

— FIPS PUB 140-3 (2019), „*Security Requirements for Cryptographic Modules*“ (Bezpečnostní požadavky na kryptografické moduly).

b) Prohlášení o zásadách a postupech (bod 6.1)

— Použijí se požadavky stanovené v normě CEN/TS 18170, bodě 6.1.

— Použijí se požadavky stanovené v normě ETSI EN 319 401, bodě 5.

— Poskytovatel služby elektronické archivace vytvářející důvěru (EATSP) zavede postupy, kterými se orgánu dohledu oznamují veškeré změny v poskytování služby elektronické archivace vytvářející důvěru a záměr ukončit tyto činnosti, a to v souladu s podnikatelskými požadavky a příslušnými právními předpisy, též v souladu s požadavky prováděcích aktů přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014 [i.2].

— EATSP informuje příslušný orgán dohledu alespoň:

  — jeden měsíc před provedením jakékoli změny,

  — tři měsíce před plánovaným ukončením poskytování služby vytvářející důvěru.

c) Podmínky (bod 6.2)

— Použijí se požadavky stanovené v normě CEN/TS 18170, bodě 6.2.

— Účastníci a strany spoléhající se na službu elektronické archivace vytvářející důvěru musí být před uzavřením smluvního vztahu jasným, úplným a snadno přístupným způsobem, ve veřejně přístupném prostoru a jednotlivě informováni o přesných podmínkách.

([1]) Prováděcí nařízení Komise (EU) 2024/482 ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC) (Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Prováděcí nařízení Komise (EU) 2024/3144 ze dne 18. prosince 2024, kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o použitelné mezinárodní normy, a kterým se uvedené prováděcí nařízení opravuje (Úř. věst. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

d) Lidské zdroje (bod 7.3)

— Použijí se požadavky stanovené v normě CEN/TS 18170, bodě 7.3.

— Pracovníci EATSP na důvěryhodných pozicích a v příslušných případech jeho subdodavatelé na důvěryhodných pozicích musí být schopni splnit požadavek na „odborné znalosti, zkušenosti a kvalifikaci“ prostřednictvím formální odborné přípravy a osvědčení, skutečných zkušeností, nebo kombinace obojího. To zahrnuje pravidelné (alespoň každých dvanáct měsíců) aktualizace pokrývající nové hrozby a aktuální bezpečnostní postupy.

e) Kryptografická opatření a monitorování (bod 7.6)

— Systém archivace musí zaručit důvěrnost dat a dokumentů během celého životního cyklu archivu od uložení až po skartaci.

— Použijí se požadavky stanovené v normě ETSI EN 319 401, bodě 7.5 „Kryptografická opatření“.

— EATSP určí původ dat, která mají být archivována v elektronickém archivačním systému. Pokud k tomu používá elektronické podpisy nebo elektronické pečetě, musí být tyto elektronické podpisy nebo elektronické pečetě kvalifikované.

— Pokud EATSP digitálně podepíše digitální předmět nebo záznam (nebo jeho část), musí být soukromý podpisový klíč EATSP uchováván a používán buď v rámci kvalifikovaného prostředku pro vytváření elektronických podpisů nebo pečetí, nebo v zabezpečeném kryptografickém prostředku, který je důvěryhodným systémem certifikovaným:

  a) v souladu se společnými kritérii pro hodnocení bezpečnosti informačních technologií stanovenými v normě ISO/IEC 15408 nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verzí CC:2022, částmi 1 až 5, zveřejněnými účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT, a je certifikován na úrovni EAL 4 nebo vyšší, nebo

  b) v souladu s evropským systémem certifikace kybernetické bezpečnosti založeným na společných kritériích (prováděcí nařízení Komise (EU) 2024/482, prováděcí nařízení Komise (EU) 2024/3144) a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

  c) do 31. 12. 2030 v souladu s FIPS PUB 140-3, úrovní 3.

— Tato certifikace musí odpovídat bezpečnostnímu cíli nebo profilu ochrany nebo dokumentaci návrhu modulu a jeho bezpečnosti, které splňují požadavky tohoto dokumentu, vycházet z analýzy rizik a přihlížet k fyzickým a jiným netechnickým bezpečnostním opatřením.

— Pokud je bezpečný kryptografický prostředek certifikován podle systému EUCC (prováděcí nařízení Komise (EU) 2024/482, prováděcí nařízení Komise (EU) 2024/3144), musí být tento prostředek nakonfigurován a používán v souladu s touto certifikací.

— EATSP monitoruje sílu kryptografických algoritmů, které se používaly a používají. V případě domněnky, že jeden z použitých algoritmů nebo parametrů přestane být vhodným, jak je definováno v řízení rizik, EATSP buď aktualizuje příslušnou politiku archivace, nebo vytvoří nový profil archivace, aby mohl nakládat s balíčky archivních informací (AIP) a definovat a provést vhodná opatření.

— Hodnocení kryptografických algoritmů a způsobu jejich používání, které provádí EATSP, musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA (ACM-ECCG).

— Technické komponenty služby elektronické archivace vytvářející důvěru (EATS) se před komunikací navzájem autentizují na základě kryptografických technik.

f) Síť (bod 7.9)

— Použijí se požadavky stanovené v normě ETSI EN 319 401, bodě 7.8 „Bezpečnost sítí“.

— Skenování zranitelností podle požadavku REQ-7.8-13 normy ETSI EN 319 401 se provádí nejméně jednou za čtvrtletí.

— Penetrační test podle požadavku REQ-7.8-17X normy ETSI EN 319 401 se provádí nejméně jednou ročně.

— Firewally musí být nakonfigurovány tak, aby blokovaly všechny protokoly a přístupy, které nejsou nutné pro provoz EATSP.

g) Shromažďování důkazů (bod 7.11)

— Použijí se požadavky uvedené v bodě 7.10 „Sběr důkazů“ normy ETSI EN 319 401, a to i pro kritické a nekritické události (viz bod 13.2).

h) Ukončení činnosti a plán ukončení činnosti EATSP (bod 7.13)

— Použijí se požadavky stanovené v normě CEN/TS 18170, bodě 7.13.

— Plán ukončení činnosti EATSP musí splňovat požadavky stanovené v prováděcích aktech přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014.

i) Spolehlivý čas událostí (bod 13.3.1)

— Použijí se požadavky stanovené v normě CEN/TS 18170, bodě 13.3.1.

— Používá-li EATSP časová razítka, použije kvalifikované časové razítko.