2024/1183

30.4.2024

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

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru ([1]),

s ohledem na stanovisko Výboru regionů ([2]),

v souladu s řádným legislativním postupem ([3]),

vzhledem k těmto důvodům:

(1) Sdělení Komise ze dne 19. února 2020 nazvané „Formování digitální budoucnosti Evropy“ oznamuje revizi nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([4]) s cílem zlepšit jeho účinnost, rozšířit jeho přínosy na soukromý sektor a podporovat důvěryhodnou digitální identitu pro všechny Evropany.

(2) Evropská rada ve svých závěrech ze zasedání konaného ve dnech 1. a 2. října 2020 vyzvala Komisi, aby navrhla vytvořit celounijní rámec pro bezpečnou veřejnou elektronickou identifikaci zahrnující interoperabilní digitální podpisy, jehož prostřednictvím budou mít lidé kontrolu nad vlastní on-line identitou a údaji, jakož i přístup k veřejným i soukromým a přeshraničním digitálním službám.

(3) Politický program Digitální dekáda 2030 zavedený rozhodnutím Evropského parlamentu a Rady (EU) 2022/2481 ([5]), stanoví obecné a digitální cíle rámce Unie, jež mají do roku 2030 vést k tomu, aby byla v široké míře zavedena důvěryhodná a dobrovolná digitální identita kontrolovaná uživatelem, která je uznávána v celé Unii a umožňuje každému uživateli kontrolovat své údaje v on-line interakcích.

(4) V „evropském prohlášení o digitálních právech a zásadách pro digitální dekádu“ vyhlášeném Evropským parlamentem, Radou a Komisí ([6]) (dále jen „prohlášení“) se zdůrazňuje právo každého jednotlivce na přístup k digitálním technologiím, produktům a službám, které jsou koncipovány tak, aby byly bezpečné, zabezpečené a chránily soukromí. Znamená to mimo jiné zajistit, aby všem lidem žijícím v Unii byla nabídnuta dostupná, bezpečná a důvěryhodná digitální identita, která umožňuje přístup k široké škále on-line i off-line služeb chráněných před riziky v oblasti kybernetické bezpečnosti a kyberkriminality, včetně porušení zabezpečení údajů, krádeže identity nebo manipulace s ní. V prohlášení se rovněž uvádí, že každý má právo na ochranu svých osobních údajů. Toto právo zahrnuje kontrolu toho, jak jsou údaje využívány a s kým jsou sdíleny.

([1]) Úř. věst. C 105, 4.3.2022, s. 81.
([2]) Úř. věst. C 61, 4.2.2022, s. 42.
([3]) Postoj Evropského parlamentu ze dne 29. února 2024 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 26. března 2024.
([4]) 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 (Úř. věst. L 257, 28.8.2014, s. 73).
([5]) Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030 (Úř. věst. L 323, 19.12.2022, s. 4).
([6]) Úř. věst. C 23, 23.1.2023, s. 1.

(5) Občané Unie a rezidenti v Unii by měli mít právo na digitální identitu, která je pod jejich výhradní kontrolou a která jim umožňuje vykonávat jejich práva v digitálním prostředí a podílet se na digitální ekonomice. K dosažení tohoto cíle by měl být vytvořen evropský rámec pro digitální identitu, který občanům Unie a rezidentům v Unii umožní přístup k veřejným a soukromým on-line i off-line službám v celé Unii.

(6) Harmonizovaný rámec pro digitální identitu by měl přispět k vytvoření digitálně integrovanější Unie tím, že sníží digitální překážky mezi členskými státy a umožní občanům Unie a rezidentům v Unii využívat výhod digitalizace a zároveň zvýší transparentnost a ochranu jejich práv.

(7) Harmonizovanější přístup k elektronické identifikaci by měl snížit rizika a náklady spojené se současnou roztříštěností, jejíž příčinou je používání odlišných vnitrostátních řešení nebo skutečnost, že v některých členských státech tato řešení elektronické identifikace chybí. Tento přístup by měl posílit vnitřní trh tím, že umožní občanům Unie, rezidentům v Unii ve smyslu vnitrostátního práva a podnikům identifikovat se a provést autentizaci své totožnosti v on-line a v off-line prostředí v celé Unii bezpečným, důvěryhodným, uživatelsky přívětivým, pohodlným, dostupným a harmonizovaným způsobem. Evropská peněženka digitální identity by měla fyzickým a právnickým osobám v celé Unii poskytnout harmonizovaný prostředek pro elektronickou identifikaci umožňující provádět autentizaci údajů spojených s jejich totožností a sdílet je. Každý by měl mít bezpečný přístup k veřejným a soukromým službám založeným na zdokonaleném ekosystému služeb vytvářejících důvěru a na ověřených dokladech totožnosti a elektronických potvrzeních atributů, jako jsou akademické kvalifikace, včetně vysokoškolských diplomů nebo jiných dosažených forem vzdělání či odborné kvalifikace. Evropský rámec pro digitální identitu má dosáhnout přechodu od závislosti pouze na vnitrostátních řešeních v oblasti digitální identity k poskytování elektronických potvrzení atributů platných a právně uznávaných v celé Unii. Poskytovatelé elektronických potvrzení atributů by měli mít prospěch z jasného a jednotného souboru pravidel, zatímco orgány veřejné správy by měly mít možnost používat elektronické dokumenty v daném formátu.

(8) Několik členských států zavedlo a používá prostředky pro elektronickou identifikaci, které jsou poskytovateli služeb v Unii akceptovány. Kromě toho byly na základě nařízení (EU) č. 910/2014 investovány prostředky do vnitrostátních i přeshraničních řešení, včetně interoperability oznámených systémů elektronické identifikace podle uvedeného nařízení. V zájmu zajištění doplňkovosti a rychlého přijetí evropských peněženek digitální identity stávajícími uživateli oznámených prostředků pro elektronickou identifikaci a v zájmu minimalizace dopadu na stávající poskytovatele služeb se očekává, že evropské peněženky digitální identity budou využívat zkušeností získaných se stávajícími prostředky pro elektronickou identifikaci a infrastruktury oznámených systémů elektronické identifikace zavedené na úrovni Unie a na vnitrostátní úrovni.

(9) Na všechny činnosti zpracování osobních údajů podle nařízení (EU) č. 910/2014 se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([7]) a případně směrnice Evropského parlamentu a Rady 2002/58/ES ([8]). Řešení spadající do rámce interoperability stanoveného v tomto nařízení jsou s těmito pravidly rovněž v souladu. Právní předpisy Unie v oblasti ochrany údajů stanoví zásady ochrany údajů, jako je zásada minimalizace údajů a účelového omezení a povinnosti, jako je záměrná a standardní ochrana údajů.

(10) S cílem podpořit konkurenceschopnost podniků v Unii by měli mít poskytovatelé on-line i off-line služeb možnost spoléhat se na řešení v oblasti digitální identity uznávaná v celé Unii, bez ohledu na to, ve kterém členském státě jsou tato řešení poskytována, a těžit tak z harmonizovaného unijního přístupu k důvěře, bezpečnosti a interoperabilitě. Uživatelé i poskytovatelé služeb by měli mít prospěch z toho, že jsou elektronickým potvrzením atributů přiznány stejné právní účinky v celé Unii. Harmonizovaný rámec pro digitální identitu má vytvářet ekonomickou hodnotu poskytováním snadnějšího přístupu ke zboží a službám a výrazným snížením provozních nákladů spojených s postupy elektronické identifikace a autentizace, například při zapojování nových zákazníků, a omezením potenciálního prostoru pro kyberkriminalitu, jako jsou krádeže identity, krádeže údajů a podvody on-line, čímž podpoří úspory na základě vyšší efektivity a bezpečnou digitální transformaci mikropodniků a malých a středních podniků v Unii.

([7]) 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).

([8]) 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).

(11) Evropské peněženky digitální identity by měly usnadnit uplatňování zásady „pouze jednou“, a tím snížit administrativní zátěž a podpořit přeshraniční mobilitu občanů Unie a rezidentů v Unii a podniků v celé Unii a podpořit rozvoj interoperabilních služeb elektronické veřejné správy v celé Unii.

(12) Zpracovávání osobních údajů při provádění tohoto nařízení se řídí nařízením (EU) 2016/679, nařízením Evropského parlamentu a Rady (EU) 2018/1725 ([9]) a směrnicí 2002/58/ES. Toto nařízení by proto mělo stanovit zvláštní záruky, které poskytovatelům prostředků pro elektronickou identifikaci a elektronického potvrzování atributů zabrání kombinovat osobní údaje získané při poskytování jiných služeb s osobními údaji zpracovávanými za účelem poskytování služeb, jež spadají do oblasti působnosti tohoto nařízení. Osobní údaje týkající se poskytování evropské peněženky digitální identity by měly být uchovávány logicky odděleně od jakýchkoli jiných dat v držení poskytovatele evropské peněženky digitální identity. Toto nařízení by poskytovatelům evropských peněženek digitální identity nemělo bránit v uplatňování dodatečných technických opatření, která přispívají k ochraně osobních údajů, jako je fyzické oddělení osobních údajů týkajících se poskytování evropských peněženek digitální identity od jakýchkoli jiných dat v držení poskytovatele. Aniž je dotčeno nařízení (EU) 2016/679, toto nařízení podrobněji upřesňuje uplatňování zásad účelového omezení, minimalizace údajů a záměrné a standardní ochrany údajů.

(13) Evropské peněženky digitální identity by měly mít koncepčně zabudovanou funkci společného přehledu, aby byla zajištěna vyšší míra transparentnosti, soukromí a kontroly ze strany uživatelů nad jejich osobními údaji. Tato funkce by měla poskytovat snadný a uživatelsky přívětivý přehled o všech spoléhajících se stranách, s nimiž uživatel sdílí údaje, včetně atributů, a o druhu údajů sdílených s každou spoléhající se stranou. Měla by uživatelům umožnit sledovat všechny transakce provedené prostřednictvím evropské peněženky digitální identity, a to alespoň pokud jde o následující údaje: čas a datum transakce, identifikace protistrany, požadované osobní údaje a sdílené údaje. Tyto informace by měly být uloženy, i když transakce nebyla uzavřena. Nemělo by být možné vyvrátit pravost informací obsažených v historii transakce. Taková funkce by měla být standardně nastavena jako aktivní. Uživatelé by měli mít možnost snadno požádat o okamžité vymazání osobních údajů podle článku 17 nařízení (EU) 2016/679 spoléhající se stranou a snadno nahlásit spoléhající se stranu příslušnému vnitrostátnímu úřadu pro ochranu osobních údajů, pokud obdrží údajně protiprávní nebo podezřelou žádost o osobní údaje, a to přímo prostřednictvím evropské peněženky digitální identity.

(14) Členské státy by měly do evropské peněženky digitální identity začlenit různé technologie na ochranu soukromí, jako je důkaz s nulovou znalostí. Tyto kryptografické metody by měly spoléhající se straně umožnit ověřit, zda je dané tvrzení založené na osobních identifikačních údajích a potvrzení atributů pravdivé, a to aniž by byly odhaleny jakékoliv údaje, na nichž je uvedené prohlášení založeno, čímž je chráněno soukromí uživatele.

(15) Toto nařízení stanoví harmonizované podmínky pro vytvoření rámce pro evropské peněženky digitální identity poskytované členskými státy. Všichni občané Unie a rezidenti v Unii ve smyslu vnitrostátních právních předpisů by měli mít možnost bezpečně požadovat, vybírat, kombinovat, uchovávat, mazat, sdílet a předkládat údaje týkající se jejich identity a požádat o vymazání svých osobních údajů, a to uživatelsky přívětivým a pohodlným způsobem, pod výhradní kontrolou uživatele, přičemž by mělo být umožněno výběrové zpřístupňování osobních údajů. Toto nařízení odráží sdílené evropské hodnoty a respektuje základní práva, právní záruky a odpovědnost, a chrání tak demokratickou společnost, občany Unie a rezidenty v Unii. Technologie používané k dosažení těchto cílů by měly být vyvinuty tak, aby bylo dosaženo nejvyšší úrovně bezpečnosti, soukromí, uživatelské přívětivosti, přístupnosti, široké použitelnosti a bezproblémové interoperability. Členské státy by měly všem svým občanům a rezidentům zajistit rovný přístup k elektronické identifikaci. Členské státy by neměly přímo ani nepřímo omezovat přístup k veřejným nebo soukromým službám fyzickým či právnickým osobám, které se rozhodly evropskou peněženku digitální identity nepoužívat, a měly by zpřístupnit vhodná alternativní řešení.

([9]) 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).

(16) Členské státy by měly využít možností nabízených tímto nařízením k tomu, aby na svou odpovědnost poskytovaly evropské peněženky digitální identity pro použití fyzickými a právnickými osobami s bydlištěm na jejich území. S cílem poskytnout členským státům flexibilitu a využít špičkových technologií by toto nařízení mělo umožnit poskytování evropských peněženek digitální identity přímo členským státem, na základě pověření členského státu nebo nezávisle na členském státě, avšak uznané tímto členským státem.

(17) Pro účely registrace by spoléhající se strany měly poskytnout informace nezbytné k jejich elektronické identifikaci a autentizaci pro účely evropské peněženky digitální identity. Při prohlášení o zamýšleném použití evropské peněženky digitální identity by spoléhající se strany měly poskytnout informace o údajích, které budou případně požadovat za účelem poskytování svých služeb, a o důvodech žádosti. Registrace spoléhající se strany usnadňuje členským státům ověřování souladu činností spoléhajících se stran s právem Unie. Povinností registrace stanovenou v tomto nařízení by neměly být dotčeny povinnosti stanovené v jiných unijních nebo vnitrostátních právních předpisech, jako jsou informace, které mají být poskytnuty subjektům údajů podle nařízení (EU) 2016/679. Spoléhající se strany by měly dodržovat záruky stanovené v článcích 35 a 36 uvedeného nařízení, zejména prováděním posouzení vlivu na ochranu údajů a tím, že před zpracováním údajů konzultují příslušné úřady pro ochranu osobních údajů, pokud z posouzení dopadu na ochranu údajů vyplyne, že by zpracování vedlo k vysokému riziku. Tyto záruky by měly podporovat zákonné zpracování osobních údajů spoléhajícími se stranami, zejména pokud jde o zvláštní kategorie údajů, jako jsou údaje o zdravotním stavu. Registrace spoléhajících se stran má zvýšit transparentnost a důvěru, pokud jde o používání evropských peněženek digitální identity. Registrace by měla být nákladově efektivní a přiměřená souvisejícím rizikům, aby se zajistilo přijetí ze strany poskytovatelů služeb. V této souvislosti by registrace měla umožňovat používání automatizovaných postupů, včetně spoléhání se na stávající rejstříky ze strany členských států a jejich využívání těmito členskými státy, a neměl by se uplatňovat postup předběžného povolení. Proces registrace by měl umožňovat různé případy použití, které se mohou lišit co do provozního režimu – on-line/off-line – nebo požadavku na autentizaci zařízení pro účely interakce s evropskou peněženkou digitální identity. Registrace by se měla vztahovat výhradně na spoléhající se strany poskytující služby prostřednictvím digitální interakce.

(18) Ochrana občanů Unie a rezidentů v Unii před neoprávněným nebo podvodným používáním evropských peněženek digitální identity má velký význam pro zajištění důvěry v evropské peněženky digitální identity a jejich široké využívání. Uživatelům by měla být proti zneužití poskytnuta účinná ochrana. Zejména pokud vnitrostátní justiční orgán zjistí v rámci jiného postupu skutečnosti, které zakládají skutkovou podstatu podvodného nebo jinak nezákonného použití evropské peněženky digitální identity, měly by orgány dohledu, které jsou odpovědné za vydavatele evropské peněženky digitální identity, po oznámení přijmout nezbytná opatření k zajištění toho, aby registrace spoléhající se strany a začlenění spoléhajících se stran do mechanismu autentizace byly zrušeny nebo pozastaveny, dokud oznamující orgán nepotvrdí, že zjištěné nesrovnalosti byly napraveny.

(19) Všechny evropské peněženky digitální identity by měly uživatelům umožnit jejich přeshraniční elektronickou identifikaci a autentizaci on-line a v off-line režimu, aby měli přístup k široké škále veřejných a soukromých služeb. Aniž jsou dotčeny výsady členských států s ohledem na identifikaci jejich občanů a rezidentů, mohou evropské peněženky digitální identity rovněž sloužit institucionálním potřebám orgánů veřejné správy, mezinárodních organizací a orgánů, institucí a jiných subjektů Unie. Autentizace v off-line režimu má význam v mnoha odvětvích, včetně zdravotnictví, kde jsou služby často poskytovány prostřednictvím osobního kontaktu a při ověřování pravosti elektronických předpisů by mělo být možné využívat QR kódy nebo podobné technologie. Evropské peněženky digitální identity, které se v rámci systému elektronické identifikace spoléhají na vysokou úroveň záruky, by měly využít potenciálu, který nabízejí řešení odolná proti neoprávněné manipulaci, jako jsou bezpečnostní prvky, aby byly v souladu s bezpečnostními požadavky podle tohoto nařízení. Evropské peněženky digitální identity by rovněž měly uživatelům umožnit vytvářet a používat kvalifikované elektronické podpisy a pečetě, které jsou přijímány v celé Unii. Jakmile se fyzické osoby zapojí do používání evropské peněženky digitální identity, měly by mít možnost ji standardně a bezplatně používat k podpisu kvalifikovaným elektronickým podpisem, a to bez nutnosti absolvovat další administrativní postupy. Uživatelé by měli mít možnost podepisovat nebo pečetit vlastní prohlášení nebo atributy. V zájmu zjednodušení a snížení nákladů pro osoby a podniky v celé Unii, mimo jiné umožněním pravomocí k zastupování a elektronických mandátů, by členské státy měly poskytovat evropské peněženky digitální identity založené na společných normách a technických specifikacích s cílem zajistit bezproblémovou interoperabilitu a přiměřené zvýšení bezpečnosti IT a posílit odolnost proti kybernetickým útokům, a tím výrazně snížit potenciální rizika probíhající digitalizace pro občany Unie, rezidenty v Unii a podniky. Pouze příslušné orgány

členských států mohou při zjišťování totožnosti osoby poskytnout vysokou úroveň spolehlivosti, a tedy poskytnout záruku, že osoba, která uvádí nebo uplatňuje určitou totožnost, je skutečně osobou, kterou tvrdí, že je. Při poskytování evropských peněženek digitální identity je proto nutné spoléhat na právní identitu občanů Unie, rezidentů v Unii nebo právnických osob. Spoléhání se na právní identitu by nemělo uživatelům evropské peněženky digitální identity bránit v přístupu ke službám prostřednictvím pseudonymů, pokud nebyl pro účely autentizace stanoven právní požadavek uvádět právní identitu. Důvěra v evropské peněženky digitální identity by se posílila, kdyby vydávající strany a správci byli povinni zavést vhodná technická a organizační opatření k zajištění nejvyšší úrovně bezpečnosti odpovídající rizikům, která představují pro práva a svobody fyzických osob, v souladu s nařízením (EU) 2016/679.

(20) Používání kvalifikovaného elektronického podpisu pro neprofesionální účely by mělo být pro všechny fyzické osoby bezplatné. Členské státy by měly mít možnost stanovit opatření, která zabrání bezplatnému používání kvalifikovaných elektronických podpisů fyzickými osobami k profesionálním účelům, a zároveň zajistit, aby veškerá taková opatření byla přiměřená zjištěným rizikům a byla odůvodněná.

(21) Je prospěšné usnadnit zavádění a využívání evropských peněženek digitální identity tím, že se bezproblémově integrují do ekosystému veřejných a soukromých digitálních služeb, které jsou na vnitrostátní, místní nebo regionální úrovni již zavedeny. Za tímto účelem by členské státy měly mít možnost stanovit právní a organizační opatření s cílem zvýšit flexibilitu pro poskytovatele evropských peněženek digitální identity a umožnit dodatečné funkce evropských peněženek digitální identity nad rámec funkcí stanovených v tomto nařízení, mimo jiné zvýšením interoperability se stávajícími vnitrostátními prostředky pro elektronickou identifikaci. Tyto dodatečné funkce by však neměly být na úkor zajišťování hlavních funkcí evropských peněženek digitální identity stanovených v tomto nařízení, ani by neměly vést k upřednostňování stávajících vnitrostátních řešení před evropskou peněženkou digitální identity. Vzhledem k tomu, že tyto dodatečné funkce přesahují rámec tohoto nařízení, nevztahují se na ně ustanovení o přeshraničním spoléhání se na evropské peněženky digitální identity stanovená v tomto nařízení.

(22) Evropské peněženky digitální identity by měly obsahovat funkci pro generování pseudonymů, zvolených a spravovaných uživatelem, pro účely autentizace při přístupu k on-line službám.

(23) V zájmu dosažení vysoké úrovně bezpečnosti a důvěryhodnosti stanoví toto nařízení požadavky na evropské peněženky digitální identity. Soulad evropských peněženek digitální identity s těmito požadavky by měl být certifikován akreditovanými subjekty posuzování shody, jež určí členské státy.

(24) Aby se zabránilo rozdílným přístupům a harmonizovalo se provádění požadavků stanovených tímto nařízením, měla by Komise za účelem certifikace evropských peněženek digitální identity přijmout prováděcí akty, kterými stanoví seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely vyjádření podrobných technických specifikací těchto požadavků. Pokud se na certifikaci shody evropských peněženek digitální identity s příslušnými požadavky na kybernetickou bezpečnost nevztahují stávající schémata certifikace kybernetické bezpečnosti, na něž se odkazuje v tomto nařízení, a pokud jde o jiné požadavky než požadavky na kybernetickou bezpečnost týkající se evropských peněženek digitální identity, členské státy by měly zavést vnitrostátní schémata certifikace podle harmonizovaných požadavků stanovených v tomto nařízení a přijatých podle tohoto nařízení. Členské státy by měly předat návrhy svých vnitrostátních schémat certifikace skupině pro evropskou spolupráci v oblasti digitální identity, která by měla mít možnost vydávat stanoviska a doporučení.

(25) Certifikace shody s požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení by se měla opírat o – jsou-li k dispozici – příslušná evropská schémata certifikace kybernetické bezpečnosti zavedená podle nařízení Evropského parlamentu a Rady (EU) 2019/881 ([10]), kterým se zřizuje dobrovolný evropský rámec pro certifikaci kybernetické bezpečnosti produktů, procesů a služeb IKT.

([10]) 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).

(26) Aby bylo možné průběžně posuzovat a zmírňovat rizika spojená s bezpečností, měly by být certifikované evropské peněženky digitální identity podrobovány pravidelným posouzením zranitelnosti, jejichž cílem je odhalit veškerá zranitelná místa v komponentech evropské peněženky digitální identity souvisejících s certifikovaným produktem, procesem či službou.

(27) Základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení chrání uživatele a podniky před kybernetickými bezpečnostními riziky, a přispívají tak rovněž ke zvýšení ochrany osobních údajů a soukromí jednotlivců. Měly by být zváženy možnosti synergie v oblasti normalizace i certifikace týkající se aspektů kybernetické bezpečnosti, a to prostřednictvím spolupráce mezi Komisí, evropskými normalizačními organizacemi, Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA), Evropským sborem pro ochranu osobních údajů zřízeným nařízením (EU) 2016/679 a vnitrostátními úřady pro ochranu osobních údajů.

