Rada
Evropské unie

Brusel 25. listopadu 2022
(OR. en)

14959/22

Interinstitucionální spis:
2021/0136(COD)

LIMITE

TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774

POZNÁMKA

Odesílatel:	Výbor stálých zástupců (část I)
Příjemce:	Rada
Č. předchozího dokumentu:	14344/22
Č. dok. Komise:	9471/21
Předmět:	Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu – obecný přístup

I. ÚVOD

1. Dne 3. června 2021 Komise přijala návrh nařízení o evropské digitální identitě (**evropská elektronická identifikace**)[1]. Tato iniciativa mění nařízení eIDAS z roku 2014[2], které položilo nezbytné základy pro bezpečný přístup ke službám a provádění transakcí on-line a přeshraničně v rámci EU.

[1] Dokument 9471/21.
[2] Nařízení (EU) č. 910/2014.

2. Tento návrh je založen na článku 114 SFEU a vyžaduje, aby členské státy v rámci oznámeného systému elektronické identifikace vydávaly evropskou peněženku digitální identity, která bude vycházet ze společných technických norem a bude založena na povinné certifikaci. S cílem vytvořit nezbytnou technickou architekturu, urychlit provádění revidovaného nařízení, poskytnout členským státům pokyny a zabránit roztříštěnosti byl návrh doplněn doporučením pro vytvoření souboru nástrojů Unie.

3. Návrh nařízení má za cíl zajistit všeobecný přístup občanů a podniků k bezpečné a důvěryhodné elektronické identifikaci a autentizaci prostřednictvím osobní digitální peněženky v mobilním telefonu.

II. ČINNOST V RÁMCI JINÝCH ORGÁNŮ A INSTITUCÍ

1. V Evropském parlamentu byl návrh svěřen Výboru pro průmysl, výzkum a energetiku (ITRE), přičemž tři další přidružené výbory, konkrétně Výbor pro vnitřní trh a ochranu spotřebitelů (IMCO), Výbor pro právní záležitosti (JURI) a Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE), by měly k tomuto návrhu zaujmout stanovisko. Zpravodajkou pro tento spis je Romana Jerkovićová (S&D, Chorvatsko). Výbor ITRE svou zprávu dosud nepřijal.

2. Dne 15. července 2021 byl Evropský hospodářský a sociální výbor požádán o stanovisko k návrhu, které bylo následně vydáno dne 20. října 2021. Evropský výbor regionů vydal spontánně stanovisko k návrhu dne 12. října 2021.

3. Evropský inspektor ochrany údajů vydal formální připomínky k návrhu dne 28. července 2021.

III. AKTUÁLNÍ STAV JEDNÁNÍ V RÁMCI RADY

1. V Radě návrh posuzovala Pracovní skupina pro telekomunikace a informační společnost (dále jen „pracovní skupina TELECOM“), jež o návrhu začala jednat v červnu 2021 v rámci portugalského předsednictví. S analýzou návrhu pracovní skupina TELECOM pokračovala za slovinského předsednictví, přičemž první čtení bylo úspěšně dokončeno dne 15. listopadu 2021.

2. Francouzské předsednictví předložilo svůj **první kompromisní návrh** ve dnech 15. února a 5. dubna 2022 a **druhý** byl projednán ve dnech 23. května a 9. června 2022. V souvislosti s politickou rozpravou, která v rámci pracovní skupiny TELECOM proběhla dne 19. července 2022, pak české předsednictví – na základě práce vykonané francouzským předsednictvím – poukázalo na hlavní nevyřešené otázky na vysoké úrovni a požádalo delegace, aby uvedly jimi upřednostňované možnosti, s cílem příslušné části druhého kompromisního návrhu odpovídajícím způsobem přepracovat. Výsledkem revidovaného znění byl **třetí kompromisní návrh**, který české předsednictví předložilo na zasedání pracovní skupiny TELECOM ve dnech 5. a 8. září 2022. Na základě dalších verzí a souvisejících úprav bylo u většiny nevyřešených otázek dosaženo hlubší úrovně konvergence.