(28) Zapojení občanů Unie a rezidentů v Unii do používání evropské peněženky digitální identity (tzv. onboarding) by mělo být usnadněno využitím prostředků pro elektronickou identifikaci vydaných s vysokou úrovní záruky. Prostředky pro elektronickou identifikaci vydané se značnou úrovní záruky by se měly používat pouze tehdy, když harmonizované technické specifikace a postupy používající prostředky pro elektronickou identifikaci vydané se značnou úrovní záruky v kombinaci s doplňkovými prostředky pro ověřování totožnosti umožní splnit požadavky stanovené v tomto nařízení, pokud jde o vysokou úroveň záruky. Tyto doplňkové prostředky by měly být spolehlivé a snadno použitelné, přičemž by mohly být založeny na možnosti používat postupy vzdáleného zapojení do používání, kvalifikované certifikáty kvalifikovaných elektronických podpisů, kvalifikované elektronické potvrzení atributů nebo jejich kombinaci. K zajištění dostatečného rozšíření evropských peněženek digitální identity by měly být v prováděcích aktech stanoveny harmonizované technické specifikace a postupy pro zapojení uživatelů do používání peněženky pomocí prostředků pro elektronickou identifikaci, a to včetně těch, které jsou vydávány se značnou úrovní záruky.

(29) Cílem tohoto nařízení je poskytnout uživateli plně mobilní, bezpečnou a uživatelsky přívětivou evropskou peněženku digitální identity. Jako přechodné opatření do doby, než budou k dispozici certifikovaná řešení odolná proti neoprávněné manipulaci, jako jsou bezpečnostní prvky v zařízeních uživatelů, by evropské peněženky digitální identity měly mít možnost se spoléhat na certifikované externí bezpečnostní prvky pro ochranu kryptografického materiálu a jiných citlivých dat nebo na oznámené prostředky pro elektronickou identifikaci s vysokou úrovní záruky s cílem prokázat soulad s příslušnými požadavky tohoto nařízení, pokud jde o úroveň záruky evropské peněženky digitální identity. Tímto nařízením by neměly být dotčeny vnitrostátní podmínky, pokud jde o vydávání a používání certifikovaného externího bezpečnostního prvku v případě, že se o něj toto přechodné opatření opírá.

(30) Evropské peněženky digitální identity by měly zajišťovat nejvyšší úroveň ochrany údajů a zabezpečení pro účely elektronické identifikace a autentizace s cílem usnadnit přístup k veřejným a soukromým službám bez ohledu na to, zda jsou tyto údaje uchovávány lokálně, nebo v rámci řešení založených na cloudu, a to při náležitém zohlednění různých úrovní rizika.

(31) Evropské peněženky digitální identity by měly být bezpečné již od fáze návrhu a měly by zavést pokročilé bezpečnostní prvky na ochranu před krádeží identity, krádeží dat, odepřením služby a jakoukoli jinou kybernetickou hrozbou. Součástí tohoto zabezpečení by měly být nejmodernější metody šifrování a ukládání, které jsou přístupné pouze uživateli a dešifrovatelné pouze jím, a využívají šifrované komunikace mezi koncovými body s jinými evropskými peněženkami digitální identity a spoléhajícími se stranami. Kromě toho by evropské peněženky digitální identity měly u operací, které jsou jejich prostřednictvím prováděny, vyžadovat bezpečné, výslovné a aktivní potvrzení ze strany uživatelů.

(32) Bezplatné používání evropských peněženek digitální identity by nemělo vést ke zpracování údajů nad rámec toho, co je nezbytné pro poskytování služeb evropské peněženky digitální identity. Toto nařízení by nemělo umožňovat zpracování osobních údajů, které jsou v evropské peněžence digitální identity uložené či jsou výsledkem jejího používání, poskytovatelem evropské peněženky digitální identity pro jiné účely než pro poskytování služeb evropské peněženky digitální identity. V zájmu zajištění soukromí by poskytovatelé evropské peněženky digitální identity měli zajistit tzv. nepozorovatelnost tím, že nebudou shromažďovat údaje a nebudou mít žádný náhled do transakcí uživatelů evropské peněženky digitální identity. Taková nepozorovatelnost znamená, že poskytovatelé nejsou schopni vidět podrobnosti transakcí prováděných uživatelem. Avšak ve zvláštních případech, kdy je udělen předchozí výslovný souhlas uživatele pro každý z těchto konkrétních případů, a v plném souladu s nařízením (EU) 2016/679 by poskytovatelům evropských peněženek digitální identity mohl být udělen přístup k informacím

nezbytným pro poskytování konkrétní služby související s evropskými peněženkami digitální identity.

(33) Transparentnost evropských peněženek digitální identity a odpovědnost jejich poskytovatelů jsou klíčovými prvky potřebnými pro vytvoření společenské důvěry a podmínek příznivých pro akceptování rámce. Fungování evropských peněženek digitální identity by tedy mělo být transparentní a mělo by zejména umožňovat ověřitelné zpracování osobních údajů. Za tímto účelem by členské státy měly zveřejňovat zdrojový kód komponent uživatelského aplikačního softwaru evropských peněženek digitální identity, včetně těch, které souvisejí se zpracováním osobních údajů a údajů právnických osob. Zveřejnění tohoto zdrojového kódu na základě licence otevřeného zdrojového kódu by mělo společnosti, včetně uživatelů a vývojářů, umožnit pochopit jeho fungování a provádět jeho kontrolu a přezkum. Zvýšilo by to důvěru uživatelů v daný ekosystém a bezpečnost evropských peněženek digitální identity tím, že na slabá místa a chyby ve zdrojovém kódu by mohl upozorňovat každý uživatel. Celkově by to měl být pro dodavatele impuls k tomu, aby nabízeli vysoce bezpečný výrobek a jeho bezpečnost udržovali. V některých řádně odůvodněných případech by však zveřejnění zdrojového kódu používaných knihoven, komunikačních kanálů nebo jiných prvků, které nejsou umístěny na uživatelském zařízení, mohly členské státy omezit, zejména z důvodu veřejné bezpečnosti.

(34) Používání evropských peněženek digitální identity, jakož i ukončení jejich používání by mělo být výhradním právem a volbou uživatelů. Členské státy by měly vytvořit jednoduché a bezpečné postupy, které uživatelům umožní požádat o okamžité zrušení platnosti evropské peněženky digitální identity, a to i v případě ztráty nebo odcizení. V případě úmrtí uživatele nebo ukončení činnosti právnické osoby by měl být vytvořen mechanismus, který orgánu odpovědnému za vypořádání dědictví fyzické osoby nebo majetku právnické osoby umožní požádat o okamžité zrušení evropské peněženky digitální identity.

(35) V zájmu podpory zavádění evropských peněženek digitální identity a širšího využívání digitálních identit by členské státy měly nejen propagovat přínosy příslušných služeb, ale také by měly ve spolupráci se soukromým sektorem, výzkumnými pracovníky a akademickou obcí vypracovat vzdělávací programy zaměřené na posílení digitálních dovedností svých občanů a rezidentů, zejména pro zranitelné skupiny, jako jsou osoby se zdravotním postižením a starší osoby. Členské státy by prostřednictvím komunikačních kampaní měly zvyšovat povědomí o přínosech a rizicích evropských peněženek digitální identity.

(36) Aby se zajistilo, že evropský rámec pro digitální identitu bude otevřen inovacím a technologickému rozvoji a obstojí v budoucnosti, jsou členské státy vybízeny k tomu, aby společně zřizovaly zkušební prostředí (tzv. „sandboxy“ čili pískoviště) pro testování inovativních řešení v kontrolovaném a bezpečném prostředí, zejména za účelem zlepšení funkčnosti, ochrany osobních údajů, bezpečnosti a interoperability řešení a vytvářely podklady pro budoucí aktualizace týkající se technických odkazů a právních požadavků. Toto prostředí by mělo podporovat začlenění malých a středních podniků, start-upů a samostatných inovátorů a výzkumných pracovníků, jakož i aktérů z relevantních průmyslových odvětví. Tyto iniciativy by měly přispívat k dodržování právních předpisů a k technické odolnosti evropských peněženek digitální identity, jež mají být poskytovány občanům Unie a rezidentům v Unii, a tento soulad s předpisy a technickou odolnost posilovat, což zamezí vývoji řešení, která nejsou v souladu s právem Unie v oblasti ochrany údajů nebo která jsou z bezpečnostního hlediska zranitelná.

(37) Nařízením Evropského parlamentu a Rady (EU) 2019/1157 ([11]) se od srpna 2021 posiluje zabezpečení průkazů totožnosti prostřednictvím posílených bezpečnostních prvků. Členské státy by měly zvážit proveditelnost jejich oznamování v rámci systémů elektronické identifikace s cílem rozšířit přeshraniční dostupnost prostředků pro elektronickou identifikaci.

(38) Postup oznamování systémů elektronické identifikace by měl být zjednodušen a urychlen s cílem podpořit přístup k pohodlným, důvěryhodným, bezpečným a inovativním řešením v oblasti autentizace a identifikace a případně vyzývat soukromé poskytovatele identity, aby orgánům členského státu nabízeli systémy elektronické identifikace k oznamování jako vnitrostátní systémy elektronické identifikace podle nařízení (EU) č. 910/2014.

([11]) Nařízení Evropského parlamentu a Rady (EU) 2019/1157 ze dne 20. června 2019 o posílení zabezpečení průkazů totožnosti občanů Unie a povolení k pobytu vydávaných občanům Unie a jejich rodinným příslušníkům, kteří vykonávají své právo volného pohybu (Úř. věst. L 188, 12.7.2019, s. 67).

(39) Zjednodušení stávajících postupů oznamování a vzájemného hodnocení zabrání uplatňování nejednotných přístupů k posuzování různých oznámených systémů elektronické identifikace a usnadní budování důvěry mezi členskými státy. Nové, zjednodušené mechanismy mají podporovat spolupráci členských států v oblasti bezpečnosti a interoperability jejich oznámených systémů elektronické identifikace.

(40) Členské státy by měly k zajištění souladu s požadavky tohoto nařízení a příslušných prováděcích aktů přijatých na jeho základě využívat nových a pružných nástrojů. Toto nařízení by mělo členským státům umožnit používat zprávy a posouzení vypracovaná akreditovanými subjekty posuzování shody, jak je stanoveno v kontextu schémat certifikace, které mají být zavedeny na úrovni Unie podle nařízení (EU) 2019/881, na podporu jejich tvrzení o souladu schémat nebo jejich částí s nařízením (EU) č. 910/2014.

(41) Poskytovatelé veřejných služeb používají osobní identifikační údaje dostupné z prostředků pro elektronickou identifikaci podle nařízení (EU) č. 910/2014, aby elektronickou identitu uživatelů z jiného členského státu spárovali s osobními identifikačními údaji poskytnutými těmto uživatelům v členském státě, který provádí postup přeshraničního párování totožnosti. V řadě případů jsou však navzdory použití minimálního souboru údajů poskytnutého v rámci oznámených systémů elektronické identifikace k zajištění přesného spárování totožnosti v případě, že členské státy jednají jako spoléhající se strany, nezbytné dodatečné informace o uživateli a na vnitrostátní úrovni je třeba provést specifické doplňkové postupy jednoznačné identifikace. S cílem intenzivněji podporovat použitelnost prostředků pro elektronickou identifikaci, poskytovat lepší veřejné on-line služby a zvýšit právní jistotu v souvislosti s elektronickou identitou uživatelů by nařízení (EU) č. 910/2014 mělo vyžadovat, aby členské státy přijaly zvláštní on-line opatření k zajištění jednoznačné shody totožnosti v případech, kdy mají uživatelé v úmyslu získat přístup k přeshraničním veřejným on-line službám.

(42) Při vývoji evropských peněženek digitální identity je nezbytné zohlednit potřeby uživatelů. Měly by být k dispozici smysluplné případy použití a on-line služeb, které využívají evropských peněženek digitální identity. V zájmu pohodlí uživatelů a zajištění přeshraniční dostupnosti těchto služeb je důležité přijmout opatření s cílem usnadnit, aby byl ve všech členských státech přijat podobný přístup k navrhování, vývoji a zavádění on-line služeb. K tomu mohou posloužit nezávazné pokyny, v nichž se doporučuje, jak on-line služby spoléhající se na evropské peněženky digitální identity navrhovat, vyvíjet a zavádět. Tyto pokyny by měly být vypracovány s náležitým ohledem na rámec interoperability Unie. Při jejich přijímání by měly hrát vedoucí úlohu členské státy.

(43) V souladu se směrnicí Evropského parlamentu a Rady (EU) 2019/882 ([12]) by osoby se zdravotním postižením měly mít možnost používat evropské peněženky digitální identity, služby vytvářející důvěru a produkty pro koncové uživatele používané při poskytování těchto služeb na stejném základě jako ostatní uživatelé.

(44) V zájmu zajištění účinného prosazování tohoto nařízení by měla být stanovena minimální výše pro maximální výši správních pokut pro kvalifikované i nekvalifikované poskytovatele služeb vytvářejících důvěru. Členské státy by měly stanovit účinné, přiměřené a odrazující sankce. Při stanovování sankcí by měla být náležitě zohledněna velikost dotčených subjektů, jejich obchodní modely a závažnost porušení předpisů.

(45) Členské státy by měly stanovit pravidla pro sankce za porušení předpisů, jako jsou přímé nebo nepřímé praktiky vedoucí k záměně nekvalifikovaných a kvalifikovaných služeb vytvářejících důvěru nebo ke zneužívání značky důvěry EU nekvalifikovanými poskytovateli služeb vytvářejících důvěru. Značka důvěry EU by se neměla používat za podmínek, které přímo či nepřímo vytvářejí dojem, že veškeré nekvalifikované služby vytvářející důvěru nabízené těmito poskytovateli jsou kvalifikované.

(46) Toto nařízení by se nemělo vztahovat na aspekty související s uzavíráním a platností smluv nebo jiných právních povinností, pokud existují požadavky na formu stanovené právem Unie nebo vnitrostátním právem. Neměly by jím být dotčeny ani vnitrostátní požadavky na formu týkající se veřejných rejstříků, zejména obchodních rejstříků a katastrů nemovitostí.

([12]) Směrnice Evropského parlamentu a Rady (EU) 2019/882 ze dne 17. dubna 2019 o požadavcích na přístupnost u výrobků a služeb (Úř. věst. L 151, 7.6.2019, s. 70).

(47) Poskytování a využívání služeb vytvářejících důvěru a výhody z hlediska pohodlného používání a právní jistoty v kontextu přeshraničních transakcí, zejména při používání kvalifikovaných služeb vytvářejících důvěru, mají stále větší význam pro mezinárodní obchod a spolupráci. Mezinárodní partneři Unie vytvářejí důvěryhodné rámce inspirované nařízením (EU) č. 910/2014. S cílem usnadnit uznávání kvalifikovaných služeb vytvářejících důvěru a jejich poskytovatelů může Komise přijmout prováděcí akty, jimiž stanoví podmínky, za nichž by mohly být důvěryhodné rámce třetích zemí považovány za rovnocenné s důvěryhodným rámcem pro kvalifikované služby vytvářející důvěru a jejich poskytovatele v tomto nařízení. Tento přístup by měl doplňovat možnost vzájemného uznávání služeb vytvářejících důvěru a jejich poskytovatelů usazených v Unii a ve třetích zemích v souladu s článkem 218 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“). Při stanovování podmínek, za nichž by mohly být důvěryhodné rámce třetích zemí považovány za rovnocenné s důvěryhodným rámcem pro kvalifikované služby vytvářející důvěru a jejich poskytovatele podle nařízení (EU) č. 910/2014, by měl být rovněž zajištěn soulad s příslušnými ustanoveními směrnice Evropského parlamentu a Rady (EU) 2022/2555 ([13]) a nařízení (EU) 2016/679, jakož i používání důvěryhodných seznamů jako základních prvků pro budování důvěry.

(48) Toto nařízení by mělo podporovat možnost volby a možnost přechodu mezi evropskými peněženkami digitální identity, pokud členský stát na svém území schválil více než jedno řešení evropské peněženky digitální identity. Aby se v takových situacích zamezilo efektu závislosti na určitém poskytovateli, měli by poskytovatelé evropských peněženek digitální identity v případě, že je to technicky proveditelné, na žádost uživatelů evropských peněženek digitální identity zajistit účinnou přenositelnost údajů a neměli by mít možnost používat smluvní, ekonomické nebo technické překážky, které by bránily účinnému přechodu mezi jednotlivými evropskými peněženkami digitální identity nebo od něj odrazovaly.

(49) Aby bylo zajištěno řádné fungování evropských peněženek digitální identity, potřebují poskytovatelé evropských peněženek digitální identity účinnou interoperabilitu a spravedlivé, přiměřené a nediskriminační podmínky pro přístup těchto peněženek ke specifickým hardwarovým a softwarovým prvkům mobilních zařízení. Tyto komponenty by mohly zahrnovat zejména antény s technologií pro blízkou komunikaci (NFC) a bezpečnostní prvky (včetně univerzálních karet s integrovaným obvodem, zabudovaných bezpečnostních prvků, karet Micro SD a funkce Bluetooth Low Energy). Kontrolu nad přístupem k těmto komponentám by mohli mít operátoři mobilních sítí a výrobci zařízení. Výrobci původního vybavení mobilních zařízení nebo poskytovatelé služeb elektronických komunikací by tedy neměli odmítat přístup k těmto komponentám, jestliže je nezbytný k poskytování služeb evropských peněženek digitální identity. Na podniky, které byly určeny jako strážci přístupu pro hlavní služby platforem uvedené na seznamu Komise podle nařízení Evropského parlamentu a Rady (EU) 2022/1925 ([14]), by se navíc i nadále měla vztahovat zvláštní ustanovení uvedeného nařízení na základě jeho čl. 6 odst. 7.

(50) S cílem zefektivnit povinnosti v oblasti kybernetické bezpečnosti uložené poskytovatelům služeb vytvářejících důvěru a umožnit těmto poskytovatelům a jejich příslušným orgánům využívat právní rámec stanovený směrnicí (EU) 2022/2555 jsou služby vytvářející důvěru povinny přijmout vhodná technická a organizační opatření podle uvedené směrnice, jako jsou opatření zaměřená na selhání systémů, chyby způsobené lidským faktorem, svévolné zásahy nebo přírodní jevy, za účelem řízení rizik pro bezpečnost sítí a informačních systémů, které tito poskytovatelé používají při poskytování svých služeb, jakož i oznamování významných incidentů a kybernetických hrozeb v souladu s uvedenou směrnicí. Pokud jde o oznamování incidentů, poskytovatelé služeb vytvářejících důvěru by měli hlásit veškeré incidenty, které mají na poskytování jejich služeb významný dopad, včetně těch, které byly způsobeny krádeží nebo ztrátou zařízení, poškozením síťového kabelu, nebo incidentů, k nimž dochází v souvislosti s identifikací osob. Požadavky na řízení kybernetických bezpečnostních rizik a oznamovací povinnosti podle směrnice (EU) 2022/2555 by měly být považovány za doplňkové k požadavkům uloženým poskytovatelům služeb vytvářejících důvěru podle tohoto nařízení. V případě potřeby by příslušné orgány určené podle směrnice (EU) 2022/2555 měly nadále uplatňovat zavedené vnitrostátní postupy nebo pokyny týkající se provádění požadavků na bezpečnost a oznamování a dohledu nad dodržováním těchto požadavků podle nařízení (EU) č. 910/2014. Tímto nařízením není dotčena povinnost oznamovat porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679.

([13]) 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).

([14]) Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích) (Úř. věst. L 265, 12.10.2022, s. 1).

(51) Je třeba věnovat náležitou pozornost zajištění účinné spolupráce mezi orgány dohledu určenými podle článku 46b nařízení (EU) č. 910/2014 a příslušnými orgány určenými nebo zřízenými podle čl. 8 odst. 1 směrnice (EU) 2022/2555. V případech, kdy se tento orgán dohledu liší od příslušného orgánu, měly by úzce a včas spolupracovat formou výměny příslušných informací s cílem zajistit účinný dohled nad poskytovateli služeb vytvářejících důvěru a dodržování požadavků stanovených v nařízení (EU) č. 910/2014 a ve směrnici (EU) 2022/2555 ze strany těchto poskytovatelů. Zejména orgány dohledu určené podle nařízení (EU) č. 910/2014 by měly být oprávněny požádat příslušné orgány určené nebo zřízené podle směrnice (EU) 2022/2555 o poskytnutí příslušných informací potřebných k udělení kvalifikovaného statusu a k provádění opatření dohledu s cílem ověřit, zda poskytovatelé služeb vytvářejících důvěru splňují příslušné požadavky podle směrnice (EU) 2022/2555, nebo po nich požadovat nápravu v případě, že je nesplňují.

(52) Je nezbytné stanovit právní rámec, který usnadní přeshraniční uznávání služeb elektronického doporučeného doručování mezi stávajícími vnitrostátními právními systémy. Tento rámec by mohl rovněž přinést nové tržní příležitosti pro poskytovatele služeb vytvářejících důvěru z Unie, kteří tak budou moci nabízet nové služby elektronického doporučeného doručování na celém území Unie. Aby bylo zajištěno, že jsou data při použití kvalifikované služby elektronického doporučeného doručování doručeny správnému adresátovi, měly by kvalifikované služby elektronického doporučeného doručování zajistit s úplnou jistotou identifikaci adresáta, přičemž pokud jde o identifikaci odesílatele, postačovala by vysoká úroveň spolehlivosti. Poskytovatelé kvalifikovaných služeb elektronického doporučeného doručování by měli být členskými státy vybízeni k tomu, aby u svých služeb zajistili interoperabilitu s kvalifikovanými službami elektronického doporučeného doručování poskytovanými jinými kvalifikovanými poskytovateli služeb vytvářejících důvěru s cílem zajistit snadné přenesení dat elektronického doporučeného doručování mezi dvěma nebo více kvalifikovanými poskytovateli služeb vytvářejících důvěru a prosazovat spravedlivé postupy na vnitřním trhu.

(53) Ve většině případů si občané Unie a rezidenti v Unii nemohou přeshraničně a současně bezpečně s vysokou úrovní ochrany údajů vyměňovat v digitální podobě informace týkající se jejich totožnosti, jako jsou jejich adresy, věk a odborné kvalifikace, řidičské průkazy, jiná povolení a platební údaje.

(54) Mělo by být možné vydávat a zpracovávat důvěryhodné elektronické atributy a přispívat ke snižování administrativní zátěže, což by občany Unie a rezidenty v Unii motivovalo využívat je při svých soukromých a veřejných transakcích. Občané Unie a ostatní rezidenti v Unii by například měli mít možnost prokázat vlastnictví platného řidičského průkazu vydaného orgánem v jednom členském státě, který může být ověřen příslušnými orgány v jiných členských státech a na nějž se tyto orgány mohou spolehnout, a využívat v přeshraničním kontextu své doklady týkající se sociálního zabezpečení nebo budoucí digitální cestovní doklady.