3. **Čtvrtý kompromisní návrh**, který byl delegacím předložen na zasedání pracovní skupiny TELECOM dne 28. září 2022, však odhalil přetrvávající rozdíly mezi členskými státy, zejména pokud jde o jednu otázku na vysoké úrovni, konkrétně o úroveň záruky, jež byla pro evropskou peněženku digitální identity zvolena. Některé členské státy, které již vnitrostátní systém elektronické identifikace zavedly, původně schválily „značnou“ úroveň záruky a následně do ní investovaly, zatímco ve stávajícím návrhu elektronické identifikace se vyžaduje „vysoká“ úroveň záruky. Vzhledem k tomu, že české předsednictví si je vědomo skutečnosti, že v některých členských státech byl vydán vysoký počet prostředků pro elektronickou identifikaci se „značnou“ úrovní záruky, navrhlo dále mechanismus, který usnadní zapojení uživatelů (tzv. onboarding), čímž přispěje k využívání evropských peněženek digitální identity. Toto ustanovení uživatelům umožňuje zřídit si evropskou peněženku digitální identity za použití stávajících vnitrostátních prostředků pro elektronickou identifikaci se „značnou“ úrovní záruky a zároveň zavést dodatečné postupy distančního onboardingu, které společně splňují požadavky

„vysoké“ úrovně záruky. Technické a provozní specifikace podléhají prováděcím právním předpisům, přičemž musí být ověřena shoda s příslušnými požadavky.

4. **Pátý kompromisní návrh** byl projednán na zasedání pracovní skupiny TELECOM dne 25. října 2022. Během zasedání pracovní skupiny TELECOM dne 8. listopadu 2022 představilo české předsednictví drobné změny a v návaznosti na dodatečné připomínky a formulační návrhy delegací připravilo **konečné znění kompromisního návrhu** za účelem jeho předložení Coreperu.

5. Dne 18. listopadu 2022 Coreper tento kompromisní návrh posoudil a **jednomyslně se dohodl na jeho předložení Radě pro dopravu, telekomunikace a energetiku (telekomunikace) bez jakýchkoli změn za účelem dosažení obecného přístupu na jejím zasedání dne** 6. prosince 2022**.**

IV. HLAVNÍ PRVKY KOMPROMISNÍHO NÁVRHU

1. Evropská peněženka digitální identity

Jedním z hlavních politických cílů návrhu Komise týkajícího se evropské peněženky digitální identity (dále jen „peněženka“) je poskytnout občanům a ostatním rezidentům ve smyslu vnitrostátních právních předpisů harmonizovaný prostředek evropské digitální identity založený na koncepci evropské peněženky digitální identity. Jako prostředek pro elektronickou identifikaci (dále jen „prostředek eID“) vydaný v rámci vnitrostátních systémů s „vysokou“ úrovní záruky by peněženka byla samostatným prostředkem pro elektronickou identifikaci, jež by se zakládal na vydávání osobních identifikačních údajů a peněženky členskými státy.

2. Úroveň záruky evropské peněženky digitální identity

Úrovně záruky by měly vyjadřovat míru spolehlivosti prostředků pro elektronickou identifikaci při určování totožnosti osob a tím poskytovat záruku, že osoba deklarující konkrétní totožnost je skutečně osobou, s níž je tato totožnost spojena. Na základě široké podpory zaznamenané na zasedáních pracovní skupiny TELECOM a při rozpravě v Coreperu dne 14. října 2022 musí být peněženka vydávána v rámci elektronického identifikačního systému s „vysokou“ úrovní záruky. Kromě toho bylo do **článku 6a** doplněno zvláštní ustanovení o onboardingu uživatelů. Cílem této změny je reagovat na obavy členských států, v nichž již byl vydán významný počet

vnitrostátních prostředků pro elektronickou identifikaci se „značnou“ úrovní záruky. Uvedené ustanovení umožňuje uživateli používat vnitrostátní prostředek pro elektronickou identifikaci ve spojení s dodatečnými postupy onboardingu na dálku, aby bylo možné prokazovat totožnost při „vysoké“ úrovni záruky a v konečném důsledku peněženku získat. Vzhledem k tomu, že návrh nařízení o elektronické identifikaci se opírá o systémy certifikace kybernetické bezpečnosti, které by měly zajistit harmonizovanou úroveň důvěry v bezpečnost evropských peněženek digitální identity, se očekává, že certifikace kybernetické bezpečnosti se bude rovněž vztahovat na bezpečné ukládání kryptografických materiálů. Předsednictví proto navrhlo nový **bod odůvodnění 10b**, který se zabývá těmito technickými předpoklady pro dosažení „vysoké“ úrovně záruky a umožnění procesu následné kontroly v rámci zavádění evropských peněženek digitální identity.

3. Oznamování spoléhajících se stran

3.1 **Článek 6b** o oznamování spoléhajících se stran byl přeformulován. Obecně platí, že postup oznamování, jehož prostřednictvím spoléhající se strana sděluje svůj záměr používat peněženku, by měl být nákladově efektivní, přiměřený riziku a měl by zajistit, aby spoléhající se strana poskytla alespoň informace nezbytné k autentizaci v rámci peněženky. Standardně se požadují pouze minimální informace a oznamování by mělo umožnit použití automatizovaných nebo jednoduchých postupů vlastního oznamování.

3.2 Z důvodu odvětvových požadavků však může být nezbytný zvláštní režim, například u těch požadavků, které se vztahují na zpracování zvláštních kategorií osobních údajů. Proto bylo zavedeno příslušné ustanovení, jehož cílem je upravovat případy, kdy je vyžadován přísnější postup registrace nebo povolení. Naopak, pokud unijní nebo vnitrostátní právní předpisy nestanoví zvláštní požadavky na přístup k informacím poskytovaným prostřednictvím peněženky, mohou členské státy tyto spoléhající se strany od povinnosti oznámit svůj záměr využívat peněženky osvobodit.

4. Certifikace

4.1 Za účelem osvědčení souladu peněženek nebo jejich částí s platnými požadavky na kybernetickou bezpečnost by nařízení mělo využívat příslušné a stávající systémy certifikace podle aktu o kybernetické bezpečnosti nebo jejich části, a mělo by se na ně spoléhat a nařizovat jejich použití. V důsledku toho se rámec aktu o kybernetické bezpečnosti plně uplatňuje, včetně

mechanismu vzájemného hodnocení mezi vnitrostátními orgány certifikace kybernetické bezpečnosti, který je stanoven v aktu o kybernetické bezpečnosti. Členské státy určí veřejné a soukromé subjekty akreditované k certifikaci peněženky, jak je stanoveno v aktu o kybernetické bezpečnosti, s cílem zajistit co největší soulad mezi nařízením o elektronické identifikaci a aktem o kybernetické bezpečnosti.

4.2 Kromě toho se Komise vyzývá, aby pověřila agenturu ENISA vypracováním a přijetím zvláštního systému v rámci aktu o kybernetické bezpečnosti pro certifikaci kybernetické bezpečnosti peněženky. Dokud nebude takový systém vyvinut, bude jako základní metodika pro certifikaci digitálních peněženek používán evropský systém certifikace kybernetické bezpečnosti založený na společných kritériích (EUCC) zveřejněný v rámci aktu o kybernetické bezpečnosti. U požadavků nesouvisejících s kybernetickou bezpečností, zejména těch, které se týkají jiných funkčních a provozních aspektů peněženky, je třeba sestavit seznam specifikací, postupů a referenčních norem. Tyto požadavky podléhají certifikaci.

5. Prováděcí lhůta pro poskytnutí peněženky

Na základě pokynů členských států bylo navrženo, aby se prováděcí období v délce 24 měsíců počítalo od přijetí prováděcích aktů uvedených v **čl. 6a odst. 11** a **čl. 6c odst. 4**.

6. Poplatky

V čl. 6a odst. 6a a v odpovídajícím bodě odůvodnění bylo objasněno, že vydání digitálních peněženek, jejich používání k autentizaci a zrušení by mělo být pro fyzické osoby bezplatné. S výjimkou případů, kdy se peněženky používají k autentizaci, mohou službám využívajícím peněženku vzniknout náklady, např. při vydávání elektronických potvrzení atributů k dané peněžence.