(55) Každý poskytovatel služeb, který vydává potvrzené atributy v elektronické podobě, jako jsou diplomy, licence, rodné listy nebo plné moci a pověření k zastupování fyzických nebo právnických osob či k jednání jejich jménem, by měl být považován za poskytovatele služeb vytvářejících důvěru vydávajícího elektronické potvrzení atributů. Elektronickému potvrzení atributů by neměly být upírány právní účinky proto, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické potvrzení atributů. Měly by být stanoveny obecné požadavky, které zajistí, aby kvalifikované elektronické potvrzení atributů mělo rovnocenný právní účinek jako potvrzení v listinné podobě vydaná v souladu s právními předpisy. Tyto požadavky by se však měly uplatňovat, aniž jsou dotčeny právní předpisy Unie nebo vnitrostátní právní předpisy vymezující dodatečné požadavky pro konkrétní odvětví, co se týče formy se základními právními účinky, a zejména případné přeshraniční uznávání kvalifikovaného elektronického potvrzení atributů.

(56) Široká dostupnost a použitelnost evropských peněženek digitální identity by měla posílit jejich přijetí a důvěru v ně ze strany soukromých osob i soukromých poskytovatelů služeb. Soukromé spoléhající se strany poskytující služby například v oblasti dopravy, energetiky, bankovnictví, finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, telekomunikací nebo vzdělávání by proto měly akceptovat používání evropských peněženek digitální identity za účelem poskytování služeb, u nichž se na základě unijních nebo vnitrostátních právních předpisů či smluvního závazku vyžaduje silná autentizace uživatele k identifikaci on-line. Jakákoli žádost spoléhající se strany o informace od uživatele evropské peněženky digitální identity by měla být nezbytná pro zamýšlené použití v daném případě a tomuto použití přiměřená, měla by být v souladu se zásadou minimalizace údajů a měla by zajistit transparentnost, pokud jde o druh sdílených údajů a účel jejich sdílení. V zájmu snazšího používání a přijímání evropských peněženek digitální identity by měly být při jejich zavádění zohledněny obecně uznávané odvětvové normy a specifikace.

(57) V případech, kdy velmi velké on-line platformy ve smyslu čl. 33 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2022/2065 ([15]) vyžadují od uživatelů za účelem přístupu k on-line službám autentizaci, by tyto platformy měly mít povinnost akceptovat použití evropské peněženky digitální identity na dobrovolnou žádost uživatele. Uživatelé by neměli mít povinnost používat evropskou peněženku digitální identity k přístupu k soukromým službám a neměli by být omezováni v přístupu ke službám ani by jim nemělo být v tomto přístupu bráněno z důvodu, že evropskou peněženku digitální identity nepoužívají. Avšak pokud si to uživatelé přejí, měly by velmi velké on-line platformy za tímto účelem evropskou peněženku digitální identity akceptovat, přičemž by měla být dodržena zásada minimalizace údajů a právo uživatelů na použití svobodně zvoleného pseudonymu. Vzhledem k významu velmi velkých on-line platforem a k jejich dosahu, vyjádřenému zejména počtem příjemců služby a ekonomických transakcí, je povinnost akceptovat evropskou peněženku digitální identity nezbytná ke zvýšení ochrany uživatelů před podvody a k zajištění vysoké úrovně ochrany údajů.

(58) S cílem přispět k široké dostupnosti a použitelnosti prostředků pro elektronickou identifikaci, včetně evropských peněženek digitální identity, které spadají do oblasti působnosti tohoto nařízení, by měly být vypracovány kodexy chování na úrovni Unie. Tyto kodexy chování by měly usnadnit široké přijímání prostředků pro elektronickou identifikaci, včetně evropských peněženek digitální identity, těmi poskytovateli služeb, kteří nejsou kvalifikováni jako velmi velké platformy a kteří pro autentizaci uživatelů využívají služeb elektronické identifikace poskytovaných třetími stranami.

(59) Koncept výběrového zpřístupňování opravňuje vlastníka údajů zpřístupnit pouze určité části většího souboru údajů, aby přijímající subjekt získal pouze ty informace, které jsou nezbytné pro poskytnutí služby požadované uživatelem. Evropská peněženka digitální identity by měla výběrové zpřístupňování atributů spoléhajícím se stranám technicky umožňovat. Pro uživatele by mělo být technicky možné, aby výběrově zpřístupňoval atributy, a to i z několika odlišných elektronických potvrzení, kombinoval je a bezproblémově předkládal spoléhajícím se stranám. Tento prvek by se měl stát základním koncepčním prvkem evropských peněženek digitální identity, čímž se zvýší uživatelská přívětivost a ochrana osobních údajů, včetně minimalizace údajů.

(60) Pokud zvláštní pravidla podle práva Unie nebo vnitrostátního práva nevyžadují, aby se uživatelé identifikovali, nemělo by být používání služeb s využitím pseudonymu zakázáno.

(61) Atributy poskytované kvalifikovanými poskytovateli služeb vytvářejících důvěru jako součást kvalifikovaného potvrzování atributů by měly být ověřovány na základě autentických zdrojů buď přímo kvalifikovaným poskytovatelem služeb vytvářejících důvěru, nebo prostřednictvím určených zprostředkovatelů uznaných na vnitrostátní úrovni v souladu s právem Unie nebo s vnitrostátním právem pro účely bezpečné výměny potvrzených atributů mezi poskytovateli služeb v oblasti identifikace nebo potvrzování atributů a spoléhajícími se stranami. Členské státy by měly na vnitrostátní úrovni zavést vhodné mechanismy k zajištění toho, aby kvalifikovaní poskytovatelé služeb vytvářejících důvěru vydávající kvalifikované elektronické potvrzení atributů mohli na základě souhlasu osoby, jíž je potvrzení vydáváno, ověřit pravost atributů na základě autentických zdrojů. Mělo by být umožněno, aby vhodné mechanismy zahrnovaly využívání konkrétních zprostředkovatelů nebo technických řešení v souladu s vnitrostátním právem, které poskytují přístup k autentickým zdrojům. Zajištění dostupnosti mechanismu, který umožňuje ověřování atributů na základě autentických zdrojů, má za cíl usnadnit, aby kvalifikovaní poskytovatelé služeb vytvářejících důvěru poskytující kvalifikované elektronické potvrzování atributů plnili své povinnosti stanovené nařízením (EU) č. 910/2014. Nová příloha uvedeného nařízení by měla obsahovat seznam kategorií atributů, u nichž mají členské státy zajistit, aby byla přijata opatření, která kvalifikovaným poskytovatelům služeb vytvářejících důvěru poskytujícím elektronická potvrzení atributů umožní na žádost uživatele ověřit elektronickými prostředky jejich pravost ve vztahu k příslušnému autentickému zdroji.

(62) Díky bezpečné elektronické identifikaci a potvrzování atributů by mělo mít odvětví finančních služeb k dispozici dodatečnou flexibilitu a řešení, jež umožní identifikaci zákazníků a výměnu konkrétních atributů nezbytných ke splnění například požadavků na hloubkovou kontrolu klienta podle budoucího nařízení o zřízení Orgánu pro boj proti praní peněz a požadavků přiměřenosti vyplývajících z právních předpisů na ochranu investorů nebo podpoří plnění požadavků na silnou autentizaci klienta k identifikaci pro účely on-line přihlášení se k účtu a zahájení transakcí v oblasti platebních služeb.

(63) Právní účinek elektronického podpisu nelze zpochybňovat z důvodu, že je v elektronické podobě nebo že nesplňuje požadavky na kvalifikovaný elektronický podpis. Právní účinek elektronických podpisů však má být vymezen vnitrostátním právem, s výhradou požadavku stanoveného tímto nařízením, aby byl právní účinek kvalifikovaného elektronického podpisu považován za rovnocenný vlastnoručnímu podpisu. Při určování právního účinku

([15]) Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách) (Úř. věst. L 277, 27.10.2022, s. 1).

elektronických podpisů by členské státy měly zohlednit zásadu proporcionality mezi právním významem písemnosti, která má být podepsána, a úrovní bezpečnosti a nákladů, které elektronický podpis vyžaduje. V zájmu zvýšení dostupnosti a používání elektronických podpisů se členské státy vyzývají, aby zvážily používání zaručených elektronických podpisů v každodenních transakcích, pro něž zajišťují dostatečnou úroveň bezpečnosti a důvěryhodnosti.

(64) V zájmu zajištění jednotnosti certifikačních postupů v celé Unii by Komise měla vydat pokyny pro certifikaci a opětovnou certifikaci kvalifikovaných prostředků pro vytváření elektronických podpisů a kvalifikovaných prostředků pro vytváření elektronických pečetí, včetně jejich platnosti a časových omezení. Toto nařízení nebrání veřejným ani soukromým subjektům, které kvalifikované prostředky pro vytváření elektronických podpisů již certifikovaly, aby na základě výsledků předchozího certifikačního procesu dočasně provedly opětovnou certifikaci těchto prostředků na krátké certifikační období, pokud tuto opětovnou certifikaci nelze provést v zákonem stanovené lhůtě z jiného důvodu, než je narušení bezpečnosti nebo bezpečnostní incident, a aniž je dotčena povinnost provést posouzení zranitelnosti a aniž je dotčena příslušná certifikační praxe.

(65) Vydávání certifikátů pro autentizaci internetových stránek poskytuje uživatelům záruku vysoké úrovně spolehlivosti, pokud jde o totožnost subjektu, který stojí za danými stránkami, bez ohledu na to, která platforma se k zobrazení této totožnosti využívá. Tyto certifikáty by měly přispět k budování důvěry v on-line obchodování, neboť uživatelé budou mít spíše důvěru v internetové stránky, které byly autentizovány. Využívání takových certifikátů internetovými stránkami by mělo být dobrovolné. Aby se autentizace internetových stránek stala prostředkem ke zvyšování důvěry, k zajištění lepší uživatelské zkušenosti a k podpoře růstu na vnitřním trhu, stanoví toto nařízení důvěryhodný rámec zahrnující minimální povinnosti v oblasti bezpečnosti a odpovědnosti, jež jsou uloženy poskytovatelům kvalifikovaných certifikátů pro autentizaci internetových stránek, jakož i požadavky na vydávání těchto certifikátů. Vnitrostátní důvěryhodné seznamy by měly potvrdit kvalifikovaný status služeb autentizace internetových stránek a jejich poskytovatelů služeb vytvářejících důvěru, včetně jejich plného souladu s požadavky tohoto nařízení, pokud jde o vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek. Uznáním kvalifikovaných certifikátů pro autentizaci internetových stránek se rozumí, že by poskytovatelé internetových prohlížečů neměli popírat pravost těchto kvalifikovaných certifikátů pouze za účelem potvrzení spojení mezi názvem internetové domény a fyzickou nebo právnickou osobou, jíž je certifikát vydán, nebo potvrzení totožnosti této osoby. Poskytovatelé internetových prohlížečů by měli certifikované údaje o totožnosti a ostatní potvrzené atributy koncovému uživateli zobrazovat v prostředí prohlížeče uživatelsky přívětivým způsobem, a to s využitím technických prostředků dle vlastního výběru. Za tímto účelem by poskytovatelé internetových prohlížečů měli zajistit podporu a interoperabilitu s kvalifikovanými certifikáty pro autentizaci internetových stránek vydanými v plném souladu s tímto nařízením. Povinností uznávání, interoperability a podpory kvalifikovaných certifikátů pro autentizaci internetových stránek není dotčena svoboda poskytovatelů internetových prohlížečů, pokud jde o zajišťování bezpečnosti internetových stránek, autentizaci domén a šifrování internetového provozu, pro něž mohou zvolit způsob a technologie, které považují za nejvhodnější. S cílem přispět k on-line bezpečnosti koncových uživatelů by poskytovatelé internetových prohlížečů měli mít za výjimečných okolností možnost přijmout nezbytná a současně přiměřená předběžná opatření v reakci na odůvodněné obavy týkající se narušení bezpečnosti nebo ztráty integrity identifikovaného certifikátu nebo souboru certifikátů. Pokud poskytovatelé internetových prohlížečů taková předběžná opatření přijmou, měli by bez zbytečného odkladu informovat Komisi a vnitrostátní orgán dohledu a dále subjekt, kterému byl certifikát vydán, a kvalifikovaného poskytovatele služeb vytvářejících důvěru, který tento certifikát nebo soubor certifikátů vydal, o veškerých obavách souvisejících s tímto narušením bezpečnosti nebo s touto ztrátou integrity, jakož i o opatřeních přijatých v souvislosti s jediným certifikátem nebo souborem certifikátů. Těmito opatřeními by neměla být dotčena povinnost poskytovatelů internetových prohlížečů uznávat kvalifikované certifikáty pro autentizaci internetových stránek v souladu s vnitrostátními důvěryhodnými seznamy. Za účelem zvýšení ochrany občanů Unie a rezidentů v Unii a další podpory používání kvalifikovaných certifikátů pro autentizaci internetových stránek by orgány veřejné moci v členských státech měly zvážit jejich začlenění do vlastních internetových stránek. Opatření stanovená tímto nařízením, jejichž cílem je zajistit větší soudržnost mezi rozdílnými přístupy a postupy členských států v oblasti dohledu, mají přispět ke zvýšení důvěry v bezpečnost, kvalitu a dostupnost kvalifikovaných certifikátů pro autentizaci internetových stránek.

(66) Mnoho členských států zavedlo vnitrostátní požadavky na služby poskytující bezpečnou a důvěryhodnou elektronickou archivaci, aby bylo možné dlouhodobě uchovávat elektronická data a elektronické dokumenty, jakož i na a související služby vytvářející důvěru. V zájmu zajištění právní jistoty, důvěryhodnosti a harmonizace ve všech členských státech by měl být vytvořen právní rámec pro kvalifikované služby elektronické archivace, který by se inspiroval rámcem pro jiné služby vytvářející důvěru stanovené v tomto nařízení. Tento právní rámec pro kvalifikované služby elektronické archivace by měl poskytovatelům služeb vytvářejících důvěru a uživatelům nabídnout účinný soubor nástrojů, který zahrnuje funkční požadavky na službu elektronické archivace, jakož i jasné právní účinky v případě využití kvalifikované služby elektronické archivace. Tato ustanovení by se měla vztahovat elektronická data a elektronické dokumenty, které byly vytvořeny v elektronické podobě, i na listinné dokumenty, které byly naskenovány a digitalizovány. V případě potřeby by tato ustanovení měla umožnit přenos uchovávaných

elektronických dat a elektronických dokumentů na různá média nebo jejich převedení do různých formátů za účelem prodloužení jejich trvanlivosti a čitelnosti i po uplynutí doby technologické použitelnosti a zároveň v rámci možností předejít jejich ztrátě a pozměnění. Pokud elektronická data a elektronické dokumenty předložené elektronické archivační službě obsahují jeden nebo více kvalifikovaných elektronických podpisů nebo kvalifikovaných elektronických pečetí, měla by uvedená služba používat postupy a technologie umožňující prodloužení důvěryhodnosti těchto dat na dobu jejich uchovávání, případně s využitím jiných kvalifikovaných služeb vytvářejících důvěru, stanovených tímto nařízením. Za účelem vytváření důkazů o uchovávání v případech, kdy se používají elektronické podpisy, elektronické pečetě nebo elektronická časová razítka, by se měly používat kvalifikované služby vytvářející důvěru. Členské státy by v rozsahu, v jakém služby elektronické archivace tímto nařízením nejsou harmonizovány, měly mít možnost v souladu s právem Unie zachovat nebo zavést vnitrostátní předpisy týkající se těchto služeb, jako jsou zvláštní ustanovení pro služby integrované do organizace a používané výhradně pro interní archivaci v rámci této organizace. Toto nařízení by nemělo rozlišovat mezi elektronickými daty a elektronickými dokumenty, které byly vytvořeny v elektronické podobě, a fyzickými dokumenty, které byly digitalizovány.

(67) Činnost národních archivů a paměťových institucí je jakožto činnost organizací zabývajících se ochranou dokumentárního dědictví ve veřejném zájmu obvykle regulována vnitrostátním právem a tyto instituce nemusí nutně poskytovat služby vytvářející důvěru ve smyslu tohoto nařízení. Pokud tyto instituce takové služby vytvářející důvěru neposkytují, není jejich fungování tímto nařízením dotčeno.

(68) Elektronické knihy záznamů představují pořadí elektronických datových záznamů, které zajišťuje jejich integritu a přesnost jejich chronologického řazení. Elektronické knihy záznamů by měly vytvořit chronologickou posloupnost datových záznamů. Ve spojení s dalšími technologiemi by měly přispět k nalezení řešení pro účinnější a transformační veřejné služby, jako jsou elektronické hlasování, přeshraniční spolupráce celních orgánů, přeshraniční spolupráce akademických institucí a zaznamenávání vlastnictví nemovitostí v decentralizovaných katastrech nemovitostí. Kvalifikované elektronické knihy záznamů by měly vytvořit právní předpoklad pro jedinečné a přesné sekvenční chronologické pořadí a integritu datových záznamů v knize záznamů. Vzhledem ke svým specifickým rysům, jako je postupné chronologické řazení datových záznamů, by elektronické knihy záznamů měly být odlišovány od ostatních služeb vytvářejících důvěru, jako jsou elektronická časová razítka a služby elektronického doporučeného doručování. V zájmu zajištění právní jistoty a podpory inovací by měl být zřízen unijní právní rámec, který upravuje přeshraniční uznávání služeb vytvářejících důvěru pro účely zaznamenávání dat do kvalifikovaných elektronických knih záznamů. Mělo by to v dostatečné míře zabránit tomu, aby bylo stejné digitální aktivum zkopírováno a opakovaně prodáno různým stranám. Proces vytváření a aktualizace elektronické knihy záznamů závisí na typu používané knihy záznamů, jmenovitě na tom, zda se jedná o centralizovanou nebo distribuovanou knihu záznamů. Toto nařízení by mělo zajistit technologickou neutralitu, konkrétně by nemělo upřednostňovat ani diskriminovat žádnou technologii používanou k zavedení nové služby vytvářející důvěru pro elektronické knihy záznamů. Kromě toho by Komise měla při přípravě prováděcích aktů upřesňujících požadavky na kvalifikované elektronické knihy záznamů za použití odpovídajících metodik zohlednit ukazatele udržitelnosti týkající se jakýchkoli nepříznivých dopadů na klima nebo jiné nepříznivé dopady související s životním prostředím.

(69) Úloha poskytovatelů služeb vytvářejících důvěru pro elektronické knihy záznamů by měla spočívat v kontrole postupného zaznamenávání dat do knihy záznamů. Tímto nařízením nejsou dotčeny právní povinnosti uživatelů elektronických knih záznamů stanovené právem Unie nebo vnitrostátním právem. Například případy použití, které zahrnují zpracování osobních údajů, by měly být v souladu s nařízením (EU) 2016/679 a případy použití, které se týkají finančních služeb, by měly být v souladu s příslušnými právními předpisy Unie v oblasti finančních služeb.

(70) K tomu, aby se zabránilo roztříštěnosti a překážkám na vnitřním trhu v důsledku rozdílných norem a technických omezení a aby se zajistil koordinovaný postup, který zamezí narušení provádění evropského rámce pro digitální identitu, je nezbytné zavést úzkou a strukturovanou spolupráci mezi Komisí, členskými státy, občanskou společností, akademickou obcí a soukromým sektorem. K dosažení tohoto cíle by členské státy a Komise měly spolupracovat v rámci stanoveném v doporučení Komise (EU) 2021/946 ([16]) s cílem určit soubor nástrojů Unie pro evropský rámec pro digitální identitu. V této souvislosti by se členské státy měly dohodnout na komplexní technické architektuře a referenčním rámci, souboru společných norem a technických referencí, včetně uznávaných platných norem, a souboru pokynů a popisu osvědčených postupů zahrnujících alespoň všechny funkce a interoperabilitu evropských peněženek digitální identity, včetně elektronických podpisů, a poskytovatelů kvalifikované služby vytvářející důvěru pro elektronické potvrzování atributů, jak je stanoveno v tomto nařízení. V této souvislosti by členské státy měly rovněž dosáhnout dohody o společných prvcích týkajících se obchodního modelu a o struktuře poplatků evropských peněženek digitální identity s cílem usnadnit jejich přijímání, zejména malými a středními

([16]) 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).

podniky v přeshraničním kontextu. Obsah souboru nástrojů by se měl vyvíjet souběžně s diskusí a procesem přijetí evropského rámce pro digitální identitu a měl by odrážet výsledek této diskuse a tohoto procesu.

(71) Toto nařízení stanoví harmonizovanou úroveň kvality, důvěryhodnosti a bezpečnosti kvalifikovaných služeb vytvářejících důvěru bez ohledu na to, kde jsou operace prováděny. Kvalifikovaný poskytovatel služeb vytvářejících důvěru by proto měl mít možnost zadávat externě své operace související s poskytováním kvalifikované služby vytvářející důvěru ve třetí zemi, pokud tato třetí země poskytne odpovídající záruky, jimiž zajistí, aby mohly být činnosti dohledu a audity vymáhány tak, jako by byly prováděny v Unii. Nelze-li soulad s tímto nařízením plně zajistit, měly by mít orgány dohledu možnost přijmout přiměřená a odůvodněná opatření, včetně odnětí statusu kvalifikované služby vytvářející důvěru.

(72) V zájmu zajištění právní jistoty ohledně platnosti zaručených elektronických podpisů založených na kvalifikovaných certifikátech je nezbytné upřesnit posouzení spoléhající se stranou, která provádí ověření platnosti daného zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu.

(73) Poskytovatelé služeb vytvářejících důvěru by měli používat kryptografické metody odrážející stávající osvědčené postupy a důvěryhodné provádění těchto algoritmů, aby zajistili bezpečnost a spolehlivost svých služeb vytvářejících důvěru.

(74) Toto nařízení stanoví povinnost kvalifikovaných poskytovatelů služeb vytvářejících důvěru ověřovat totožnost fyzické nebo právnické osoby, kterým jsou kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů vydávány, a to na základě různých harmonizovaných metod platných v celé Unii. K zajištění toho, aby kvalifikované certifikáty a kvalifikovaná elektronická potvrzení atributů byly vydávány osobě, k níž náleží, a aby osvědčovaly správný a jedinečný soubor údajů představujících totožnost této osoby, by kvalifikovaní poskytovatelé služeb vytvářejících důvěru vydávající kvalifikované certifikáty nebo kvalifikovaná elektronická potvrzení atributů měli v okamžiku vydání těchto certifikátů a potvrzení zajistit s úplnou jistotou identifikaci této osoby. Kromě povinného ověření totožnosti osoby, je-li to relevantní pro vydávání kvalifikovaných certifikátů a při vydávání kvalifikovaného elektronického potvrzení atributů, by kvalifikovaní poskytovatelé služeb vytvářejících důvěru měli s úplnou jistotou zajistit správnost a přesnost potvrzených atributů osoby, jíž jsou kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů vydávány. Tyto povinnosti týkající se výsledku a úplné jistoty při ověřování potvrzených údajů by měly být podpořeny odpovídajícími prostředky, včetně použití jedné nebo případně několika konkrétních metod stanovených v tomto nařízení. Tyto metody by mělo být možné kombinovat s cílem poskytnout vhodný základ pro ověření totožnosti osoby, jíž jsou kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů vydávány. Mělo by být možné, aby tato kombinace zahrnovala využití prostředků pro elektronickou identifikaci, které splňují požadavky na značnou úroveň záruky, v kombinaci s jinými prostředky pro ověření totožnosti. Taková elektronické identifikace by umožnila splnění harmonizovaných požadavků stanovených v tomto nařízení, pokud jde o vysokou úroveň záruky, v rámci dalších harmonizovaných postupů na dálku, které zajišťují identifikaci s vysokou úrovní spolehlivosti. Tyto metody by měly kvalifikovanému poskytovateli služeb vytvářejících důvěru, který vydává kvalifikované elektronické potvrzení atributů, umožnit, aby na žádost uživatele a v souladu s unijním nebo vnitrostátním právem ověřil atributy, které mají být potvrzeny elektronickými prostředky, a to i na základě autentických zdrojů.