7. Přístup k hardwarovým a softwarovým prvkům včetně zabezpečeného prvku (Secure Element)

Předsednictví navrhlo stanovit výslovné propojení s nařízením (EU) 2022/1925, které zajišťuje přístup k hardwarovým a softwarovým prvkům v rámci hlavních služeb platforem poskytovaných strážci přístupu. Nově doplněný **článek 12b** objasňuje, že poskytovatelé digitálních peněženek a vydavatelé oznámených prostředků pro elektronickou identifikaci

jednající v rámci obchodní nebo profesní činnosti jsou podnikatelskými uživateli strážců přístupu ve smyslu příslušné definice v nařízení o digitálních trzích. Bod odůvodnění byl doplněn tak, aby uváděl důsledky propojení s aktem o digitálních trzích, konkrétně že by se od strážců přístupu mělo vyžadovat, aby bezplatně zajišťovali účinnou interoperabilitu se stejným operačním systémem, hardwarovými nebo softwarovými funkcemi, které jsou dostupné nebo používané při poskytování jejich vlastních doplňkových a podpůrných služeb, a aby zajišťovali přístup k tomuto operačnímu systému a funkcím za účelem interoperability.

8. Alternativní možnosti vydávání elektronického potvrzení atributů veřejnými subjekty

Bylo zachováno vydávání kvalifikovaných elektronických potvrzení atributů kvalifikovanými poskytovateli, včetně povinnosti členských států zajistit, aby atributy mohly být ověřovány na základě autentického zdroje v rámci veřejného sektoru. Kromě toho byla zavedena možnost, že elektronické potvrzení atributů se stejnými právními účinky jako kvalifikované elektronické potvrzení atributů může pro peněženku vydávat přímo subjekt veřejného sektoru odpovědný za daný autentický zdroj nebo subjekt veřejného sektoru pověřený subjektem veřejného sektoru odpovědným za daný autentický zdroj, pokud jsou splněny nezbytné požadavky. Tento návrh je zohledněn v nových **článcích 45a**, **45da** a v **příloze VII**.

9. Porovnání záznamů

Původní **článek 11a** byl přejmenován na Porovnání záznamů, neboť to lépe odráží cíl tohoto ustanovení. Na základě diskuse byl pro peněženky zachován koncept jedinečného a trvalého identifikátoru. Příslušná definice objasňuje, že identifikátor může sestávat z kombinace několika vnitrostátních a odvětvových identifikátorů, pokud slouží svému účelu. Výslovně se uvádí, že porovnávání záznamů může být usnadněno kvalifikovaným elektronickým potvrzením atributů. Dále bylo do **článku 11a** začleněno ochranné ustanovení, podle něhož členské státy zajistí ochranu osobních údajů a zabrání profilování uživatelů. Porovnání záznamů zajistí členské státy jakožto spoléhající se strany.

VI. ZÁVĚR

1. S ohledem na výše uvedené se Rada vyzývá, aby:

   – projednala kompromisní znění uvedené v příloze tohoto dokumentu;

– na zasedání Rady pro dopravu, telekomunikace a energetiku (telekomunikace) dne 6. prosince 2022 potvrdila obecný přístup k návrhu nařízení o evropské digitální identitě (evropská elektronická identifikace).

_____

PŘÍLOHA

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou 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[3],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

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

[3] Úř. věst. C, , s .
[4] COM(2020) 67 final.

(2) Evropská rada ve svých závěrech ze zasedání konaného ve dnech 1. a 2. října 2020[5] 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) Sdělení Komise ze dne 9. března 2021 nazvané „Digitální kompas 2030: Evropské pojetí digitální dekády“[6] stanoví cíl rámce Unie, který do roku 2030 povede k širokému zavedení důvěryhodné identity kontrolované uživatelem, která každému uživateli umožní mít svou komunikaci a přítomnost na internetu pod kontrolou.

(4) Harmonizovanější přístup k digitální identifikaci by měl snížit rizika a náklady spojené se současnou roztříštěností, jejíž příčinou je používání odlišných vnitrostátních řešení, a posílí jednotný trh tím, že umožní občanům, dalším rezidentům ve smyslu vnitrostátních právních předpisů a podnikům identifikovat se v on-line prostředí v celé Unii pohodlným a jednotným způsobem. Evropská peněženka digitální identity poslouží fyzickým a právnickým osobám v celé Unii jako harmonizovaný prostředek pro elektronickou identifikaci, který jim umožní provádět autentizaci údů 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 potvrzeních atributů, jako je vysokoškolský titul právně uznávaný a přijímaný všude v Unii. Cílem rámce pro evropskou digitální identitu je dosáhnout toho, že v oblasti digitální identity nebude třeba se spoléhat pouze na vnitrostátní řešení, ale postupně bude možné poskytovat elektronická potvrzení atributů platná na evropské úrovni. Poskytovatelé elektronických potvrzení atributů by měli těžit z jasného a jednotného souboru pravidel a orgány veřejné správy by měly mít možnost používat elektronické dokumenty v daném formátu.

---

5 https://www.consilium.europa.eu/cs/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

6 COM(2021) 118 final/2.

(4a) Několik členských států zavedlo a již do značné míry používá prostředky pro elektronickou identifikaci, které jsou v současné době poskytovateli služeb v Unii akceptovány. Kromě toho byly na základě stávajícího nařízení eIDAS investovány prostředky do vnitrostátních i přeshraničních řešení, včetně technické infrastruktury pro účely interoperability uzlů eIDAS. Aby byla zaručena doplňkovost a rychlé přijetí evropských peněženek digitální identity stávajícími uživateli oznámených prostředků pro elektronickou identifikaci a v zájmu minimalizace dopadů na stávající poskytovatele služeb, se očekává, že evropské peněženky digitální identity budou těžit ze zkušeností se stávajícími prostředky pro elektronickou identifikaci a budou využívat zavedenou infrastrukturu eIDAS na evropské a vnitrostátní úrovni.

(5) S cílem podpořit konkurenceschopnost evropských podniků by měli mít poskytovatelé on-line služeb možnost využívat řešení v oblasti digitální identity uznávaná v celé Unii, bez ohledu na to, ve kterém členském státě byla vydána, a těžit tak z harmonizovaného evropského přístupu k důvěře, bezpečnosti a interoperabilitě. Uživatelé i poskytovatelé služeb by měli mít možnost využívat stejné právní hodnoty, která je elektronickým potvrzením atributů přiznána v celé Unii.

(6) Zpracovávání osobních údajů při provádění tohoto nařízení se řídí nařízením (EU) 2016/679[7]. Toto nařízení by proto mělo stanovit zvláštní záruky, které poskytovatelům prostředků pro elektronickou identifikaci a elektronického potvrzování atributů zabrání kombinovat osobní údaje z jiných služeb s osobními údaji týkajícími se služeb, jež spadající do oblasti působnosti tohoto nařízení. Osobní údaje týkající se poskytování evropské peněženky digitální identity by měly být uchovávány logicky odděleně od jakýchkoli jiných údajů v držení vydavatele. Toto nařízení nebrání vydavatelům evropských peněženek digitální identity uplatňovat dodatečná technická opatření přispívající k ochraně osobních údajů, jako je fyzické oddělení osobních údajů týkajících se poskytování peněženek od jakýchkoli jiných údajů v držení vydavatele.

[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.

(7) Je nezbytné stanovit harmonizované podmínky pro vytvoření rámce pro evropské peněženky digitální identity, který mají členské státy zajistit a který by měl všem občanům Unie a ostatním rezidentům ve smyslu vnitrostátních právních předpisů umožnit bezpečně sdílet údaje týkající se jejich identity uživatelsky přívětivým a pohodlným způsobem a pod výhradní kontrolou uživatele. Technologie používané k dosažení těchto cílů by měly být vyvinuty tak, aby bylo dosaženo nejvyšší úrovně bezpečnosti, soukromí, uživatelské přívětivosti a široké použitelnosti. Členské státy by měly všem svým státním příslušníkům a rezidentům zajistit rovný přístup k digitální identifikaci.