(75) Aby bylo toto nařízení v souladu s globálním vývojem a aby byly dodržovány osvědčené postupy na vnitřním trhu, měly by být akty v přenesené pravomoci a prováděcí akty přijaté Komisí pravidelně přezkoumávány a v případě potřeby aktualizovány. Při posuzování nezbytnosti těchto aktualizací by se měly zohlednit nové technologie, postupy, normy a technické specifikace.

(76) Jelikož cílů tohoto nařízení, totiž rozvoje celounijního evropského rámce pro digitální identitu a rámce pro služby vytvářející důvěru, nemůže být dosaženo uspokojivě členskými státy, ale spíše jich, z důvodu jejich rozsahu a účinků, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení těchto cílů.

(77) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 42 odst. 1 nařízení (EU) 2018/1725.

(78) Nařízení (EU) č. 910/2014 by proto mělo být odpovídajícím způsobem změněno,

PŘIJALY TOTO NAŘÍZENÍ:

Článek 1

Změny nařízení (EU) č. 910/2014

Nařízení (EU) č. 910/2014 se mění takto:

1) Článek 1 se nahrazuje tímto:

„*Článek 1*

Předmět

Cílem tohoto nařízení je zajistit řádné fungování vnitřního trhu a poskytování odpovídající úrovně bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru používaných v celé Unii, aby byl fyzickým a právnickým osobám umožněn a usnadněn výkon práva na bezpečnou účast v digitální společnosti a na přístup k veřejným a soukromým on-line službám v celé Unii. Za těmito účely toto nařízení:

a) stanoví podmínky, za nichž mají členské státy uznávat prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému elektronické identifikace jiného členského státu, a poskytovat a uznávat evropské peněženky digitální identity;

b) stanoví pravidla pro služby vytvářející důvěru, zejména u elektronických transakcí;

c) stanoví právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování, certifikační služby pro autentizaci internetových stránek, elektronickou archivaci, elektronické potvrzování atributů, prostředky pro vytváření elektronických podpisů, prostředky pro vytváření elektronických pečetí a pro elektronické knihy záznamů;“.

2) Článek 2 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Toto nařízení se vztahuje na systémy elektronické identifikace oznámené členskými státy, na evropské peněženky digitální identity poskytované členskými státy a na poskytovatele služeb vytvářejících důvěru usazené v Unii.“;

b) odstavec 3 se nahrazuje tímto:

„3. Tímto nařízením nejsou dotčeny právo Unie ani vnitrostátní právo týkající se uzavírání a platnosti smluv, jiné právní nebo procesní povinnosti týkající se formy nebo požadavky pro konkrétní odvětví týkajících se formy.

4. Tímto nařízením není dotčeno nařízení Evropského parlamentu a Rady (EU) 2016/679 (*).

(*) 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).“

3) Článek 3 se mění takto:

a) body 1 až 5 se nahrazují tímto:

„1) ‚elektronickou identifikací‘ postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující jinou fyzickou či právnickou osobu;

2) ‚prostředkem pro elektronickou identifikaci' hmotná či nehmotná jednotka obsahující osobní identifikační údaje, která se používá k autentizaci pro účely on-line služby nebo případně off-line služby;

3) ‚osobními identifikačními údaji' soubor údajů vydaných v souladu s právem Unie nebo vnitrostátním právem a umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující jinou fyzickou či právnickou osobu;

4) ‚systémem elektronické identifikace' systém pro elektronickou identifikaci, na jehož základě jsou fyzickým či právnickým osobám nebo fyzickým osobám zastupujícím jiné fyzické či právnické osoby vydávány prostředky pro elektronickou identifikaci;

5) ‚autentizací' elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě;";

b) vkládá se nový bod, který zní:

„5a) ‚uživatelem' fyzická či právnická osoba nebo fyzická osoba zastupující jinou fyzickou či právnickou osobu, které využívají služeb vytvářejících důvěru nebo prostředků pro elektronickou identifikaci poskytovaných v souladu s tímto nařízením;";

c) bod 6 se nahrazuje tímto:

„6) ‚spoléhající se stranou' fyzická nebo právnická osoba, které se spoléhají na elektronickou identifikaci, evropské peněženky digitální identity nebo jiné prostředky pro elektronickou identifikaci nebo na službu vytvářející důvěru;";

d) bod 16 se nahrazuje tímto:

„16) ‚službou vytvářející důvěru' elektronická služba, která je zpravidla poskytována za úplatu a spočívá:

a) ve vydávání certifikátů pro elektronické podpisy, certifikátů pro elektronické pečetě, certifikátů pro autentizaci internetových stránek nebo certifikátů pro poskytování jiných služeb vytvářejících důvěru;

b) v ověřování platnosti certifikátů pro elektronické podpisy, certifikátů pro elektronické pečetě, certifikátů pro autentizaci internetových stránek nebo certifikátů pro poskytování jiných služeb vytvářejících důvěru;

c) ve vytváření elektronických podpisů nebo elektronických pečetí;

d) v ověřování platnosti elektronických podpisů nebo elektronických pečetí;

e) v uchovávání elektronických podpisů, elektronických pečetí, certifikátů pro elektronické podpisy nebo certifikátů pro elektronické pečetě;

f) ve správě prostředků pro vytváření elektronických podpisů na dálku nebo prostředků pro vytváření elektronických pečetí na dálku;

g) ve vydávání elektronických potvrzení atributů;

h) v ověřování platnosti elektronického potvrzení atributů;

i) ve vytváření elektronických časových razítek;

j) v ověřování platnosti elektronických časových razítek;

k) v poskytování služeb elektronického doporučeného doručování;

l) v ověřování platnosti dat přenášených prostřednictvím služeb elektronického doporučeného doručování a souvisejících důkazů;

m) v elektronické archivaci elektronických dat a elektronických dokumentů;

n) v zaznamenávání elektronických dat do elektronické knihy záznamů;“;

e) bod 18 se nahrazuje tímto:

„18) ‚subjektem posuzování shody‘ subjekt posuzování shody ve smyslu čl. 2 bodu 13 nařízení (ES) č. 765/2008, který je v souladu s uvedeným nařízením akreditován jako způsobilý provádět posuzování shody kvalifikovaného poskytovatele služeb vytvářejících důvěru a jím poskytovaných kvalifikovaných služeb vytvářejících důvěru nebo jako příslušný k provádění certifikace evropských peněženek digitální identity nebo prostředků pro elektronickou identifikaci;“;

f) bod 21 se nahrazuje tímto:

„21) ‚produktem‘ technické zařízení nebo programové vybavení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb elektronické identifikace a služeb vytvářejících důvěru;“;

g) vkládají se nová písmena, která znějí:

„23a) ‚kvalifikovaným prostředkem pro vytváření elektronických podpisů na dálku‘ kvalifikovaný prostředek pro vytváření elektronických podpisů, který jménem podepisující osoby v souladu s článkem 29a spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru;

23b) ‚kvalifikovaným prostředkem pro vytváření elektronických pečetí na dálku‘ kvalifikovaný prostředek pro vytváření elektronických pečetí, který jménem pečetící osoby spravuje v souladu s článkem 39a kvalifikovaný poskytovatel služeb vytvářejících důvěru;“;

h) bod 38 se nahrazuje tímto:

„38) ‚certifikátem pro autentizaci internetových stránek‘ elektronické potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jimž je certifikát vydán;“;

i) bod 41 se nahrazuje tímto:

„41) ‚ověřováním platnosti‘ postup ověření a potvrzení, že data v elektronické podobě jsou v souladu s tímto nařízením platná;“;

j) doplňují se nové body, které znějí:

„42) ‚evropskou peněženkou digitální identity‘ prostředek pro elektronickou identifikaci, který uživateli umožňuje bezpečně ukládat, spravovat a ověřovat osobní identifikační údaje a elektronická potvrzení atributů za účelem jejich poskytnutí spoléhajícím se stranám a dalším uživatelům evropských peněženek digitální identity a podepisovat prostřednictvím kvalifikovaných elektronických podpisů nebo pečetit prostřednictvím kvalifikovaných elektronických pečetí;

43) ‚atributem‘ vlastnost, kvalita, právo nebo povolení fyzické nebo právnické osoby nebo předmětu;

44) ‚elektronickým potvrzením atributů‘ potvrzení v elektronické podobě, které umožňuje autentizaci atributů;

45) ‚kvalifikovaným elektronickým potvrzením atributů‘ elektronické potvrzení atributů, které je vydáno kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze V;

46) ‚elektronickým potvrzením atributů vydaným subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem‘ elektronické potvrzení atributů, které je vydáno subjektem veřejného sektoru odpovědným za autentický zdroj nebo subjektem veřejného sektoru určeným členským státem k vydávání těchto potvrzení atributů jménem subjektů veřejného sektoru odpovědných za autentické zdroje v souladu s článkem 45f a přílohou VII;

47) ‚autentickým zdrojem‘ úložiště nebo systém, za které odpovídá subjekt veřejného sektoru nebo soukromý subjekt a které obsahují a poskytují atributy fyzické nebo právnické osoby nebo předmětu a jsou považovány za primární zdroj těchto informací nebo jsou v souladu s právem Unie nebo vnitrostátním právem, včetně správní praxe, uznány za autentické;

48) ‚elektronickou archivací' služba zajišťující 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;

49) ‚kvalifikovanou službou elektronické archivace' služba elektronické archivace, kterou poskytuje kvalifikovaný poskytovatel služeb vytvářejících důvěru a která splňuje požadavky stanovené v článku 45j;

50) ‚značkou důvěry EU pro peněženku digitální identity' ověřitelné, jednoduché a rozpoznatelné označení, které jasným způsobem sděluje, že evropská peněženka digitální identity byla poskytnuta v souladu s tímto nařízením;

51) ‚silnou autentizací uživatele' autentizace založená na použití nejméně dvou navzájem nezávislých autentizačních faktorů z různých kategorií, kterými může být znalost, tedy něco, co ví pouze uživatel, držení, tedy něco, co má v držení pouze uživatel, nebo inherence, tedy něco, čím uživatel je, přičemž nesplněním jednoho z nich není ovlivněna spolehlivost ostatních a postup je koncipován tak, aby byla chráněna důvěrnost autentizačních dat;

52) ‚elektronickou knihou záznamů' posloupnost elektronických datových záznamů zajišťující integritu těchto záznamů a přesnost chronologického pořadí těchto záznamů;

53) ‚kvalifikovanou elektronickou knihou záznamů' elektronická kniha záznamů, kterou poskytuje kvalifikovaný poskytovatel služeb vytvářejících důvěru a která splňuje požadavky stanovené v článku 45l;

54) ‚osobními údaji' veškeré informace vymezené v čl. 4 bodu 1 nařízení (EU) 2016/679;

55) ‚párováním totožnosti' postup, při němž jsou osobní identifikační údaje nebo prostředky pro elektronickou identifikaci párovány nebo propojeny se stávajícím účtem patřícím téže osobě;

56) ‚datovým záznamem' elektronická data zaznamenaná pomocí souvisejících metadat podporujících zpracování těchto dat;

57) ‚off-line režimem' pokud jde o používání evropských peněženek digitální identity, interakce mezi uživatelem a třetí stranou na fyzickém místě s využitím technologií pro blízkou komunikaci, při níž evropská peněženka digitální identity nemusí mít pro účely dané interakce přístup ke vzdáleným systémům prostřednictvím sítí elektronických komunikací."

4) Článek 5 se nahrazuje tímto:

„Článek 5

Pseudonymy v elektronických transakcích

Aniž jsou dotčena zvláštní pravidla práva Unie nebo vnitrostátního práva, která vyžadují, aby se uživatelé identifikovali, nebo právní účinky, které vnitrostátní právo přiznává pseudonymům, není používání pseudonymů, které si uživatel zvolil, zakázáno."

5) V kapitole II se vkládá nový oddíl, který zní:

„ODDÍL 1

EVROPSKÁ PENĚŽENKA DIGITÁLNÍ IDENTITY

Článek 5a

Evropské peněženky digitální identity

1. S cílem zajistit, aby všechny fyzické a právnické osoby v Unii měly bezpečný, důvěryhodný a bezproblémový přeshraniční přístup k veřejným a soukromým službám a zároveň plnou kontrolu nad svými údaji, každý členský stát do 24 měsíců ode dne vstupu prováděcích aktů uvedených v odstavci 23 tohoto článku a v čl. 5c odst. 6 v platnost poskytne alespoň jednu evropskou peněženku digitální identity.

2. Evropské peněženky digitální identity jsou poskytovány jedním nebo vícero z následujících způsobů:

a) přímo členským státem;

b) z pověření členského státu;

c) nezávisle na členském státu, ale tímto členským státem uznávané.

3. Zdrojový kód komponent aplikačního softwaru evropských peněženek digitální identity musí mít licenci otevřeného zdrojového kódu. Členské státy mohou stanovit, že v řádně odůvodněných případech se zdrojový kód konkrétních komponent jiných než těch, které jsou instalovány na uživatelských zařízeních, nezveřejní.

4. Evropské peněženky digitální identity umožní uživateli způsobem, který je pro uživatele přívětivý, transparentní a sledovatelný:

a) bezpečně a pod výhradní kontrolou uživatele požadovat, získat, vybírat, kombinovat, uchovávat, mazat, sdílet a předkládat osobní identifikační údaje a případně ve spojení s elektronickým potvrzením atributů se autentizovat vůči spoléhajícím se stranám on-line a případně v off-line režimu s cílem přistupovat k veřejným a soukromým službám, přičemž je zajištěna možnost výběrového zpřístupňování údajů;

b) generovat pseudonymy a ukládat je zašifrované a lokálně v rámci evropské peněženky digitální identity;

c) bezpečně autentizovat evropskou peněženku digitální identity jiné osoby a přijímat a sdílet osobní identifikační údaje a elektronická potvrzení atributů zabezpečeným způsobem mezi dvěma evropskými peněženkami digitální identity;

d) přistupovat k záznamu všech transakcí provedených prostřednictvím evropské peněženky digitální identity, a to na základě společného přehledu, který uživateli umožní:

   i) zobrazit aktuální seznam spoléhajících se stran, s nimiž uživatel navázal spojení, a případně všech sdílených údajů;

   ii) snadno požádat o výmaz osobních údajů podle článku 17 nařízení (EU) 2016/679 spoléhající se stranou;

   iii) snadno nahlásit spoléhající se stranu vnitrostátnímu úřadu pro ochranu osobních údajů, pokud obdrží údajně protiprávní nebo podezřelou žádost o údaje;

e) podepisovat kvalifikovanými elektronickými podpisy nebo pečetit kvalifikovanými elektronickými pečetěmi;

f) v rozsahu, v jakém je to technicky proveditelné, stahovat údaje uživatele, elektronické potvrzení atributů a konfigurace;

g) uplatňovat práva uživatelů na přenositelnost údajů.

5. Evropské peněženky digitální identity zejména:

a) podporují společné protokoly a rozhraní:

   i) pro vydávání osobních identifikačních údajů, kvalifikovaných a nekvalifikovaných elektronických potvrzení atributů nebo kvalifikovaných a nekvalifikovaných certifikátů k dané evropské peněžence digitální identity;

   ii) pro spoléhající se strany, aby mohly požadovat a ověřovat platnost osobních identifikačních údajů a elektronických potvrzení atributů;

   iii) pro sdílení osobních identifikačních údajů, elektronických potvrzení atributů nebo výběrově zpřístupněných souvisejících údajů se spoléhajícími se stranám a pro jejich předkládání spoléhajícím se stranám, a to on-line a případně v off-line režimu;

iv) umožňující uživateli interakci s evropskou peněženkou digitální identity a zobrazení značky důvěry EU pro peněženku digitální identity;

v) pro bezpečné zapojení uživatele pomocí prostředků pro elektronickou identifikaci v souladu s čl. 5a odst. 24;

vi) pro interakci mezi evropskými peněženkami digitální identity dvou osob pro účely přijímání, ověřování platnosti a sdílení osobních identifikačních údajů a elektronických potvrzení atributů zabezpečeným způsobem;

vii) pro autentizaci a identifikaci spoléhajících se stran zavedením mechanismů autentizace v souladu s článkem 5b;

viii) umožňující spoléhajícím se stranám ověřit pravost a platnost evropských peněženek digitální identity;

ix) pro požádání spoléhající se strany o výmaz osobních údajů podle článku 17 nařízení (EU) 2016/679;

x) pro nahlášení spoléhající se strany příslušnému vnitrostátnímu úřadu pro ochranu osobních údajů, pokud je obdržena údajně protiprávní nebo podezřelá žádost o údaje;

xi) pro vytváření kvalifikovaných elektronických podpisů nebo elektronických pečetí pomocí prostředků pro vytváření kvalifikovaných elektronických podpisů nebo elektronických pečetí;

b) neposkytují žádné informace poskytovatelům služeb vytvářejících důvěru vydávajícím elektronická potvrzení atributů o používání těchto elektronických potvrzení;

c) zajišťují možnost autentizace a identifikace spoléhajících se stran zavedením mechanismů autentizace v souladu s článkem 5b;

d) splňují požadavky stanovené v článku 8, pokud jde o vysokou úroveň záruky, zejména co se týče požadavků na prokazování a ověřování totožnosti a správu a autentizaci prostředků pro elektronickou identifikaci;

e) v případě elektronického potvrzování atributů, jehož součástí jsou zásady zpřístupňování informací, zavádějí vhodný mechanismus informování uživatele o tom, že spoléhající se strana nebo uživatel evropské peněženky digitální identity, kteří žádají o elektronické potvrzení atributů, mají povolení přístupu k tomuto potvrzení;

f) zajišťují, aby osobní identifikační údaje, které jsou dostupné ze systému elektronické identifikace, v jehož rámci je evropská peněženka digitální identity poskytována, jedinečným způsobem identifikovaly fyzickou osobu, právnickou osobu nebo fyzickou osobu zastupující fyzickou či právnickou osobu a byly s touto evropskou peněženkou digitální identity spojeny;

g) poskytují standardně a bezplatně všem fyzickým osobám možnost podepisovat kvalifikovanými elektronickými podpisy.

Bez ohledu na první pododstavec písm. g) mohou členské státy stanovit přiměřená opatření k zajištění toho, aby bezplatné používání kvalifikovaných elektronických podpisů fyzickými osobami bylo omezeno na neprofesionální účely.

6. Členské státy bezodkladně informují uživatele o všech případech narušení bezpečnosti, které mohlo zcela nebo částečně ohrozit jejich evropské peněženky digitální identity nebo jejich obsah, zejména pokud vedlo k pozastavení nebo zrušení platnosti jejich evropských peněženek digitální identity podle článku 5e.

7. Aniž je dotčen článek 5f, mohou členské státy v souladu s vnitrostátním právem stanovit dodatečné funkce evropských peněženek digitální identity, včetně interoperability se stávajícími vnitrostátními prostředky pro elektronickou identifikaci. Tyto dodatečné funkce musí být v souladu s tímto článkem.

8. Členské státy zajistí bezplatné mechanismy ověřování platnosti s cílem:

a) zajistit, aby bylo možné ověřit pravost a platnost evropských peněženek digitální identity;

b) umožnit uživatelům ověřit pravost a platnost totožnosti spoléhajících se stran registrovaných v souladu s článkem 5b.

9. Členské státy zajistí, aby platnost evropské peněženky digitální identity mohla být zrušena za následujících okolností:

a) na výslovnou žádost uživatele;

b) pokud byla ohrožena bezpečnost evropské peněženky digitální identity;

c) v případě úmrtí uživatele nebo ukončení činnosti právnické osoby.

10. Poskytovatelé evropských peněženek digitální identity zajistí, aby uživatelé mohli snadno požádat o technickou podporu a hlásit technické problémy nebo jakékoli jiné incidenty, které mají negativní dopad na používání evropské peněženky digitální identity.

11. Evropské peněženky digitální identity jsou poskytovány v rámci systému elektronické identifikace s vysokou úrovní záruky.

12. Evropské peněženky digitální identity zajišťují bezpečnost již od fáze návrhu.

13. Vydávání, používání a rušení evropských peněženek digitální identity je pro všechny fyzické osoby bezplatné.

14. Uživatelé mají používání své evropské peněženky digitální identity a údajů v ní obsažených plně pod kontrolou. Poskytovatel evropské peněženky digitální identity neshromažďuje informace o používání evropské peněženky digitální identity, které nejsou nezbytné pro poskytování služeb evropské peněženky digitální identity, ani nekombinuje osobní identifikační údaje či jakékoli jiné uložené osobní údaje nebo údaje týkající se používání evropské peněženky digitální identity s osobními údaji z jiných služeb nabízených tímto poskytovatelem nebo ze služeb třetích stran, které nejsou nezbytné pro poskytování služeb evropské peněženky digitální identity, ledaže o to uživatel výslovně požádal. Osobní údaje týkající se poskytování evropské peněženky digitální identity jsou uchovávány logicky odděleně od jakýchkoli jiných údajů v držení poskytovatele evropské peněženky digitální identity. Pokud evropskou peněženku digitální identity poskytují soukromé strany v souladu s odst. 2 písm. b) a c) tohoto článku, použijí se přiměřeně ustanovení čl. 45h odst. 3.

15. Používání evropských peněženek digitální identity je dobrovolné. Fyzické či právnické osoby, které evropskou peněženku digitální identity nepoužívají, nesmí být v žádném případě omezovány ani znevýhodňovány v přístupu k veřejným a soukromým službám, přístupu na trh práce, ani pokud jde o svobodu podnikání. Přístup k veřejným a soukromým službám musí být i nadále možný za použití jiných stávajících prostředků identifikace a autentizace.

16. Technický rámec evropské peněženky digitální identity:

a) neumožňuje poskytovatelům elektronických potvrzení atributů ani žádné jiné straně po vydání potvrzení atributů získávat data umožňující sledovat transakce nebo chování uživatelů, propojovat je nebo mezi nimi vytvářet vztahy ani jiným způsobem získávat informace o transakcích nebo chování uživatelů, pokud to uživatel výslovně nepovolil;

b) umožňuje techniky ochrany soukromí, které zajišťují nepropojitelnost, pokud potvrzení atributů nevyžaduje identifikaci uživatele.

17. Veškeré zpracování osobních údajů prováděné členskými státy nebo jejich jménem subjekty nebo stranami odpovědnými za poskytování evropských peněženek digitální identity jako prostředku pro elektronickou identifikaci se provádí v souladu s vhodnými a účinnými opatřeními na ochranu údajů. Musí být prokázán soulad takového zpracování s nařízením (EU) 2016/679. Členské státy mohou zavést vnitrostátní ustanovení s cílem dále upřesnit uplatňování těchto opatření.

18. Členské státy bez zbytečného odkladu oznámí Komisi informace o:

a) subjektu odpovědném za zřízení a udržování seznamu registrovaných spoléhajících se stran, které využívají evropské peněženky digitální identity v souladu s čl. 5b odst. 5, a místu, na kterém se tento seznam nachází;

b) subjektech odpovědných za poskytování evropských peněženek digitální identity v souladu s čl. 5a odst. 1;

c) subjektech odpovědných za zajištění toho, aby osobní identifikační údaje byly spojeny s evropskou peněženkou digitální identity v souladu s čl. 5a odst. 5 písm. f);

d) mechanismu umožňujícím ověření platnosti osobních identifikačních údajů uvedených v čl. 5a odst. 5 písm. f) a totožnosti spoléhajících se stran;

e) mechanismu pro ověření pravosti a platnosti evropských peněženek digitální identity.

Komise zpřístupní informace oznámené podle prvního pododstavce veřejnosti prostřednictvím zabezpečeného kanálu v elektronicky podepsané nebo zapečetěné podobě vhodné pro automatizované zpracování.

19. Aniž je dotčen odstavec 22 tohoto článku, článek 11 se použije přiměřeně na evropskou peněženku digitální identity.

20. Ustanovení čl. 24 odst. 2 písm. b) a d) až h) se použije přiměřeně na poskytovatele evropské peněženky digitální identity.

21. Evropské peněženky digitální identity jsou přístupné pro použití osobami se zdravotním postižením na rovnoprávném základě s ostatními uživateli v souladu se směrnicí Evropského parlamentu a Rady (EU) 2019/882 (*).

22. Pro účely poskytování evropských peněženek digitální identity se na evropské peněženky digitální identity a systémy elektronické identifikace, v jejichž rámci jsou poskytovány, nevztahují požadavky stanovené v článcích 7, 9, 10, 12 a 12a.

23. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely požadavků uvedených v odstavcích 4, 5, 8 a 18 tohoto článku o zavedení evropské peněženky digitální identity. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

24. Komise stanoví prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví technické specifikace a postupy s cílem usnadnit zapojení uživatelů do používání evropské peněženky digitální identity za použití prostředků pro elektronickou identifikaci odpovídajících vysoké úrovni záruky, nebo prostředků pro elektronickou identifikaci odpovídajících značné úrovni záruky ve spojení s dalšími postupy vzdáleného zapojení, které společně splňují požadavky vysoké úrovně záruky. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 5b

Spoléhající se strany u evropských peněženek digitální identity

1. Pokud spoléhající se strana hodlá spoléhat na evropské peněženky digitální identity pro účely poskytování veřejných nebo soukromých služeb prostřednictvím digitální interakce, zaregistruje se v členském státě, v němž je usazena.

2. Proces registrace musí být nákladově efektivní a přiměřený riziku. Spoléhající se strana poskytne alespoň:

a) informace nezbytné k autentizaci evropských peněženek digitální identity, které zahrnují přinejmenším:

   i) členský stát, v němž je spoléhající se strana usazena a

ii) název spoléhající se strany a případně její registrační číslo uvedené v úředním záznamu spolu s identifikačními údaji tohoto úředního záznamu;

b) kontaktní údaje spoléhající se strany;

c) zamýšlené použití evropských peněženek digitální identity, včetně uvedení údajů, které spoléhající se strana bude požadovat od uživatelů.

3. Spoléhající se strany nesmí od uživatelů požadovat, aby poskytli jiné údaje než ty, které jsou uvedeny podle odst. 2 písm. c).

4. Odstavci 1 a 2 nejsou dotčena ustanovení práva Unie nebo vnitrostátního práva, která upravují poskytování konkrétních služeb.

5. Členské státy zpřístupní informace uvedené v odstavci 2 veřejnosti on-line v elektronicky podepsané nebo zapečetěné podobě vhodné pro automatizované zpracování.

6. Spoléhající se strany registrované v souladu s tímto článkem neprodleně informují členské státy o veškerých změnách informací poskytnutých při registraci podle odstavce 2.

7. Členské státy zajistí společný mechanismus umožňující identifikaci a autentizaci spoléhajících se stran, jak je uvedeno v čl. 5a odst. 5 písm. c).

8. Pokud spoléhající se strany hodlají spoléhat na evropské peněženky digitální identity, musí se vůči uživateli identifikovat.

9. Spoléhající se strany jsou odpovědné za provádění postupu pro autentizaci a ověření platnosti osobních identifikačních údajů a elektronického potvrzení atributů vyžádaných z evropských peněženek digitální identity. Spoléhající se strany neodmítnou použití pseudonymů, pokud identifikace uživatele není vyžadována právem Unie nebo vnitrostátním právem.

10. Zprostředkovatelé, kteří jednají jménem spoléhajících se stran, se považují za spoléhající se strany a neuchovávají údaje o obsahu transakce.

11. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcích aktů o zavedení evropské peněženky digitální identity, jak jsou uvedeny v čl. 5a odst. 23, technické specifikace a postupy pro požadavky uvedené v odstavcích 2, 5 a 6 až 9 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 5c

Certifikace evropských peněženek digitální identity

1. Shodu evropských peněženek digitální identity a systému elektronické identifikace, v jehož rámci jsou poskytovány, s požadavky stanovenými v čl. 5a odst. 4, 5 a 8, s požadavkem na logické oddělení stanoveným v čl. 5a odst. 14 a případně s normami a technickými specifikacemi uvedenými v čl. 5a odst. 24 certifikují subjekty posuzování shody určené členskými státy.

2. Certifikace shody evropských peněženek digitální identity s požadavky uvedenými v odstavci 1 tohoto článku nebo jejich částmi, které se týkají kybernetické bezpečnosti, se provádí v souladu s evropskými schématy certifikace kybernetické bezpečnosti zavedenými podle nařízení Evropského parlamentu a Rady (EU) 2019/881 (**) a uvedenými v prováděcích aktech uvedených v odstavci 6 tohoto článku.

3. Pokud jde o požadavky uvedené v odstavci 1 tohoto článku, které se netýkají kybernetické bezpečnosti, a požadavky uvedené v odstavci 1 tohoto článku, které se kybernetické bezpečnosti týkají, ale schémata certifikace kybernetické bezpečnosti uvedená v odstavci 2 tohoto článku se na ně nevztahují nebo se na ně vztahují pouze částečně, členské státy zavedou rovněž pro tyto požadavky v příslušném rozsahu vnitrostátní schémata certifikace v souladu s požadavky stanovenými v prováděcích aktech uvedených v odstavci 6 tohoto článku. Členské státy předají své návrhy vnitrostátních schémat certifikace skupině pro evropskou spolupráci v oblasti digitální identity zřízené podle čl. 46e odst. 1 (dále jen ‚skupina pro spolupráci'). Skupina pro spolupráci může vydávat stanoviska a doporučení.

4. Certifikace podle odstavce 1 je platná až po dobu pěti let, pokud se každé dva roky provádí hodnocení zranitelnosti. Je-li identifikována zranitelnost a není-li včas odstraněna, certifikace se zruší.

5. Soulad s požadavky stanovenými v článku 5a tohoto nařízení týkajícími se zpracování osobních údajů lze certifikovat podle nařízení (EU) 2016/679.

6. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a případně stanoví specifikace a postupy pro certifikaci evropských peněženek digitální identity uvedenou v odstavcích 1, 2 a 3 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

7. Členské státy sdělí Komisi názvy a adresy subjektů posuzování shody uvedených v odstavci 1. Komise tyto informace zpřístupní všem členským státům.

8. Komisi je svěřena pravomoc přijímat v souladu s článkem 47 akty v přenesené pravomoci, které stanoví zvláštní kritéria, která mají splňovat určené subjekty posuzování shody uvedené v odstavci 1 tohoto článku.

Článek 5d

Zveřejnění seznamu certifikovaných evropských peněženek digitální identity

1. Členské státy bez zbytečného odkladu informují Komisi a skupinu pro spolupráci zřízenou podle čl. 46e odst. 1 o evropských peněženkách digitální identity, které byly poskytnuty podle článku 5a a certifikovány subjekty posuzování shody uvedenými v čl. 5c odst. 1. V případě zrušení certifikace bez zbytečného odkladu informují Komisi a skupinu pro spolupráci zřízenou podle čl. 46e odst. 1 a uvedou důvody zrušení.

2. Aniž je dotčen čl. 5a odst. 18, informace poskytnuté členskými státy uvedené v odstavci 1 tohoto článku zahrnují alespoň:

a) certifikát a zprávu o posouzení certifikace certifikované evropské peněženky digitální identity;

b) popis systému elektronické identifikace, v jehož rámci je evropská peněženka digitální identity poskytována;

c) použitelný režim dohledu a informace o režimu odpovědnosti, pokud jde o stranu poskytující evropskou peněženku digitální identity;

d) orgán nebo orgány odpovědné za systém elektronické identifikace;

e) opatření k pozastavení platnosti nebo zrušení systému elektronické identifikace nebo autentizace či dotčených ohrožených součástí.

3. Na základě informací obdržených podle odstavce 1 Komise sestaví, zveřejní v *Úředním věstníku Evropské unie* a vede ve strojově čitelné podobě seznam certifikovaných evropských peněženek digitální identity.

4. Členský stát může Komisi požádat o vyřazení evropské peněženky digitální identity a systému elektronické identifikace, v jehož rámci je poskytována, ze seznamu uvedeného v odstavci 3.

5. V případě změn týkajících se informací poskytnutých podle odstavce 1 poskytne členský stát Komisi aktualizované informace.

6. Komise seznam uvedený v odstavci 3 aktualizuje zveřejněním odpovídajících změn seznamu v *Úředním věstníku Evropské unie* do jednoho měsíce od obdržení žádosti podle odstavce 4 nebo aktualizovaných informací podle odstavce 5.

7. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity, jak je uveden v čl. 5a odst. 23, formáty a postupy použitelné pro účely uvedené v odstavcích 1, 4 a 5 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 5e

Narušení bezpečnosti evropských peněženek digitální identity

1. Pokud jsou evropské peněženky digitální identity poskytované podle článku 5a nebo mechanismy ověření platnosti uvedené v čl. 5a odst. 8 nebo systém elektronické identifikace, v jehož rámci jsou evropské peněženky digitální identity poskytovány, narušeny nebo částečně ohroženy způsobem, který ovlivňuje jejich spolehlivost nebo spolehlivost jiných evropských peněženek digitální identity, členský stát, který evropské peněženky digitální identity poskytl, bez zbytečného odkladu poskytování a používání evropských peněženek digitální identity pozastaví.

Je-li to odůvodněno závažností narušení bezpečnosti nebo ohrožení uvedeného v prvním pododstavci, členský stát evropské peněženky digitální identity bez zbytečného odkladu stáhne.

Členský stát o stažení odpovídajícím způsobem informuje dotčené uživatele, jednotná kontaktní místa určená podle čl. 46c odst. 1, spoléhající se strany a Komisi.

2. Není-li narušení bezpečnosti nebo ohrožení uvedené v odst. 1 prvním pododstavci tohoto článku napraveno do tří měsíců od pozastavení, členský stát, který evropské peněženky digitální identity poskytl, evropské peněženky digitální identity stáhne a zruší jejich platnost. Členský stát o stažení odpovídajícím způsobem informuje dotčené uživatele, jednotná kontaktní místa určená podle čl. 46c odst. 1, spoléhající se strany a Komisi.

3. Pokud bylo narušení bezpečnosti nebo ohrožení bezpečnosti uvedené v odst. 1 prvním pododstavci tohoto článku napraveno, poskytující členský stát obnoví poskytování a používání evropských peněženek digitální identity a bez zbytečného odkladu o tom uvědomí dotčené uživatele a spoléhající se strany, jednotná kontaktní místa určená podle čl. 46c odst. 1 a Komisi.

4. Komise bez zbytečného odkladu zveřejní v *Úředním věstníku Evropské unie* odpovídající změny v seznamu uvedeném v článku 5d.

5. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro opatření uvedená v odstavcích 1, 2 a 3 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 5f

Přeshraniční využívání evropských peněženek digitální identity

1. Pokud členské státy pro přístup k on-line službě poskytované subjektem veřejného sektoru vyžadují elektronickou identifikaci a autentizaci, akceptují rovněž evropské peněženky digitální identity poskytnuté v souladu s tímto nařízením.

2. Pokud právo Unie nebo vnitrostátní právo vyžaduje od soukromých spoléhajících se stran, které poskytují služby – s výjimkou mikropodniků a malých podniků ve smyslu článku 2 přílohy doporučení Komise 2003/361/ES (***) – silnou autentizaci uživatele k on-line identifikaci nebo pokud takovou silnou autentizaci uživatele k on-line identifikaci vyžaduje smluvní závazek, a to i v oblasti dopravy, energetiky, bankovnictví, finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, vzdělávání nebo telekomunikací, uvedené soukromé spoléhající se strany do 36 měsíců ode dne vstupu prováděcích aktů uvedených v čl. 5a odst. 23 a čl. 5c odst. 6 v platnost a pouze na dobrovolnou žádost uživatele začnou akceptovat rovněž evropské peněženky digitální identity poskytnuté v souladu s tímto nařízením.

3. V případech, kdy poskytovatelé velmi velkých on-line platforem uvedených v článku 33 nařízení Evropského parlamentu a Rady (EU) 2022/2065 (****) vyžadují autentizaci uživatelů pro přístup k on-line službám, tito poskytovatelé pro autentizaci uživatele rovněž akceptují a usnadňují používání evropských peněženek digitální identity poskytnutých v souladu s tímto nařízením, a to pouze na dobrovolnou žádost uživatele a s ohledem na minimální údaje nezbytné pro konkrétní on-line službu, pro kterou se autentizace požaduje.

4. Komise ve spolupráci s členskými státy usnadní vypracování kodexů chování v úzké spolupráci se všemi příslušnými zúčastněnými stranami, včetně občanské společnosti, s cílem přispět k široké dostupnosti a použitelnosti evropských peněženek digitální identity v oblasti působnosti tohoto nařízení a podpořit poskytovatele služeb, aby dokončili vypracování kodexů chování.

5. Do 24 měsíců od zavedení evropských peněženek digitální identity vyhodnotí Komise poptávku po evropských peněženkách digitální identity a jejich dostupnost a použitelnost, s přihlédnutím ke kritériím, jako jsou rozšíření mezi uživateli, přeshraniční přítomnost poskytovatelů služeb, technologický vývoj, vývoj způsobů využívání a poptávka spotřebitelů.

(*) Směrnice Evropského parlamentu a Rady (EU) 2019/882 ze dne 17. dubna 2019 o požadavcích na přístupnost u výrobků a služeb (Úř. věst. L 151, 7.6.2019, s. 70).

(**) 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).

(***) Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

(****) Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách) (Úř. věst. L 277, 27.10.2022, s. 1)."

6) Před článek 6 se vkládá nadpis, který zní:

„ODDÍL 2

SYSTÉMY ELEKTRONICKÉ IDENTIFIKACE".

7) V článku 7 se písmeno g) nahrazuje tímto:

„g) nejméně šest měsíců před oznámením podle čl. 9 odst. 1 poskytne oznamující členský stát ostatním členským státům pro účely čl. 12 odst. 5 popis daného systému v souladu s procesními opatřeními stanovenými v prováděcích aktech přijatých podle čl. 12 odst. 6;".

8) V čl. 8 odst. 3 se první pododstavec nahrazuje tímto:

„3. Do 18. září 2015 Komise prostřednictvím prováděcích aktů s přihlédnutím k příslušným mezinárodním normám a s výhradou odstavce 2 stanoví minimální technické specifikace, normy a postupy, jejichž pomocí jsou vymezeny nízká, značná a vysoká úroveň záruky prostředků pro elektronickou identifikaci."

9) V článku 9 se odstavce 2 a 3 nahrazují tímto:

„2. Komise bez zbytečného odkladu zveřejní v *Úředním věstníku Evropské unie* seznam systémů elektronické identifikace, které byly oznámeny podle odstavce 1, spolu se základními informacemi o těchto systémech.

3. Komise zveřejní v *Úředním věstníku Evropské unie* změny seznamu uvedeného v odstavci 2 do jednoho měsíce od obdržení daného oznámení."

10) V článku 10 se nadpis nahrazuje tímto:

„Narušení bezpečnosti systémů elektronické identifikace".

11) Vkládá se nový článek, který zní:

„Článek 11a

Přeshraniční párování totožnosti

1. Pokud členské státy jednají jako spoléhající se strany pro účely přeshraničních služeb, zajistí jednoznačné párování totožnosti fyzických osob používajících oznámené prostředky pro elektronickou identifikaci nebo evropské peněženky digitální identity.

2. Členské státy stanoví technická a organizační opatření s cílem zajistit vysokou úroveň ochrany osobních údajů používaných pro párování totožnosti a zabránit profilování uživatelů.

3. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro požadavky uvedené v odstavci 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

12) Článek 12 se mění takto:

a) název se nahrazuje tímto:

„Interoperabilita“;

b) odstavec 3 se mění takto:

i) písmeno c) se nahrazuje tímto:

„c) usnadňuje zavádění ochrany soukromí a bezpečnosti již od fáze návrhu;“;

ii) písmeno d) se zrušuje;

c) v odstavci 4 se písmeno d) nahrazuje tímto:

„d) odkazu na minimální soubor osobních identifikačních údajů nezbytných k jedinečné identifikaci fyzické nebo právnické osoby nebo fyzické osoby zastupující jinou fyzickou či právnickou osobu, který je v systémech elektronické identifikace k dispozici;“;

d) odstavce 5 a 6 se nahrazují tímto:

„5. Členské státy provádějí vzájemná hodnocení systémů elektronické identifikace, které spadají do oblasti působnosti tohoto nařízení a jsou oznamovány podle čl. 9 odst. 1 písm. a).

6. Do 18. března 2025 stanoví Komise prostřednictvím prováděcích aktů nezbytná procesní opatření pro vzájemná hodnocení uvedená v odstavci 5 tohoto článku v zájmu podpory vysoké úrovně důvěry a bezpečnosti odpovídající míře rizika. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

e) odstavec 7 se zrušuje;

f) odstavec 8 se nahrazuje tímto:

„8. Do 18. září 2025 přijme Komise za účelem stanovení jednotných podmínek pro provádění požadavku podle odstavce 1 tohoto článku, s výhradou kritérií stanovených v odstavci 3 tohoto článku a s přihlédnutím k výsledkům spolupráce mezi členskými státy, prováděcí akty týkající se rámce interoperability stanoveného v odstavci 4 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

13) V kapitole II se vkládají nové články, které znějí:

„Článek 12a

Certifikace systémů elektronické identifikace

1. Shodu systémů elektronické identifikace, které mají být oznámeny, s požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení, včetně souladu s příslušnými požadavky na kybernetickou bezpečnost stanovenými v čl. 8 odst. 2, pokud jde o úrovně záruky systémů elektronické identifikace, certifikují subjekty posuzování shody určené členskými státy.

2. Certifikace podle odstavce 1 tohoto článku se provádí v rámci příslušného schématu certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881 nebo jeho částí, pokud se certifikát kybernetické bezpečnosti nebo jeho části vztahují na uvedené požadavky kybernetické bezpečnosti.

3. Certifikace podle odstavce 1 je platná až po dobu pěti let, pokud se každé dva roky provádí hodnocení zranitelnosti. Je-li identifikována zranitelnost a není-li do tří měsíců od uvedené identifikace odstraněna, certifikace se zruší.

4. Bez ohledu na odstavec 2 mohou členské státy v souladu s uvedeným odstavcem požadovat od oznamujícího členského státu doplňující informace o systémech elektronické identifikace nebo jejich částech, které byly certifikovány.

5. Vzájemné hodnocení systémů elektronické identifikace uvedené v čl. 12 odst. 5 se nevztahuje na systémy elektronické identifikace nebo na části těchto systémů certifikované v souladu s odstavcem 1 tohoto článku. Členské státy mohou použít certifikát nebo prohlášení o shodě vydané v souladu s příslušným schématem certifikace nebo částmi takových schémat s požadavky stanovenými v čl. 8 odst. 2, které se netýkají kybernetické bezpečnosti, pokud jde o úroveň záruky systémů elektronické identifikace.

6. Členské státy sdělí Komisi názvy a adresy subjektů posuzování shody uvedených v odstavci 1. Komise tyto informace zpřístupní všem členským státům.

Článek 12b

Přístup k funkcím hardwaru a softwaru

Pokud jsou poskytovatelé evropských peněženek digitální identity a vydavatelé oznámených prostředků pro elektronickou identifikaci, kteří jednají v rámci obchodní nebo profesní činnosti a využívají hlavní služby platforem ve smyslu čl. 2 bodu 2 nařízení Evropského parlamentu a Rady (EU) 2022/1925 (*) pro účely poskytování nebo v průběhu poskytování služeb evropské peněženky digitální identity a prostředků pro elektronickou identifikaci koncovým uživatelům, podnikatelskými uživateli ve smyslu čl. 2 bodu 21 uvedeného nařízení, umožní jim strážci přístupu zejména účinnou interoperabilitu se stejným operačním systémem, hardwarovými nebo softwarovými prvky a přístup k nim pro účely interoperability. Tato účinná interoperabilita a přístup musí být umožněny bezplatně a bez ohledu na to, zda jsou hardwarové nebo softwarové prvky součástí operačního systému, zda jsou dostupné strážci přístupu nebo zda jsou strážcem přístupu používané při poskytování těchto služeb ve smyslu čl. 6 odst. 7 nařízení (EU) 2022/1925. Tímto článkem není dotčen čl. 5a odst. 14 tohoto nařízení.

(*) Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích) (Úř. věst. L 265, 12.10.2022, s. 1).“

14) V článku 13 se odstavec 1 nahrazuje tímto:

„1. Bez ohledu na odstavec 2 tohoto článku, a aniž je dotčeno nařízení (EU) 2016/679 poskytovatelé služeb vytvářejících důvěru odpovídají za újmu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle tohoto nařízení. Každá fyzická nebo právnická osoba, která v důsledku porušení tohoto nařízení poskytovatelem služeb vytvářejících důvěru utrpěla hmotnou či nehmotnou újmu, má právo požadovat náhradu újmy v souladu s právem Unie a vnitrostátním právem.

Důkazní břemeno, pokud jde o úmysl nebo nedbalost nekvalifikovaného poskytovatele služeb vytvářejících důvěru, nese fyzická nebo právnická osoba uplatňující nárok na náhradu škody podle prvního pododstavce.

V případě kvalifikovaného poskytovatele služeb vytvářejících důvěru se úmysl nebo nedbalost předpokládá, pokud daný kvalifikovaný poskytovatel služeb vytvářejících důvěru neprokáže, že újma podle prvního pododstavce nastala bez jeho úmyslu nebo nedbalosti.“

15) Články 14, 15 a 16 se nahrazují tímto:

„Článek 14

Mezinárodní aspekty

1. Služby vytvářející důvěru poskytované poskytovateli služeb vytvářejících důvěru usazenými ve třetí zemi či mezinárodní organizací se uznávají jako právně rovnocenné kvalifikovaným službám vytvářejícím důvěru poskytovaným kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými v Unii, pokud jsou služby vytvářející důvěru pocházející ze třetí země nebo mezinárodní organizace uznány prostřednictvím prováděcích aktů nebo dohody uzavřené mezi Unií a třetí zemí nebo mezinárodní organizací v souladu s článkem 218 Smlouvy o fungování EU.