(8) Aby se zajistilo, že spoléhající se strany se mohou spolehnout na používání evropských peněženek digitální identity, a aby byli uživatelé chráněni před neoprávněným používáním citlivých údajů, měly by být spoléhající se strany zaregistrovány v rámci postupu oznamování. Požadavky na oznamování, jež se uplatňují na spoléhající se strany, by se ve většině případů měly zakládat na poskytnutí omezeného množství informací požadovaných pro autentizaci spoléhající se strany pro účely evropské peněženky digitální identity. Tyto požadavky by měly rovněž umožnit používání automatizovaných nebo jednoduchých postupů vlastního hlášení, včetně spoléhání se na stávající rejstříky a jejich využívání členskými státy. Zároveň mohou na vnitrostátní úrovni nebo na úrovni Unie existovat zvláštní režimy pro kategorie citlivých údajů, které mohou spoléhajícím se stranám ukládat přísnější požadavky na registraci a povolení s cílem zabránit neoprávněnému použití údajů o totožnosti v takových případech. V jiných případech použití mohou být spoléhající se strany od povinnosti oznámit svůj záměr spoléhat se na evropskou peněženku digitální identity osvobozeny, například tehdy, pokud právo ověřovat konkrétní atributy nevyžaduje nebo neumožňuje autentizaci spoléhající se strany elektronickými prostředky. V těchto situacích, kdy dochází k osobnímu kontaktu, je uživatel obvykle schopen identifikovat spoléhající se stranu díky kontextu, například při interakci s pracovníkem půjčovny automobilů nebo lékárny. Postup oznamování se má řídit odvětvovými právními předpisy Unie nebo vnitrostátními právními předpisy, neboť umožňuje zohlednit různé případy použití, které se mohou lišit co do požadavků na registraci, provozního režimu (on-line/offline) nebo požadavku na autentizaci zařízení, jež mohou s evropskou peněženkou digitální identity interagovat. Ověřování používání evropské peněženky digitální identity spoléhajícími se stranami by se nemělo v rámci evropské peněženky digitální identity prosazovat jako povinnost.

(9) Všechny evropské peněženky digitální identity by měly uživatelům umožnit přeshraniční elektronickou identifikaci a autentizaci on-line a offline a zajistit tak přístup k široké škále veřejných a soukromých služeb. Aniž jsou dotčeny výsady členských států s ohledem na identifikaci jejich státních příslušníků a rezidentů, mohou peněženky rovněž sloužit institucionálním potřebám orgánů veřejné správy, mezinárodních organizací a orgánů, institucí a jiných subjektů Unie. Použití peněženky offline bude mít význam v mnoha odvětvích, včetně zdravotnictví, kde jsou služby často poskytovány prostřednictvím osobního kontaktu a elektronické předpisy by měly při ověřování pravosti využívat QR kódy nebo podobné technologie. Evropské peněženky digitální identity, spoléhající se na „vysokou“ úroveň záruky, by měly využít potenciálu, který nabízejí řešení odolná proti neoprávněným zásahům, jako jsou zabezpečené prvky, aby byly v souladu s bezpečnostními požadavky podle tohoto nařízení. Rovněž by měly uživatelům umožnit vytvářet a používat kvalifikované elektronické podpisy a pečetě, které jsou přijímány v celé EU. V zájmu zjednodušení a snížení nákladů pro osoby a podniky v celé EU, mimo jiné umožněním pravomocí k zastupování a elektronických mandátů, by členské státy měly vydávat evropské peněženky digitální identity založené na společných normách s cílem zajistit bezproblémovou interoperabilitu a vysokou úroveň bezpečnosti. Pouze příslušné orgány členských států mohou při zjišťování totožnosti osoby poskytnout vysoký stupeň spolehlivosti, a tedy poskytnout záruku, že osoba, která uvádí nebo uplatňuje určitou totožnost, je skutečně osobou, kterou tvrdí, že je. Evropské peněženky digitální identity se proto musí spoléhat na právní identitu občanů, ostatních rezidentů nebo právnických osob. Důvěru v evropské peněženky digitální identity by bylo možné posílit tím, že vydávající strany jsou povinny zavést vhodná technická a organizační opatření, aby zajistily úroveň bezpečnosti odpovídající rizikům, která představují pro práva a svobody fyzických osob, v souladu s nařízením (EU) 2016/679. Vydání evropských peněženek digitální identity, jejich používání k autentizaci a jejich zrušení je pro fyzické osoby bezplatné. Službám využívajícím peněženku mohou vzniknout náklady související například s vydáváním elektronických potvrzení atributů k peněžence.