Prováděcí akty uvedené v prvním pododstavci se přijímají přezkumným postupem podle čl. 48 odst. 2.

2. Prováděcí akty a dohody uvedené v odstavci 1 zajistí, že poskytovatelé služeb vytvářejících důvěru usazení ve třetí zemi nebo mezinárodní organizace a jimi poskytované služby vytvářející důvěru splňují požadavky vztahující se na kvalifikované poskytovatele služeb vytvářejících důvěru usazené v Unii a jimi poskytované kvalifikované služby vytvářející důvěru. Třetí země a mezinárodní organizace zejména sestaví, spravují a zveřejňují důvěryhodný seznam uznaných poskytovatelů služeb vytvářejících důvěru.

3. Dohody uvedené v odstavci 1 zajistí, že kvalifikované služby vytvářející důvěru poskytované kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými v Unii jsou uznány jako právně rovnocenné službám vytvářejícím důvěru poskytovaným poskytovateli služeb vytvářejících důvěru ve třetí zemi nebo mezinárodní organizací, s níž je dohoda uzavřena.

Článek 15

Přístupnost pro osoby se zdravotním postižením a zvláštními potřebami

Poskytování prostředků pro elektronickou identifikaci, služeb vytvářejících důvěru a produktů pro koncové uživatele, které jsou používány při poskytování těchto služeb, se zpřístupní jednoduchým a srozumitelným jazykem, v souladu s Úmluvou Organizace spojených národů o právech osob se zdravotním postižením a s požadavky na přístupnost obsaženými ve směrnici (EU) 2019/882, z čehož mají prospěch i osoby s funkčními omezeními, jako jsou starší osoby a osoby s omezeným přístupem k digitálním technologiím.

Článek 16

Sankce

1. Aniž je dotčen článek 31 směrnice Evropského parlamentu a Rady (EU) 2022/2555 (*), členské státy stanoví sankce za porušení tohoto nařízení. Tyto sankce musí být účinné, přiměřené a odrazující.

2. Členské státy zajistí, aby porušení tohoto nařízení kvalifikovanými a nekvalifikovanými poskytovateli služeb vytvářejících důvěru podléhalo správním pokutám v maximální výši alespoň:

a) 5 000 000 EUR, je-li poskytovatelem služeb vytvářejících důvěru fyzická osoba; nebo

b) je-li poskytovatelem služeb vytvářejících důvěru právnická osoba, 5 000 000 EUR nebo 1 % celkového celosvětového ročního obratu podniku, k němuž poskytovatel služeb vytvářejících důvěru patřil v účetním období předcházejícím roku, v němž došlo k porušení, podle toho, která hodnota je vyšší.

3. V závislosti na právním systému členských států lze pravidla pro správní pokuty uplatnit tak, aby podnět k pokutě dával příslušný orgán dohledu a ukládaly ji příslušné vnitrostátní soudy. Uplatňování těchto pravidel v uvedených členských státech zajistí, aby tyto právní prostředky byly účinné a měly rovnocenný účinek jako správní pokuty ukládané přímo orgány dohledu.

(*) 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).“

16) V kapitole III oddíle 2 se název nahrazuje tímto:

„Nekvalifikovaní poskytovatelé služeb vytvářející důvěru“;

17) Články 17 a 18 se zrušují.

18) Do kapitoly III oddílu 2 se vkládá nový článek, který zní:

„Článek 19a

Požadavky na nekvalifikované poskytovatele služeb vytvářejících důvěru

1. Nekvalifikovaný poskytovatel služeb vytvářejících důvěru poskytující nekvalifikované služby vytvářející důvěru:

a) má vhodné politiky a přijímá odpovídající opatření pro řízení právních, obchodních, provozních a jiných přímých nebo nepřímých rizik spojených s poskytováním nekvalifikované služby vytvářející důvěru, která bez ohledu na článek 21 směrnice (EU) 2022/2555 zahrnují alespoň opatření týkající se:

i) registrace ke službě vytvářející důvěru a zapojení do jejího používání;

ii) procesních nebo správních kontrol potřebných k poskytování služeb vytvářejících důvěru;

iii) řízení a provádění služeb vytvářejících důvěru;

b) oznámí orgánu dohledu, identifikovatelným dotčeným osobám, veřejnosti, pokud je to ve veřejném zájmu, a případně dalším relevantním příslušným orgánům veškerá narušení bezpečnosti nebo narušení poskytování služby nebo provádění opatření uvedených v písm. a) bodech i), ii) nebo iii), která mají významný dopad na poskytovanou službu vytvářející důvěru nebo na osobní údaje v ní uchovávané, a to bez zbytečného odkladu a v každém případě nejpozději do 24 hodin poté, co se o jakýchkoli narušeních bezpečnosti nebo jiných narušeních dozvěděl.

2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely odst. 1 písm. a) tohoto článku. Pokud jsou tyto normy, specifikace a postupy splněny, předpokládá se shoda s požadavky stanovenými v tomto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

19) Článek 20 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru se na vlastní náklady alespoň jednou za 24 měsíců podrobí auditu ze strany subjektu posuzování shody. Audit potvrdí, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení a článku 21 směrnice (EU) 2022/2555. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru předloží výslednou zprávu o posouzení shody orgánu dohledu do tří pracovních dnů od jejího obdržení.“;

b) vkládají se nové odstavce, které znějí:

„1a. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru informují orgán dohledu o plánovaných auditech alespoň jeden měsíc předem a na požádání umožní účast orgánu dohledu jako pozorovatele.

1b. Členské státy oznámí Komisi bez zbytečného odkladu názvy, adresy a údaje o akreditaci subjektů posuzování shody uvedených v odstavci 1 a veškeré jejich následné změny. Komise tyto informace zpřístupní všem členským státům.“;

c) odstavce 2, 3 a 4 se nahrazují tímto:

„2. Aniž je dotčen odstavec 1, může orgán dohledu u kvalifikovaných poskytovatelů služeb vytvářejících důvěru na jejich náklady kdykoli provést audit nebo požádat subjekt posuzování shody o provedení posouzení shody za účelem potvrzení, že oni sami i jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení. Jestliže podle všeho došlo k porušení pravidel týkajících se ochrany osobních údajů, informuje orgán dohledu bez zbytečného odkladu příslušné dozorové úřady zřízené podle článku 51 nařízení (EU) 2016/679.

3. Pokud kvalifikovaný poskytovatel služeb vytvářejících důvěru nesplňuje některý z požadavků stanovených tímto nařízením, orgán dohledu ho požádá, aby v případně stanovené lhůtě zjednal nápravu.

Pokud tento poskytovatel nezjedná nápravu, a to ve lhůtě případně stanovené orgánem dohledu, orgán dohledu, je-li to odůvodněno zejména rozsahem, délkou trvání a důsledky daného neplnění, odejme danému poskytovateli nebo dotčené službě, kterou poskytuje, status kvalifikovaného poskytovatele nebo kvalifikované služby.

3a. Pokud příslušné orgány určené nebo zřízené podle čl. 8 odst. 1 směrnice (EU) 2022/2555 informují orgán dohledu o tom, že kvalifikovaný poskytovatel služeb vytvářejících důvěru nesplňuje některý z požadavků stanovených v článku 21 uvedené směrnice, orgán dohledu, je-li to odůvodněno zejména rozsahem, délkou trvání a důsledky daného neplnění, odejme danému poskytovateli nebo dotčené službě, kterou poskytuje, status kvalifikovaného poskytovatele nebo kvalifikované služby.

3b. Pokud dozorové úřady zřízené podle článku 51 nařízení (EU) 2016/679 informují orgán dohledu o tom, že kvalifikovaný poskytovatel služeb vytvářejících důvěru nesplňuje některý z požadavků stanovených v uvedeném nařízení, orgán dohledu, je-li to odůvodněno zejména rozsahem, délkou trvání a důsledky daného neplnění, odejme danému poskytovateli nebo dotčené službě, kterou poskytuje, status kvalifikovaného poskytovatele nebo kvalifikované služby.

3c. Orgán dohledu vyrozumí daného kvalifikovaného poskytovatele služeb vytvářejících důvěru o odnětí statusu kvalifikovaného poskytovatele nebo kvalifikované služby. Orgán dohledu informuje subjekt oznámený podle čl. 22 odst. 3 tohoto nařízení pro účely aktualizace důvěryhodných seznamů uvedených v odstavci 1 uvedeného článku a příslušný orgán určený nebo zřízený podle čl. 8 odst. 1 směrnice (EU) 2022/2555.

4. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro:

a) akreditaci subjektů posuzování shody a pro zprávy o posouzení shody podle odstavce 1;

b) požadavky na audit, podle nichž budou subjekty posuzování shody provádět posuzování shody, včetně kombinovaného posuzování, kvalifikovaných poskytovatelů služeb vytvářejících důvěru podle odstavce 1;

c) režimy posuzování shody vztahující se na posuzování shody kvalifikovaných poskytovatelů služeb vytvářejících důvěru prováděné subjekty posuzování shody a na předkládání zpráv uvedených v odstavci 1.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

20) Článek 21 se mění takto:

a) odstavce 1 a 2 se nahrazují tímto:

„1. Pokud poskytovatelé služeb vytvářejících důvěru hodlají začít poskytovat kvalifikovanou službu vytvářející důvěru, oznámí orgánu dohledu svůj úmysl spolu se zprávou o posouzení shody vydanou subjektem posuzování shody, která potvrzuje splnění požadavků stanovených v tomto nařízení a v článku 21 směrnice (EU) 2022/2555.

2. Orgán dohledu ověří, zda poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení, zejména požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru a na jimi poskytované kvalifikované služby vytvářející důvěru.

Za účelem ověření, zda poskytovatel služeb vytvářejících důvěru splňuje požadavky stanovené v článku 21 směrnice (EU) 2022/2555, požádá orgán dohledu příslušné orgány určené nebo zřízené podle čl. 8 odst. 1 uvedené směrnice, aby k tomu provedly opatření dohledu a poskytly informace o výsledku bez zbytečného odkladu a v každém případě do dvou měsíců od obdržení této žádosti. Není-li ověření dokončeno do dvou měsíců od oznámení, vyrozumí uvedené příslušné orgány orgán dohledu a uvedou důvody prodlení a dobu, v níž bude ověřování dokončeno.

Dospěje-li orgán dohledu k závěru, že poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení, udělí orgán dohledu tomuto poskytovateli služeb vytvářejících důvěru a jím poskytovaným službám vytvářejícím důvěru status kvalifikovaného poskytovatele a kvalifikované služby a uvědomí o tom subjekt uvedený v čl. 22 odst. 3 za účelem aktualizace důvěryhodných seznamů podle čl. 22 odst. 1, a to nejpozději do tří měsíců od obdržení oznámení podle odstavce 1 tohoto článku.

Není-li ověření dokončeno do tří měsíců od oznámení, vyrozumí orgán dohledu poskytovatele služeb vytvářejících důvěru a uvede důvody prodlení a dobu, v níž bude ověřování dokončeno.“;

b) odstavec 4 se nahrazuje tímto:

„4. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů formáty a postupy oznamování a ověřování pro účely odstavců 1 a 2 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

21) Článek 24 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Při vydávání kvalifikovaného certifikátu nebo kvalifikovaného elektronického potvrzení atributů ověří kvalifikovaný poskytovatel služeb vytvářejících důvěru totožnost a případně zvláštní atributy fyzické nebo právnické osoby, jimž se má kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů vydat.

1a. Kvalifikovaný poskytovatel služeb vytvářejících důvěru provede ověření totožnosti uvedené v odstavci 1 vhodným způsobem buď přímo, nebo prostřednictvím třetí strany, a to na základě jedné z těchto metod nebo případně jejich kombinace a v souladu s prováděcími akty uvedenými v odstavci 1c:

a) prostřednictvím evropské peněženky digitální identity nebo oznámených prostředků pro elektronickou identifikaci, které splňují požadavky stanovené v článku 8, pokud jde o vysokou úroveň záruky;

b) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaných v souladu s písmeny a), c) nebo d);

c) použitím jiných metod identifikace, které zajišťují identifikaci osoby s vysokou úrovní spolehlivosti, jejichž shodu potvrdí subjekt posuzování shody;

d) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby pomocí vhodných důkazů a postupů v souladu s vnitrostátním právem.

1b. Kvalifikovaný poskytovatel služeb vytvářejících důvěru provede ověření atributů uvedené v odstavci 1 vhodným způsobem buď přímo, nebo prostřednictvím třetí strany, a to na základě jedné z těchto metod nebo případně jejich kombinace a v souladu s prováděcími akty uvedenými v odstavci 1c:

a) prostřednictvím evropské peněženky digitální identity nebo oznámených prostředků pro elektronickou identifikaci, které splňují požadavky stanovené v článku 8, pokud jde o vysokou úroveň záruky;

b) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaných v souladu s odst. 1a písm. a), c) nebo d);

c) pomocí kvalifikovaného elektronického potvrzení atributů;

d) použitím jiných metod, které zajišťují ověření atributů s vysokou úrovní spolehlivosti, jejichž shodu potvrdí subjekt posuzování shody;

e) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby pomocí vhodných důkazů a postupů v souladu s vnitrostátním právem.

1c. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely ověřování totožnosti a atributů v souladu s odstavci 1, 1a a 1b tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

b) odstavec 2 se mění takto:

i) písmeno a) se nahrazuje tímto:

„a) informuje orgán dohledu alespoň jeden měsíc před provedením jakékoli změny v poskytování svých kvalifikovaných služeb vytvářejících důvěru nebo tři měsíce v případě záměru ukončit tyto činnosti;“;

ii) písmena d) a e) se nahrazují tímto:

„d) před uzavřením smluvního vztahu informuje jasným, srozumitelným a jednoduše přístupným způsobem, ve veřejně dostupném prostoru a individuálně každou osobu, která chce využít kvalifikovanou službu vytvářející důvěru, o přesných podmínkách používání této služby, včetně případných omezení jejího využívání;

e) používá důvěryhodné systémy a produkty, které jsou chráněny proti pozměnění, a zajišťuje technickou bezpečnost a spolehlivost procesů, které podporují, včetně použití vhodných kryptografických technik;“;

iii) vkládají se nová písmena, která znějí:

„fa) bez ohledu na článek 21 směrnice (EU) 2022/2555 má vhodné politiky a přijímá odpovídající opatření pro řízení právních, obchodních, provozních a jiných přímých nebo nepřímých rizik poskytování kvalifikované služby vytvářející důvěru, zahrnující alespoň opatření týkající se:

i) registrace ke službě a zapojení do jejího používání;

ii) procesních nebo správních kontrol;

iii) řízení a provádění služeb;

fb) oznámí orgánu dohledu, identifikovatelným dotčeným osobám, případně dalším relevantním příslušným orgánům a na žádost orgánu dohledu veřejnosti, pokud je to ve veřejném zájmu, veškerá narušení bezpečnosti nebo narušení poskytování služby nebo provádění opatření uvedených v písm. fa) bodech i), ii) nebo iii), která mají významný dopad na poskytovanou službu vytvářející důvěru nebo na osobní údaje v ní uchovávané, a to bez zbytečného odkladu a v každém případě do 24 hodin poté, co došlo k incidentu;“;

iv) písmena g), h) a i) se nahrazují tímto:

„g) přijímá vhodná opatření proti padělání, odcizení nebo zneužití dat nebo neoprávněnému vymazání, pozměnění nebo znepřístupnění dat;

h) po nezbytně dlouhou dobu poté, co ukončil svou činnost kvalifikovaného poskytovatele služeb vytvářejících důvěru, eviduje a zpřístupňuje veškeré příslušné informace týkající se dat, která vydal a obdržel, pro účely poskytnutí důkazů v soudním a správním řízení a pro účely zajištění kontinuity služby. Tato evidence může mít elektronickou podobu;

i) má k dispozici aktualizovaný plán ukončení činnosti k zajištění kontinuity služby v souladu s ustanoveními ověřenými orgánem dohledu podle čl. 46b odst. 4 písm. i);“;

v) písmeno j) se zrušuje;

vi) doplňuje se nový pododstavec, který zní:

„Orgán dohledu si může vyžádat informace nad rámec informací, které jsou mu oznamovány v souladu s prvním pododstavcem písm. a), nebo výsledek posouzení shody a může stanovit podmínky pro udělení povolení k provedení zamýšlených změn kvalifikovaných služeb vytvářejících důvěru. Není-li ověření dokončeno do tří měsíců od oznámení, vyrozumí orgán dohledu poskytovatele služeb vytvářejících důvěru a uvede důvody prodlení a dobu, v níž bude ověřování dokončeno.“;

c) odstavec 5 se nahrazuje tímto:

„4a. Odstavce 3 a 4 se odpovídajícím způsobem použijí na zneplatnění kvalifikovaných elektronických potvrzení atributů.

4b. Komisi je svěřena pravomoc přijímat v souladu s článkem 47 akty v přenesené pravomoci, které stanoví dodatečná opatření uvedená v odst. 2 písm. fa) tohoto článku.

5. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely požadavků uvedených v odstavci 2 tohoto článku. Pokud jsou tyto normy, specifikace a postupy splněny, předpokládá se shoda s požadavky stanovenými v tomto odstavci. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

22) V kapitole III oddílu 3 se vkládá nový článek, který zní:

„Článek 24a

Uznávání kvalifikovaných služeb vytvářejících důvěru

1. Kvalifikované elektronické podpisy založené na kvalifikovaném certifikátu vydaném v jednom členském státě se ve všech ostatních členských státech uznávají jako kvalifikované elektronické podpisy a kvalifikované elektronické pečeti založené na kvalifikovaném certifikátu vydaném v jednom členském státě se ve všech ostatních členských státech uznávají jako kvalifikované elektronické pečeti.

2. Kvalifikované prostředky pro vytváření elektronických podpisů certifikované v jednom členském státě se ve všech ostatních členských státech uznávají jako kvalifikované prostředky pro vytváření elektronických podpisů a kvalifikované prostředky pro vytváření elektronických pečetí certifikované v jednom členském státě se ve všech ostatních členských státech uznávají jako kvalifikované prostředky pro vytváření elektronických pečetí.

3. Kvalifikovaný certifikát pro elektronické podpisy, kvalifikovaný certifikát pro elektronické pečeti, kvalifikovaná služba vytvářející důvěru pro správu kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku a kvalifikovaná služba vytvářející důvěru pro správu kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku, poskytované v jednom členském státě se ve všech ostatních členských státech uznávají jako kvalifikovaný certifikát pro elektronické podpisy, kvalifikovaný certifikát pro elektronické pečeti, kvalifikovaná služba vytvářející důvěru pro správu kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku a kvalifikovaná služba vytvářející důvěru pro správu kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku.

4. Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických pečetí, poskytované v jednom členském státě se ve všech ostatních členských státech uznávají jako kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických pečetí.

5. Kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů a kvalifikovaná služba uchovávání kvalifikovaných elektronických pečetí poskytované v jednom členském státě se ve všech ostatních členských státech uznávají jako kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů a kvalifikovaná služba uchovávání kvalifikovaných elektronických pečetí.

6. Kvalifikované elektronické časové razítko poskytnuté v jednom členském státě se ve všech ostatních členských státech uznává jako kvalifikované elektronické časové razítko.

7. Kvalifikovaný certifikát pro autentizaci internetových stránek vydaný v jednom členském státě se ve všech ostatních členských státech uznává jako kvalifikovaný certifikát pro autentizaci internetových stránek.

8. Kvalifikovaná služba elektronického doporučeného doručování poskytovaná v jednom členském státě se ve všech ostatních členských státech uznává jako kvalifikovaná služba elektronického doporučeného doručování.

9. Kvalifikované elektronické potvrzení atributů vydané v jednom členském státě se ve všech ostatních členských státech uznává jako kvalifikované elektronické potvrzení atributů.

10. Kvalifikovaná služba elektronické archivace poskytovaná v jednom členském státě se ve všech ostatních členských státech uznává jako kvalifikovaná služba elektronické archivace.

11. Kvalifikovaná elektronická kniha záznamů poskytovaná v jednom členském státě se ve všech ostatních členských státech uznává jako kvalifikovaná elektronická kniha záznamů.“

23) V článku 25 se zrušuje odstavec 3.

24) Článek 26 se mění takto:

a) dosavadní jediný odstavec se označuje jako odstavec 1;

b) doplňuje se nový odstavec, který zní:

„2. Do 21. května 2026 Komise posoudí, zda je nezbytné přijmout prováděcí akty, kterými se stanoví seznam referenčních norem a kterými se v případě potřeby stanoví specifikace a postupy pro zaručené elektronické podpisy. Na základě tohoto posouzení může Komise takové prováděcí akty přijmout. Pokud zaručený elektronický podpis splňuje normy, specifikace a postupy, předpokládá se shoda s požadavky na zaručené elektronické podpisy. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

25) V článku 27 se zrušuje odstavec 4.

26) V článku 28 se odstavec 6 nahrazuje tímto:

„6. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro kvalifikované certifikáty pro elektronický podpis. Pokud kvalifikovaný certifikát pro elektronický podpis splňuje normy, specifikace a postupy, předpokládá se shoda s požadavky stanovenými v příloze I. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

27) V článku 29 se vkládá nový odstavec, který zní:

„1a. Vytvářet nebo spravovat data pro vytváření elektronických podpisů či tato data kopírovat pro účely zálohování lze pouze jménem podepisující osoby a na její žádost a může tak činit pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který poskytuje kvalifikovanou službu vytvářející důvěru pro správu kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku.“

28) Vkládá se nový článek, který zní:

„Článek 29a

Požadavky na kvalifikovanou službu správy kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku

1. Správu kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku jako kvalifikované služby provádí pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který:

a) vytváří nebo spravuje data pro vytváření elektronických podpisů jménem podepisující osoby;

b) bez ohledu na přílohu II bod 1 písm. d) kopíruje data pro vytváření elektronických podpisů pouze pro účely zálohování, jsou-li splněny tyto požadavky:

i) bezpečnost zkopírovaných souborů dat je na stejné úrovni jako u původních souborů dat;

ii) počet zkopírovaných souborů dat nesmí přesáhnout minimum potřebné pro zajištění kontinuity služby;

c) splňuje všechny požadavky uvedené v certifikační zprávě konkrétního kvalifikovaného prostředku pro vytváření elektronických podpisů na dálku vydané podle článku 30.

2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely odstavce 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

29) V článku 30 se vkládá nový odstavec, který zní:

„3a. Platnost certifikace uvedené v odstavci 1 nesmí překročit pět let, přičemž se každé dva roky provádí hodnocení zranitelnosti. Jsou-li identifikovány zranitelnosti a nejsou-li odstraněny, certifikace se zruší.“

30) V článku 31 se odstavec 3 nahrazuje tímto:

„3. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů formáty a postupy použitelné pro účely odstavce 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

31) Článek 32 se mění takto:

a) v odstavci 1 se doplňuje nový pododstavec, který zní:

„Pokud ověřování platnosti kvalifikovaných elektronických podpisů splňuje normy, specifikace a postupy uvedené v odstavci 3, předpokládá se shoda s požadavky stanovenými v prvním pododstavci tohoto odstavce.“

b) odstavec 3 se nahrazuje tímto:

„3. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely ověřování platnosti kvalifikovaných elektronických podpisů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

32) Vkládá se nový článek, který zní:

„Článek 32a

Požadavky na ověřování platnosti zaručených elektronických podpisů založených na kvalifikovaných certifikátech

1. Postup ověření platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu potvrdí platnost zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, pokud:

a) certifikát, na němž je podpis založen, byl v okamžiku podpisu kvalifikovaným certifikátem pro elektronický podpis, jenž je v souladu s přílohou I;

b) kvalifikovaný certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a v okamžiku podpisu byl platný;

c) data pro ověřování platnosti podpisu odpovídají datům poskytnutým spoléhající se straně;

d) spoléhající se straně je řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu;

e) pokud byl v okamžiku podpisu použit pseudonym, je jeho použití jednoznačně sděleno spoléhající se straně;

f) nebyla ohrožena integrita podepsaných dat;

g) v okamžiku podpisu byly splněny požadavky stanovené v článku 26.

2. Systém použitý k ověření platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu musí poskytnout spoléhající se straně řádný výsledek postupu ověření platnosti a umožňovat jí zjistit jakékoli problémy týkající se bezpečnosti.

3. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely ověřování platnosti zaručených elektronických podpisů založených na kvalifikovaných certifikátech. Pokud ověřování platnosti zaručených elektronických podpisů založených na kvalifikovaných certifikátech splňuje tyto normy, specifikace a postupy, předpokládá se shoda s požadavky stanovenými v odstavci 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

33) V článku 33 se odstavec 2 nahrazuje tímto:

„2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely kvalifikované služby ověřování platnosti uvedené v odstavci 1 tohoto článku. Pokud služba ověřování platnosti kvalifikovaných elektronických podpisů splňuje tyto normy, specifikace a postupy, předpokládá se shoda s požadavky stanovenými v odstavci 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

34) Článek 34 se mění takto:

a) vkládá se nový odstavec, který zní:

„1a. Pokud postupy pro kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů splňují normy, specifikace a postupy uvedené v odstavci 2, předpokládá se shoda s požadavky stanovenými v odstavci 1.“;

b) odstavec 2 se nahrazuje tímto:

„2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely kvalifikované služby uchovávání kvalifikovaných elektronických podpisů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

35) V článku 35 se zrušuje odstavec 3.

36) Článek 36 se mění takto:

a) dosavadní jediný odstavec se označuje jako odstavec 1;

b) doplňuje se nový odstavec, který zní:

„2. Do 21. května 2026 Komise posoudí, zda je nezbytné přijmout prováděcí akty, kterými se stanoví seznam referenčních norem a kterými se v případě potřeby stanoví specifikace a postupy pro zaručené elektronické pečeti. Na základě tohoto posouzení může Komise takové prováděcí akty přijmout. Pokud zaručená elektronická pečeť splňuje tyto normy, specifikace a postupy, předpokládá se shoda s požadavky pro zaručené elektronické pečeti. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

37) V článku 37 se zrušuje odstavec 4.

38) V článku 38 se odstavec 6 nahrazuje tímto:

„6. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely kvalifikovaných certifikátů pro elektronické pečetě. Pokud kvalifikovaný certifikát pro elektronickou pečeť splňuje tyto normy, specifikace a postupy, předpokládá se shoda s požadavky stanovenými v příloze III. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

39) Vkládá se nový článek, který zní:

„Článek 39a

Požadavky na kvalifikovanou službu správy kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku

Na kvalifikovanou službu správy kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku se použije přiměřeně článek 29a.“

40) V kapitole III oddílu 5 se vkládá nový článek, který zní:

„Článek 40a

Požadavky na ověřování zaručených elektronických pečetí založených na kvalifikovaných certifikátech

Na ověřování zaručených elektronických pečetí založených na kvalifikovaných certifikátech se použije přiměřeně článek 32a.“

41) V článku 41 se zrušuje odstavec 3.

42) Článek 42 se mění takto:

a) vkládá se nový odstavec, který zní:

„1a. Pokud spojení data a času s příslušnými daty a přesnost zdroje času splňují normy, specifikace a postupy uvedené v odstavci 2, předpokládá se shoda s požadavky stanovenými v odstavci 1.“;

b) odstavec 2 se nahrazuje tímto:

„2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely spojení data a času s příslušnými daty a pro účely stanovení přesnosti zdrojů času. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

43) Článek 44 se mění takto:

a) vkládá se nový odstavec, který zní:

„1a. Pokud postup odesílání a přijímání dat splňuje normy, specifikace a postupy uvedené v odstavci 2, předpokládá se shoda s požadavky stanovenými v odstavci 1.“;

b) odstavec 2 se nahrazuje tímto:

„2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely odesílání a přijímání dat. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

c) vkládají se nové odstavce, které znějí:

„2a. Poskytovatelé kvalifikovaných služeb elektronického doporučeného doručování se mohou dohodnout na interoperabilitě mezi kvalifikovanými službami elektronického doporučeného doručování, které poskytují. Tento rámec interoperability musí splňovat požadavky stanovené v odstavci 1 a tato shoda musí být potvrzena subjektem posuzování shody.

2b. Komise může prostřednictvím prováděcích aktů stanovit seznam referenčních norem a v případě potřeby stanovit specifikace a postupy pro účely rámce interoperability uvedeného v odstavci 2a tohoto článku. Technické specifikace a obsah norem musí být nákladově efektivní a přiměřené. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

44) Článek 45 se nahrazuje tímto:

„Článek 45

Požadavky na kvalifikované certifikáty pro autentizaci internetových stránek

1. Kvalifikované certifikáty pro autentizaci internetových stránek musí splňovat požadavky stanovené v příloze IV. Hodnocení shody s těmito požadavky se provádí v souladu s normami, specifikacemi a postupy uvedenými v odstavci 2 tohoto článku.

1a. Kvalifikované certifikáty pro autentizaci internetových stránek vydané v souladu s odstavcem 1 tohoto článku jsou uznávány poskytovateli internetových prohlížečů. Poskytovatelé internetových prohlížečů zajistí, aby údaje o totožnosti potvrzené v certifikátu a další potvrzené atributy byly zobrazeny uživatelsky přívětivým způsobem. Poskytovatelé internetových prohlížečů zajistí podporu a interoperabilitu s kvalifikovanými certifikáty pro autentizaci internetových stránek uvedenými v odstavci 1 tohoto článku, s výjimkou mikropodniků nebo malých podniků, jak jsou vymezeny v článku 2 přílohy doporučení 2003/361/ES, v prvních pěti letech fungování jako poskytovatelé služeb prohlížení internetových stránek.

1b. Kvalifikované certifikáty pro autentizaci internetových stránek nepodléhají žádným jiným závazným požadavkům, než jsou požadavky stanovené v odstavci 1.

2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely kvalifikovaných certifikátů pro autentizaci internetových stránek uvedené v odstavci 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

45) Vkládá se nový článek, který zní:

„Článek 45a

Předběžná opatření týkající se kybernetické bezpečnosti

1. Poskytovatelé internetových prohlížečů nepřijmou žádná opatření, která by byla v rozporu s jejich povinnostmi stanovenými v článku 45, zejména s požadavky na uznávání kvalifikovaných certifikátů pro autentizaci internetových stránek a na zobrazování poskytnutých údajů o totožnosti uživatelsky přívětivým způsobem.

2. Odchylně od odstavce 1 a pouze v případě odůvodněných obav týkajících se narušení bezpečnosti nebo ztráty integrity identifikovaného certifikátu nebo souboru certifikátů mohou poskytovatelé internetových prohlížečů v souvislosti s tímto certifikátem nebo souborem certifikátů přijmout předběžná opatření.

3. Pokud poskytovatel internetového prohlížeče přijme předběžná opatření podle odstavce 2, oznámí své obavy spolu s popisem opatření přijatých ke zmírnění těchto obav bez zbytečného odkladu písemně Komisi, příslušnému orgánu dohledu, subjektu, kterému byl certifikát vydán, a kvalifikovanému poskytovateli služeb vytvářejících důvěru, který daný certifikát nebo soubor certifikátů vydal. Po obdržení takového oznámení vydá příslušný orgán dohledu danému poskytovateli internetového prohlížeče potvrzení o přijetí.

4. Příslušný orgán dohledu prošetří otázky uvedené v oznámení v souladu s čl. 46b odst. 4 písm. k). Pokud výsledek tohoto šetření nevede k odnětí statusu kvalifikovaného certifikátu, orgán dohledu o tom informuje poskytovatele internetového prohlížeče a požádá ho, aby ukončil předběžná opatření uvedená v odstavci 2 tohoto článku.“

46) V kapitole III se doplňují nové oddíly, které znějí:

„ODDÍL 9

ELEKTRONICKÉ POTVRZENÍ ATRIBUTŮ

Článek 45b

Právní účinky elektronického potvrzení atributů

1. Elektronickému potvrzení atributů nesmějí být upírány právní účinky ani nesmí být odmítáno jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické potvrzení atributů.

2. Kvalifikované elektronické potvrzení atributů a potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem má stejný právní účinek jako potvrzení v listinné podobě vydaná v souladu s právními předpisy.

3. Potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem v jednom členském státě se ve všech členských státech uznává jako potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem.

Článek 45c

Elektronické potvrzení atributů ve veřejných službách

Pokud se pro přístup k on-line službě poskytované subjektem veřejného sektoru vyžaduje podle vnitrostátního práva elektronická identifikace s použitím prostředku pro elektronickou identifikaci a autentizace, osobní identifikační údaje v elektronickém potvrzení atributů nenahrazují elektronickou identifikaci s použitím prostředku pro elektronickou identifikaci a autentizaci pro elektronickou identifikaci, pokud to členský stát výslovně nepovolí. V takovém případě se rovněž akceptuje kvalifikované elektronické potvrzení atributů z jiných členských států.

Článek 45d

Požadavky na kvalifikované elektronické potvrzení atributů

1. Kvalifikované elektronické potvrzení atributů musí splňovat požadavky stanovené v příloze V.

2. Hodnocení shody požadavků stanovených v příloze V se provádí v souladu s normami, specifikacemi a postupy uvedenými v odstavci 5 tohoto článku.

3. Kvalifikovaná elektronická potvrzení atributů nepodléhají žádným závazným požadavkům kromě požadavků stanovených v příloze V.

4. Pokud bylo kvalifikované elektronické potvrzení atributů po počátečním vydání zneplatněno, ztrácí okamžikem zneplatnění platnost a jeho status nelze v žádném případě změnit zpět.

5. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely kvalifikovaných elektronických potvrzení atributů. Tyto prováděcí akty jsou v souladu s prováděcími akty o zavedení evropské peněženky digitální identity, uvedenými v čl. 5a odst. 23. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 45e

Ověřování atributů podle autentických zdrojů

1. Členské státy do 24 měsíců ode dne vstupu prováděcích aktů uvedených v čl. 5a odst. 23 a čl. 5c odst. 6 v platnost zajistí, aby přinejmenším pro atributy uvedené v příloze VI, pokud tyto atributy vycházejí z autentických zdrojů v rámci veřejného sektoru, byla přijata opatření, která kvalifikovaným poskytovatelům služeb vytvářejících důvěru vydávajícím elektronická potvrzení atributů umožní na žádost uživatele v souladu s právem Unie nebo s vnitrostátním právem tyto atributy elektronickými prostředky ověřit.

2. Do 21. listopadu 2024 Komise s přihlédnutím k příslušným mezinárodním normám prostřednictvím prováděcích aktů stanoví seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro katalog atributů, jakož i schémata pro potvrzování atributů a ověřovací postupy pro kvalifikovaná elektronická potvrzení atributů pro účely odstavce 1 tohoto článku. Tyto prováděcí akty jsou v souladu s prováděcími akty o zavedení evropské peněženky digitální identity, uvedeným v čl. 5a odst. 23. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 45f

Požadavky na elektronické potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem

1. Elektronické potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem musí splňovat tyto požadavky:

a) požadavky uvedené v příloze VII;

b) kvalifikovaný certifikát, na němž jsou založeny kvalifikovaný elektronický podpis nebo kvalifikovaná elektronická pečeť subjektu veřejného sektoru uvedeného v čl. 3 bodu 46, identifikovaného jako vydavatel podle písmene b) přílohy VII, který obsahuje specifický soubor certifikovaných atributů ve formě vhodné pro automatické zpracování a:

i) uvádí, že vydávající subjekt je zřízen v souladu s právem Unie nebo vnitrostátním právem jakožto subjekt odpovědný za autentický zdroj, na jehož základě je vydáváno elektronické potvrzení atributů, nebo jako subjekt pověřený jednat jeho jménem;

ii) poskytuje soubor dat jednoznačně identifikujících autentický zdroj uvedený v bodu i) a

iii) odkazuje na právo Unie nebo vnitrostátní právo podle bodu i).

2. Členský stát, v němž jsou subjekty veřejného sektoru uvedené v čl. 3 bodu 46 usazeny, zajistí, aby subjekty veřejného sektoru vydávající elektronické potvrzení atributů měly rovnocennou úroveň spolehlivosti a důvěryhodnosti jako kvalifikovaní poskytovatelé služeb vytvářejících důvěru v souladu s článkem 24.

3. Členské státy oznámí subjekty veřejného sektoru uvedené v čl. 3 bodu 46 Komisi. Toto oznámení obsahuje zprávu o posouzení shody vydanou subjektem posuzování shody potvrzující splnění požadavků stanovených v odstavcích 1, 2 a 6 tohoto článku. Seznam subjektů veřejného sektoru uvedených v čl. 3 bodu 46 Komise bezpečnou cestou zpřístupní veřejnosti ve formě opatřené elektronickým podpisem nebo pečetí a vhodné pro automatické zpracování.

4. Pokud bylo elektronické potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem po počátečním vydání zneplatněno, ztrácí platnost okamžikem zneplatnění a jeho status nelze změnit zpět.

5. Pokud elektronické potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem splňuje normy, specifikace a postupy uvedené v odstavci 6, předpokládá se shoda s požadavky stanovenými v odstavci 1.

6. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely elektronického potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem. Tyto prováděcí akty jsou v souladu s prováděcím aktem o zavedení evropské peněženky digitální identity, uvedeným v čl. 5a odst. 23. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

7. Do 21. listopadu 2024 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely odstavce 3 tohoto článku. Tyto prováděcí akty jsou v souladu s prováděcím aktem o zavedení evropské peněženky digitální identity, uvedeným v čl. 5a odst. 23. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

8. Subjekty veřejného sektoru uvedené v čl. 3 bodu 46, vydávající elektronické potvrzení atributů poskytují rozhraní s evropskými peněženkami digitální identity v souladu s článkem 5a.

Článek 45g

Vydávání elektronických potvrzení atributů pro evropské peněženky digitální identity

1. Poskytovatelé elektronických potvrzení atributů poskytnou uživatelům evropské peněženky digitální identity možnost požadovat, získat, uchovávat a spravovat elektronické potvrzení atributů bez ohledu na členský stát, který evropskou peněženku digitální identity poskytuje.

2. Poskytovatelé kvalifikovaných elektronických potvrzení atributů poskytují rozhraní s evropskými peněženkami digitální identity poskytovanými v souladu s článkem 5a.

Článek 45h

Dodatečná pravidla poskytování služeb elektronického potvrzování atributů

1. Poskytovatelé kvalifikovaných a nekvalifikovaných služeb elektronického potvrzování atributů nesmějí kombinovat osobní údaje týkající se poskytování těchto služeb s osobními údaji z jiných služeb, které nabízejí oni nebo jejich obchodní partneři.

2. Osobní údaje týkající se poskytování služeb elektronického potvrzování atributů jsou uchovávány logicky odděleně od jiných dat uchovávaných poskytovatelem elektronického potvrzování atributů.

3. Poskytovatelé kvalifikovaných služeb elektronického potvrzování atributů zavedou poskytování těchto kvalifikovaných služeb vytvářejících důvěru způsobem, který je funkčně oddělen od jiných jimi poskytovaných služeb.

ODDÍL 10

SLUŽBY ELEKTRONICKÉ ARCHIVACE

Článek 45i

Právní účinek služby elektronické archivace

1. Elektronickým datům a elektronickým dokumentům uchovávaným s použitím služby elektronické archivace nesmějí být upírány právní účinky ani nesmějí být odmítány jako důkaz v soudním nebo správním řízení pouze z toho důvodu, že mají elektronickou podobu nebo že nejsou uchovávány s použitím kvalifikované služby elektronické archivace.

2. U elektronických dat a elektronických dokumentů uchovávaných s použitím kvalifikované služby elektronické archivace platí předpoklad integrity dat a jejich původu, a to po dobu uchovávání kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Článek 45j

Požadavky na kvalifikované služby elektronické archivace

1. Kvalifikované služby elektronické archivace musí splňovat tyto požadavky:

a) jsou poskytovány kvalifikovanými poskytovateli služeb vytvářejících důvěru;

b) používají postupy a technologie umožňující zajistit trvanlivost a čitelnost elektronických dat a elektronických dokumentů i po uplynutí doby technologické použitelnosti – a alespoň po zákonně či smluvně stanovenou dobu uchovávání a současně zachovat jejich integritu a přesnost původu;

c) zajišťují, aby byla elektronická data a elektronické dokumenty uchovávány způsobem, který je chrání před ztrátou a pozměněním, s výjimkou změn jejich nosiče nebo elektronického formátu;

d) oprávněným spoléhajícím se stranám umožňují obdržet automatizovaným způsobem zprávu, která potvrzuje, že u elektronických dat a elektronických dokumentů získaných z kvalifikovaného elektronického archivu platí předpoklad integrity dat od začátku doby uchovávání do doby jejich zpřístupnění.

Zpráva uvedená v prvním pododstavci písm. d) se poskytne spolehlivým a účinným způsobem a musí být opatřena kvalifikovaným elektronickým podpisem nebo kvalifikovanou elektronickou pečetí poskytovatele kvalifikované služby elektronické archivace.

2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely kvalifikovaných služeb elektronické archivace. Pokud kvalifikovaná služba elektronické archivace splňuje tyto normy, specifikace a postupy, předpokládá se shoda s požadavky pro kvalifikované služby elektronické archivace. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

ODDÍL 11

ELEKTRONICKÉ KNIHY ZÁZNAMŮ

Článek 45k

Právní účinky elektronických knih záznamů

1. Elektronické knize záznamů nesmějí být upírány právní účinky ani nesmí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické knihy záznamů.

2. U datových záznamů obsažených v kvalifikované elektronické knize záznamů platí předpoklad jejich jedinečného a přesného sekvenčního chronologického řazení a jejich integrity.

Článek 45l

Požadavky na kvalifikované elektronické knihy záznamů

1. Kvalifikované elektronické knihy záznamů musí splňovat tyto požadavky:

a) jsou vytvářeny a spravovány jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru;

b) identifikují původ datových záznamů v knize záznamů;

c) zajišťují jedinečné sekvenční chronologické řazení datových záznamů v knize záznamů;

d) zaznamenávají data takovým způsobem, že je možné okamžitě zjistit jakoukoliv následnou změnu dat, čímž zajišťují jejich integritu v čase.

2. Pokud elektronická kniha záznamů splňuje normy, specifikace a postupy uvedené v odstavci 3, předpokládá se shoda s požadavky stanovenými v odstavci 1.

3. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro požadavky stanovené v odstavci 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

47) Vkládá se nová kapitola, která zní:

„KAPITOLA IVa

SPRÁVNÍ RÁMEC

Článek 46a

Dohled nad rámcem pro evropskou peněženku digitální identity

1. Členské státy určí jeden nebo více orgánů dohledu usazených na jejich území.

Orgánům dohledu určeným podle prvního pododstavce jsou uděleny nezbytné pravomoci a přiměřené zdroje, které jim umožňují účinně, účelně a nezávisle plnit jejich úkoly.

2. Členské státy oznámí Komisi názvy a adresy svých orgánů dohledu určených podle odstavce 1 a veškeré jejich následné změny. Komise seznam oznámených orgánů dohledu zveřejní.

3. Úlohou orgánů dohledu určených podle odstavce 1 je:

a) vykonávat dohled nad poskytovateli evropských peněženek digitální identity usazenými v členském státě, který provedl určení, a prostřednictvím činností předběžného a následného dohledu zajistit, aby tito poskytovatelé a jimi poskytované evropské peněženky digitální identity splňovali požadavky stanovené v tomto nařízení;

b) přijmout v případě potřeby prostřednictvím činností následného dohledu opatření ve vztahu k poskytovatelům evropských peněženek digitální identity usazeným na území členského státu, který provedl určení, pokud jsou informovány o tom, že tito poskytovatelé nebo jimi poskytované evropské peněženky digitální identity porušují toto nařízení.

4. Mezi úkoly orgánů dohledu určených podle odstavce 1 patří zejména:

a) spolupracovat s dalšími orgány dohledu a poskytovat jim pomoc v souladu s články 46c a 46e;

b) požadovat informace nezbytné k monitorování souladu s tímto nařízením;

c) informovat relevantní příslušné orgány dotčených členských států určené nebo zřízené podle čl. 8 odst. 1 směrnice (EU) 2022/2555 o jakémkoli závažném narušení bezpečnosti nebo ztrátě integrity, o nichž se dozví při plnění svých úkolů, a v případě závažného narušení bezpečnosti nebo ztráty integrity, které se týkají dalších členských států, informovat jednotné kontaktní místo dotčeného členského státu určené nebo zřízené podle čl. 8 odst. 3 směrnice (EU) 2022/2555 a jednotná kontaktní místa v ostatních dotčených členských státech určená podle čl. 46c odst. 1 tohoto nařízení a informovat veřejnost nebo požadovat, aby tak učinili poskytovatelé evropské peněženky digitální identity, pokud orgán dohledu rozhodne, že zveřejnění tohoto narušení bezpečnosti nebo ztráty integrity je ve veřejném zájmu;

d) provádět kontroly na místě a vzdálený dohled;

e) požadovat, aby poskytovatelé evropských peněženek digitální identity napravili případné neplnění požadavků stanovených v tomto nařízení;

f) v případě nezákonného nebo podvodného používání evropské peněženky digitální identity pozastavit nebo zrušit registraci spoléhajících se stran a začlenění spoléhajících se stran do mechanismu uvedeného v čl. 5b odst. 7;

g) spolupracovat s příslušnými dozorovými úřady zřízenými podle článku 51 nařízení (EU) 2016/679, zejména tak, že je bez zbytečného odkladu informují o tom, že zřejmě došlo k porušení pravidel týkajících se ochrany osobních údajů, jakož i o narušeních bezpečnosti, která podle všeho představují porušení zabezpečení osobních údajů.

5. Pokud orgán dohledu určený podle odstavce 1 požaduje, aby poskytovatel evropské peněženky digitální identity napravil neplnění požadavků stanovených v tomto nařízení podle odst. 4 písm. e), a tento poskytovatel odpovídajícím způsobem nejedná a případně nejedná ve lhůtě stanovené orgánem dohledu, orgán dohledu určený podle odstavce 1 může poskytovateli nařídit, aby pozastavil nebo ukončil poskytování evropské peněženky digitální identity, a to zejména s ohledem na rozsah, dobu trvání a důsledky tohoto neplnění. Orgán dohledu o rozhodnutí požadovat pozastavení nebo ukončení poskytování evropské peněženky digitální identity bez zbytečného odkladu informuje orgány dohledu ostatních členských států, Komisi, spoléhající se strany a uživatele evropské peněženky digitální identity.