(9a) 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 mohou členské státy stanovit právní a organizační opatření s cílem zvýšit flexibilitu pro vydavatele evropských peněženek digitální identity a umožnit dodatečné funkce evropských peněženek digitální identity nad rámec toho, co je stanoveno v tomto nařízení, mimo jiné zvýšením interoperability se stávajícími vnitrostátními prostředky pro elektronickou identifikaci. V žádném případě by to však nemělo být na úkor zajišťování hlavních funkcí evropských peněženek digitální identity, jak je stanoveno v tomto nařízení, ani by to nemělo vést k prosazování 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.

(10) V zájmu dosažení vysoké úrovně ochrany údajů, bezpečnosti a důvěryhodnosti by toto nařízení mělo stanovit harmonizovaný rámec upřesňující společné specifikace a požadavky platné pro evropské peněženky digitální identity. Soulad evropských peněženek digitální identity s těmito požadavky by měl být certifikován akreditovanými subjekty veřejného nebo soukromého sektoru, jež určí členské státy. Certifikace by se měla opírat zejména o příslušné evropské systémy certifikace kybernetické bezpečnosti, nebo jejich části, zřízené podle nařízení (EU) 2019/881[8], pokud zahrnují požadavky na kybernetickou bezpečnost platné pro evropské peněženky digitální identity. Využívání evropských systémů certifikace kybernetické bezpečnosti by mělo zajistit harmonizovanou úroveň důvěry v bezpečnost evropských peněženek digitální identity bez ohledu na to, kde v Unii jsou vydávány. Certifikace kybernetické bezpečnosti evropských peněženek digitální identity by měla vycházet z úlohy vnitrostátních certifikačních orgánů kybernetické bezpečnosti při dohledu a sledování souladu certifikátů vydaných subjekty posuzování shody v rámci jejich jurisdikce s příslušnými evropskými systémy kybernetické bezpečnosti. Podobně by certifikace měla případně využívat norem a technických specifikací, jak je uvedeno v nařízení (EU) 2019/881. Tyto specifikace mohou posloužit jako nejmodernější forma dokumentů, jak je uvedeno v příslušných systémech certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881. Pokud se na certifikaci příslušných služeb nebo procesů přispívajících k bezpečnosti peněženky nevztahuje žádný příslušný evropský systém certifikace kybernetické bezpečnosti zavedený podle nařízení (EU) 2019/881 , měly by být vhodné systémy vytvořeny v souladu s hlavou III nařízení (EU) 2019/881. Měl by být zaveden společný a harmonizovaný systém certifikace evropských peněženek digitální identity pro posouzení jejich souladu se společnými specifikacemi a požadavky stanovenými v tomto nařízení, s výjimkou specifikací a požadavků týkajících se kybernetické bezpečnosti a ochrany údajů, zejména pak s těmi, které se týkají funkčních a provozních aspektů. Pokud jde o tuto certifikaci, měly by být v zájmu zajištění vysoké úrovně důvěry a transparentnosti zavedeny mechanismy a postupy zaměřené na podporu vzájemného učení a spolupráce mezi členskými státy v oblasti sledování a přezkumu certifikačních orgánů a osvědčení a certifikačních zpráv, které vydávají. Tímto mechanismem vzájemného učení by nemělo být dotčeno nařízení (ES) 2016/679 a nařízení (EU) 2019/881. Certifikace peněženky podle nařízení (ES) 2016/679 je dobrovolná a lze ji mimo jiné použít k prokázání souladu s požadavky stanovenými v nařízení (ES) 2016/679, neboť se vztahují na evropské peněženky digitální identity a jejich poskytování evropským občanům.