6. Do 31. března každého roku každý orgán dohledu určený podle odstavce 1 předloží Komisi zprávu o svých hlavních činnostech v předchozím kalendářním roce. Komise poskytne tyto výroční zprávy Evropskému parlamentu a Radě.

7. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů formáty a postupy pro účely zprávy uvedené v odstavci 6 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 46b

Dohled nad službami vytvářejícími důvěru

1. Členské státy určí orgán dohledu na svém území nebo, po vzájemné dohodě s jiným členským státem, určí orgán dohledu v tomto jiném členském státě. Tento orgán dohledu odpovídá za plnění úkolů v oblasti dohledu nad službami vytvářejícími důvěru v členském státě, který provedl určení.

Orgánům dohledu určeným podle prvního pododstavce jsou k plnění těchto úkolů uděleny nezbytné pravomoci a přiměřené zdroje.

2. Členské státy oznámí Komisi názvy a adresy svých orgánů dohledu určených podle odstavce 1 a veškeré jejich následné změny. Komise seznam oznámených orgánů dohledu zveřejní.

3. Úlohou orgánů dohledu určených podle odstavce 1 je:

a) vykonávat dohled nad kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými na území členského státu, který provedl určení, a prostřednictvím činností předběžného a následného dohledu zajistit, aby tito kvalifikovaní poskytovatelé služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru splňovali požadavky stanovené v tomto nařízení;

b) přijmout v případě potřeby prostřednictvím činností následného dohledu opatření ve vztahu nekvalifikovaným poskytovatelům služeb vytvářejících důvěru usazeným na území členského státu, který provedl určení, pokud jsou informovány o tom, že tito nekvalifikovaní poskytovatelé služeb vytvářejících důvěru nebo jimi poskytované služby vytvářející důvěru údajně nesplňují požadavky stanovené v tomto nařízení.

4. Mezi úkoly orgánů dohledu určených podle odstavce 1 patří zejména:

a) informovat relevantní příslušné orgány dotčených členských států určené nebo zřízené podle čl. 8 odst. 1 směrnice (EU) 2022/2555 o jakémkoli závažném narušení bezpečnosti nebo ztrátě integrity, o nichž se dozví při plnění svých úkolů, a v případě závažného narušení bezpečnosti nebo ztráty integrity, které se týká dalších členských států, informovat jednotné kontaktní místo dotčeného členského státu určené nebo zřízené podle čl. 8 odst. 3 směrnice (EU) 2022/2555 a jednotná kontaktní místa v ostatních dotčených členských státech určená podle čl. 46c odst. 1 tohoto nařízení a informovat veřejnost nebo požadovat, aby tak učinili poskytovatelé služeb vytvářejících důvěru, pokud orgán dohledu rozhodne, že zveřejnění tohoto narušení bezpečnosti nebo ztráty integrity je ve veřejném zájmu;

b) spolupracovat s dalšími orgány dohledu a poskytovat jim pomoc v souladu s články 46c a 46e;

c) provádět analýzu zpráv o posouzení shody uvedených v čl. 20 odst. 1 a čl. 21 odst. 1;

d) podávat Komisi zprávy o svých hlavních činnostech v souladu s odstavcem 6 tohoto článku;

e) provádět audity kvalifikovaných poskytovatelů služeb vytvářejících důvěru nebo požadovat, aby subjekt posuzování shody provedl posouzení shody těchto poskytovatelů v souladu s čl. 20 odst. 2;

f) spolupracovat s příslušnými dozorovými úřady zřízenými podle článku 51 nařízení (EU) 2016/679, zejména tak, že je bez zbytečného odkladu informuje o tom, že zřejmě došlo k porušení pravidel týkajících se ochrany osobních údajů, jakož i o narušeních bezpečnosti, která podle všeho představují porušení zabezpečení osobních údajů;

g) v souladu s články 20 a 21 udělovat poskytovatelům služeb vytvářejících důvěru a jimi poskytovaným službám status kvalifikovaného poskytovatele nebo kvalifikované služby a odnímat tento status;

h) informovat subjekt odpovědný za vnitrostátní důvěryhodný seznam podle čl. 22 odst. 3 o svých rozhodnutích udělit nebo odejmout status kvalifikovaného poskytovatele nebo kvalifikované služby, pokud tento subjekt není rovněž orgánem dohledu určeným podle odstavce 1 tohoto článku;

i) ověřovat existenci a správné uplatňování ustanovení o plánech ukončení činnosti v případech, kdy kvalifikovaný poskytovatel služeb vytvářejících důvěru ukončí svou činnost, včetně způsobu zpřístupňování informací v souladu s čl. 24 odst. 2 písm. h);

j) požadovat, aby poskytovatelé služeb vytvářejících důvěru napravili případné neplnění požadavků stanovených v tomto nařízení;

k) prošetřovat tvrzení poskytovatelů internetových prohlížečů podle článku 45a a v případě potřeby přijmout opatření.

5. Členské státy mohou vyžadovat, aby orgán dohledu určený podle odstavce 1 zavedl, udržoval a aktualizoval důvěryhodnou infrastrukturu v souladu s vnitrostátním právem.

6. Do 31. března každého roku každý orgán dohledu určený podle odstavce 1 předloží Komisi zprávu o svých hlavních činnostech v předchozím kalendářním roce. Komise poskytne tyto výroční zprávy Evropskému parlamentu a Radě.

7. Do 21. května 2025 přijme Komise pokyny k provádění úkolů uvedených v odstavci 4 tohoto článku orgány dohledu určenými podle odstavce 1 tohoto článku a prostřednictvím prováděcích aktů stanoví formáty a postupy pro účely zprávy uvedené v odstavci 6 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 46c

Jednotná kontaktní místa

1. Každý členský stát určí jednotné kontaktní místo pro služby vytvářející důvěru, evropské peněženky digitální identity a oznámené systémy elektronické identifikace.

2. Každé jednotné kontaktní místo plní styčnou funkci, jejímž cílem je usnadnit přeshraniční spolupráci mezi orgány dohledu nad poskytovateli služeb vytvářejících důvěru a mezi orgány dohledu nad poskytovateli evropských peněženek digitální identity a případně s Komisí, Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) a dalšími příslušnými orgány v rámci svého členského státu.

3. Každý členský stát zveřejní a bez zbytečného odkladu oznámí Komisi název a adresu jednotného kontaktního místa určeného podle odstavce 1 a veškeré jejich následné změny.

4. Komise zveřejní seznam jednotných kontaktních míst oznámených podle odstavce 3.

Článek 46d

Vzájemná pomoc

1. S cílem usnadnit dohled nad plněním povinností podle tohoto nařízení a jejich vymáhání mohou orgány dohledu určené podle čl. 46a odst. 1 a čl. 46b odst. 1 požádat, a to i prostřednictvím skupiny pro spolupráci zřízené podle čl. 46e odst. 1, o vzájemnou pomoc orgány dohledu jiného členského státu, v němž je usazen poskytovatel evropské peněženky digitální identity nebo poskytovatel služeb vytvářejících důvěru nebo v němž se nachází jeho síť a informační systémy nebo v němž jsou poskytovány jeho služby.

2. Vzájemná pomoc obnáší alespoň to, že:

a) orgán dohledu, který uplatňuje opatření v oblasti dohledu a vymáhání v jednom členském státě, informuje orgán dohledu z druhého dotčeného členského státu a konzultuje s ním;

b) orgán dohledu může požádat orgán dohledu jiného dotčeného členského státu, aby přijal opatření v oblasti dohledu nebo vymáhání, zahrnující například žádosti o provedení kontrol v souvislosti se zprávami o posouzení shody podle článků 20 a 21, pokud jde o poskytování služeb vytvářejících důvěru;

c) orgány dohledu mohou případně provádět společná šetření s orgány dohledu jiných členských států.

Ujednání a postupy pro společné činnosti podle prvního pododstavce dohodnou a zavedou dotčené členské státy v souladu se svým vnitrostátním právem.

3. Orgán dohledu, jemuž byla podána žádost o pomoc, může tuto žádost odmítnout z kteréhokoliv z těchto důvodů:

a) požadovaná pomoc je nepřiměřená činnostem v oblasti dohledu, které daný orgán dohledu vykonává v souladu s články 46a a 46b;

b) orgán dohledu není k poskytnutí požadované pomoci příslušný;

c) poskytnutí požadované pomoci by nebylo slučitelné s tímto nařízením.

4. Do 21. května 2025 a poté každé dva roky vydá skupina pro spolupráci zřízená podle čl. 46e odst. 1 pokyny týkající se organizačních aspektů a postupů vzájemné pomoci uvedené v odstavcích 1 a 2 tohoto článku.

Článek 46e

Skupina pro evropskou spolupráci v oblasti digitální identity

1. S cílem podpořit a usnadnit přeshraniční spolupráci členských států a výměnu informací v souvislosti se službami vytvářejícími důvěru, evropskými peněženkami digitální identity a oznámenými systémy elektronické identifikace zřídí Komise skupinu pro evropskou spolupráci v oblasti digitální identity (dále jen ‚skupina pro spolupráci').

2. Skupinu pro spolupráci tvoří zástupci jmenovaní členskými státy a zástupci Komise. Skupině pro spolupráci předsedá Komise. Komise zajišťuje sekretariát skupiny pro spolupráci.

3. K účasti na zasedáních skupiny pro spolupráci a k účasti na její činnosti mohou být ad hoc jako pozorovatelé přizváni zástupci příslušných zúčastněných stran.

4. K účasti na činnosti skupiny pro spolupráci je jako pozorovatel přizvána agentura ENISA, pokud ve skupině probíhá výměna názorů, osvědčených postupů a informací týkajících se relevantních aspektů kybernetické bezpečnosti, jako je oznamování narušení bezpečnosti, a pokud se projednává používání certifikátů nebo norem kybernetické bezpečnosti.

5. Skupina pro spolupráci má tyto úkoly:

a) vyměňovat si názory a spolupracovat s Komisí na nových politických iniciativách v oblasti peněženek digitální identity, prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru;

b) ve vhodných případech poskytovat Komisi poradenství při včasné přípravě návrhů prováděcích aktů a aktů v přenesené pravomoci, které mají být přijaty podle tohoto nařízení;

c) za účelem podpory orgánů dohledu při provádění ustanovení tohoto nařízení vykonávat tyto činnosti:

   i) vyměňovat si osvědčené postupy a informace týkající se uplatňování ustanovení tohoto nařízení;

   ii) posuzovat relevantní vývoj v oblasti peněženek digitální identity, elektronické identifikace a služeb vytvářejících důvěru;

   iii) pořádat společná setkání s příslušnými zainteresovanými stranami z celé Unie za účelem projednávání činností vykonávaných skupinou pro spolupráci a shromažďování poznatků o nových výzvách v oblasti této politiky;

   iv) s podporou agentury ENISA si vyměňovat názory, osvědčené postupy a informace v souvislosti s příslušnými aspekty kybernetické bezpečnosti týkajícími se evropských peněženek digitální identity, systémů elektronické identifikace a služeb vytvářejících důvěru;

   v) vyměňovat si osvědčené postupy v souvislosti s vývojem a prováděním politik týkajících se oznamování narušení bezpečnosti a společných opatření podle článků 5e a 10;

   vi) pořádat společná setkání se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací zřízenou podle čl. 14 odst. 1 směrnice (EU) 2022/2555 s cílem vyměňovat si v souvislosti se službami vytvářejícími důvěru a s elektronickou identifikací relevantní informace týkající se kybernetických hrozeb, incidentů, zranitelností, iniciativ zaměřených na zvyšování povědomí, školení, cvičení a dovedností, budování kapacit, kapacity v oblasti norem a technických specifikací, jakož i norem a technických specifikací;

   vii) na žádost orgánu dohledu projednávat konkrétní žádosti o vzájemnou pomoc podle článku 46d;

   viii) usnadňovat výměnu informací mezi orgány dohledu poskytováním pokynů týkajících se organizačních aspektů a postupů vzájemné pomoci podle článku 46d;

d) organizovat vzájemná hodnocení systémů elektronické identifikace, které mají být oznámeny podle tohoto nařízení.

6. Členské státy zajistí, aby jimi jmenovaní zástupci ve skupině pro spolupráci účinně a účelně spolupracovali.

7. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů nezbytná procesní opatření pro usnadnění spolupráce mezi členskými státy uvedené v odst. 5 písm. d) tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

48) Článek 47 se mění takto:

a) odstavce 2 a 3 se nahrazují tímto:

„2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 5c odst. 7, čl. 24 odst. 4b a v čl. 30 odst. 4 je svěřena Komisi na dobu neurčitou ode dne 17. září 2014.

3. Evropský parlament nebo Rada mohou přenesení pravomocí uvedené v článku 5c odst. 7, čl. 24 odst. 4b a čl. 30 odst. 4 kdykoliv zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění rozhodnutí v *Úředním věstníku Evropské unie* nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.“;

b) odstavec 5 se nahrazuje tímto:

„5. Akt v přenesené pravomoci přijatý podle 5c odst. 7, čl. 24 odst. 4b a čl. 30 odst. 4 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament ani Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.“;

49) V kapitole VI se vkládá nový článek, který zní:

„Článek 48a

Požadavky na podávání zpráv

1. Členské státy zajistí shromažďování statistických údajů týkajících se fungování evropských peněženek digitální identity a kvalifikovaných služeb vytvářejících důvěru poskytovaných na jejich území.

2. Statistické údaje shromážděné v souladu s odstavcem 1 zahrnují:

a) počet fyzických a právnických osob s platnou evropskou peněženkou digitální identity;

b) druh a počet služeb, které akceptují používání evropské peněženky digitální identity;

c) počet stížností uživatelů a počet incidentů týkajících se ochrany spotřebitelů a ochrany údajů ve vztahu ke spoléhajícím se stranám a kvalifikovaným službám vytvářejícím důvěru;

d) souhrnnou zprávu včetně údajů o incidentech, jež zabránily použití evropské peněženky digitální identity;

e) souhrn významných bezpečnostních incidentů, případů porušení zabezpečení údajů a dotčených uživatelů evropské peněženky digitální identity nebo kvalifikovaných služeb vytvářejících důvěru.

3. Statistické údaje uvedené v odstavci 2 se zpřístupní veřejnosti v otevřeném a běžně používaném strojově čitelném formátu.

4. Do 31. března každého roku předloží členské státy Komisi zprávu o statistických údajích shromážděných v souladu s odstavcem 2.“

50) Článek 49 se nahrazuje tímto:

„Článek 49

Přezkum

1. Do 21. května 2026 přezkoumá Komise uplatňování tohoto nařízení a podá zprávu Evropskému parlamentu a Radě. Komise v uvedené zprávě zejména vyhodnotí, zda je s přihlédnutím ke zkušenostem s uplatňováním tohoto nařízení a k technologickému, tržnímu a právnímu vývoji vhodné upravit oblast působnosti tohoto nařízení nebo jeho konkrétní ustanovení, včetně zejména ustanovení čl. 5c odst. 5. V případě potřeby se ke zprávě připojí návrh na změnu tohoto nařízení.

2. Zpráva uvedená v odstavci 1 zahrnuje posouzení dostupnosti, bezpečnosti a použitelnosti oznámených prostředků pro elektronickou identifikaci a evropských peněženek digitální identity, které spadají do oblasti působnosti tohoto nařízení, a posuzuje, zda by všichni soukromí poskytovatelé on-line služeb využívající pro autentizaci uživatelů služby elektronické identifikace třetích stran měli být povinni akceptovat používání oznámených prostředků pro elektronickou identifikaci a evropských peněženek digitální identity.

3. Do 21. května 2030 a poté každé čtyři roky předloží Komise Evropskému parlamentu a Radě zprávu o pokroku v dosahování cílů tohoto nařízení.“;

51) Článek 51 se nahrazuje tímto:

„Článek 51

Přechodná ustanovení

1. Prostředky pro bezpečné vytváření podpisu, jejichž shoda byla stanovena podle čl. 3 odst. 4 směrnice 1999/93/ES, se považují za kvalifikované prostředky pro vytváření elektronických podpisů podle tohoto nařízení do 21. května 2027.

2. Kvalifikovaná osvědčení vydaná fyzickým osobám podle směrnice 1999/93/ES se považují za kvalifikované certifikáty pro elektronické podpisy podle tohoto nařízení do 21. května 2026.

3. Správa kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí na dálku jinými kvalifikovanými poskytovateli služeb vytvářejících důvěru, než jsou kvalifikovaní poskytovatelé služeb vytvářejících důvěru poskytující kvalifikované služby vytvářející důvěru pro účely správy kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí na dálku v souladu s články 29a a 39a může být do 21. května 2026 vykonávána i bez získání statusu kvalifikované služby pro poskytování těchto služeb souvisejících se správou.

4. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru, kteří kvalifikovaný status podle tohoto nařízení získali před 20. květnem 2024, předloží orgánu dohledu co nejdříve a v každém případě do 21. května 2026 zprávu o posouzení shody dokládající soulad s čl. 24 odst. 1, 1a a 1b.“

52) Přílohy I až IV se mění v souladu s přílohami I až IV tohoto nařízení.

53) Doplňují se nové přílohy V, VI a VII obsažené v přílohách V, VI a VII tohoto nařízení.

Článek 2

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 11. dubna 2024.

Za Evropský parlament	*Za Radu*
předsedkyně	*předsedkyně*
R. METSOLA	H. LAHBIB

PŘÍLOHA I

V příloze I nařízení (EU) č. 910/2014 se písmeno i) nahrazuje tímto:

„i) informace o platnosti kvalifikovaného certifikátu nebo údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;“

PŘÍLOHA II

V příloze II nařízení (EU) č. 910/2014 se zrušují body 3 a 4.

PŘÍLOHA III

V příloze III nařízení (EU) č. 910/2014 se písmeno i) nahrazuje tímto:

„i) informace o platnosti kvalifikovaného certifikátu nebo údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;“

PŘÍLOHA IV

Příloha IV nařízení (EU) č. 910/2014 se mění takto:

1) písmeno c) se nahrazuje tímto:

„c) v případě fyzických osob: alespoň jméno osoby, jíž byl certifikát vydán, nebo pseudonym; je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;

ca) v případě právnických osob: jedinečný soubor dat jednoznačně identifikujících právnickou osobu, jíž je certifikát vydán, včetně alespoň názvu právnické osoby, jíž je certifikát vydán, a případně registračního čísla uvedeného v úředních záznamech;“;

2) písmeno j) se nahrazuje tímto:

„j) informace o platnosti kvalifikovaného certifikátu nebo údaj o umístění služeb pro ověření platnosti certifikátu, které lze využít k zjištění platnosti kvalifikovaného certifikátu.“

PŘÍLOHA V

„PŘÍLOHA V

POŽADAVKY NA KVALIFIKOVANÉ ELEKTRONICKÉ POTVRZENÍ ATRIBUTŮ

Kvalifikované elektronické potvrzení atributů obsahuje:

a) informaci, alespoň ve formě vhodné pro automatické zpracování, že se potvrzení vydává jako kvalifikované elektronické potvrzení atributů;

b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikovaná elektronická potvrzení atributů, včetně alespoň členského státu, v němž je poskytovatel usazen, a:

   i) v případě právnické osoby: název a případně registrační číslo uvedené v úředních záznamech,

   ii) v případě fyzické osoby: jméno a příjmení osoby;

c) soubor dat jednoznačně identifikujících subjekt, kterého se potvrzené atributy týkají; je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;

d) potvrzený atribut nebo potvrzené atributy a případné informace nezbytné k určení rozsahu těchto atributů;

e) označení začátku a konce doby platnosti potvrzení;

f) identifikační číslo potvrzení, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru, a případně označení schématu potvrzování, jehož je potvrzení atributů součástí;

g) kvalifikovaný elektronický podpis nebo kvalifikovanou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který potvrzení vydává;

h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen kvalifikovaný elektronický podpis nebo kvalifikovaná elektronická pečeť podle písmene g);

i) informace o platnosti kvalifikovaného potvrzení nebo údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného potvrzení.“

PŘÍLOHA VI

„PŘÍLOHA VI

MINIMÁLNÍ SEZNAM ATRIBUTŮ

Podle článku 45e členské státy zajistí, aby byla přijata opatření, která kvalifikovaným poskytovatelům služeb vytvářejících důvěru vydávajícím elektronická potvrzení atributů umožní na žádost uživatele ověřit elektronickými prostředky oproti příslušnému autentickému zdroji na vnitrostátní úrovni nebo prostřednictvím určených zprostředkovatelů uznaných na vnitrostátní úrovni v souladu s právem Unie nebo vnitrostátním právem, pokud se tyto atributy opírají o autentické zdroje v rámci veřejného sektoru, pravost následujících atributů:

1. adresa;
2. věk;
3. pohlaví;
4. rodinný stav;
5. složení rodiny;
6. státní příslušnost nebo občanství;
7. dosažené vzdělání, tituly a osvědčení;
8. odborná kvalifikace, tituly a osvědčení;
9. plné moci a pověření k zastupování fyzických nebo právnických osob;
10. veřejná povolení a osvědčení;
11. v případě právnických osob: finanční údaje a údaje o společnosti.“

PŘÍLOHA VII

„PŘÍLOHA VII

POŽADAVKY NA ELEKTRONICKÉ POTVRZENÍ ATRIBUTŮ VYDANÉ VEŘEJNÝM SUBJEKTEM ODPOVĚDNÝM ZA AUTENTICKÝ ZDROJ NEBO JEHO JMÉNEM

Elektronické potvrzení atributů vydané veřejným subjektem odpovědným za autentický zdroj nebo jeho jménem musí obsahovat:

a) informaci, přinejmenším ve formě vhodné pro automatické zpracování, že potvrzení bylo vydáno jako elektronické potvrzení atributů vydané veřejným subjektem odpovědným za autentický zdroj nebo jeho jménem;

b) soubor dat jednoznačně identifikujících veřejný subjekt vydávající elektronické potvrzení atributů, včetně alespoň členského státu, v němž je tento veřejný subjekt usazen, a názvu veřejného subjektu a případně registračního čísla uvedeného v úředních záznamech;

c) soubor dat jednoznačně identifikujících subjekt, kterého se potvrzené atributy týkají; je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;

d) potvrzený atribut nebo potvrzené atributy a případné informace nezbytné k určení rozsahu těchto atributů;

e) označení začátku a konce doby platnosti potvrzení;

f) identifikační číslo potvrzení, které musí být jedinečné pro daný veřejný subjekt, který potvrzení vydává, a případně označení schématu potvrzování, jehož je potvrzení atributů součástí;

g) kvalifikovaný elektronický podpis nebo kvalifikovanou elektronickou pečeť subjektu, který potvrzení vydává;

h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen kvalifikovaný elektronický podpis nebo kvalifikovaná elektronická pečeť podle písmene g);

i) informace o platnosti potvrzení nebo údaj o umístění služeb, které lze využít ke zjištění platnosti potvrzení.“