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

(10a) Onboarding občanů a rezidentů týkající se používání evropské peněženky digitální identity by měl být usnadněn využitím prostředků pro elektronickou identifikaci vydaných s „vysokou“ úrovní záruky. Prostředky pro elektronickou identifikaci vydané se „značnou“ úrovní záruky by se měly používat pouze v případech, kdy harmonizované technické a provozní specifikace používající prostředky pro elektronickou identifikaci vydané se „značnou“ úrovní záruky v kombinaci s jinými doplňkovými prostředky pro ověřování totožnosti umožní splnit požadavky stanovené v tomto nařízení, pokud jde o „vysokou“ úroveň záruky. Tyto doplňkové prostředky nebo opatření by měly být spolehlivé a pro uživatele snadno použitelné, přičemž by mohly být založeny na možnosti používat postupy onboardingu na dálku, kvalifikované certifikáty podložené kvalifikovanými podpisy, kvalifikované elektronické potvrzení atributů nebo jejich kombinaci. K zajištění dostatečně širokého využívání evropských peněženek digitální identity by měly být v prováděcích aktech stanoveny harmonizované technické a provozní specifikace pro onboarding uživatelů pomocí prostředků pro elektronickou identifikaci, a to včetně těch, které jsou vydávány se „značnou“ úrovní záruky.

(10b) Cílem tohoto nařízení je poskytnout uživateli plně mobilní, bezpečnou a uživatelsky vstřícnou evropskou peněženku digitální identity. Jako přechodné opatření do doby, než budou k dispozici certifikovaná řešení zabezpečená proti nedovolené manipulaci, jako jsou zabezpečené prvky v zařízeních uživatelů, se evropské peněženky digitální identity mohou spoléhat na certifikované externí zabezpečené prvky pro ochranu kryptografického materiálu a jiných citlivých údajů nebo na oznámená vnitrostátní řešení na „vysoké“ úrovni záruky s cílem prokázat soulad s příslušnými požadavky nařízení, pokud jde o úroveň záruky peněženky. Použití výše uvedeného přechodného opatření by mělo být omezeno na případy vyžadující „vysokou“ úroveň záruky, jako je například onboarding uživatele týkající se peněženky a autentizace u služeb vyžadujících „vysokou“ úroveň záruky. Při autentizaci pro účely služeb vyžadujících „značnou“ úroveň záruky by se u evropské peněženky digitální identity použití výše uvedeného přechodného opatření vyžadovat nemělo. Tímto nařízením by neměly být dotčeny vnitrostátní podmínky pro vydávání a používání certifikovaného vnějšího zabezpečeného prvku v případě, že se o něj toto přechodné opatření opírá.

(11) Evropské peněženky digitální identity by měly zajišťovat nejvyšší úroveň ochrany a zabezpečení osobních údajů používaných k autentizaci bez ohledu na to, zda jsou tyto údaje uchovávány lokálně, nebo v rámci řešení založených na cloudu, a to při zohlednění různých úrovní rizika. Jedním ze způsobů identifikace zajišťujících vysokou úroveň spolehlivosti je zpracování biometrických údajů jako autentizačního faktoru u silné autentizace uživatele, zejména pokud se používá v kombinaci s jinými autentizačními prvky. Vzhledem k tomu, že biometrické údaje představují jedinečnou charakteristiku osoby, je jejich zpracování povoleno pouze na základě výjimek stanovených v čl. 9 odst. 2 nařízení (EU) 2016/679 a vyžaduje vhodné záruky přiměřené riziku, které může toto zpracování představovat pro práva a svobody fyzických osob.

(11a) Fungování evropských peněženek digitální identity by mělo být transparentní a mělo by umožňovat ověřitelné zpracování osobních údajů. Za tímto účelem se členské státy vyzývají, aby zveřejňovaly zdrojový kód softwarových součástí evropských peněženek digitální identity, které souvisejí se zpracováním osobních údajů a údajů právnických osob. Zveřejnění tohoto zdrojového kódu umožňuje společnosti, včetně uživatelů a vývojářů, porozumět jeho fungování. Rovněž se tím může zvýšit důvěra uživatelů v ekosystém evropských peněženek digitální identity a přispět k jejich bezpečnosti tím, že na slabá místa a chyby ve zdrojovém kódu bude moci upozorňovat každý uživatel. To dodavatele přiměje k tomu, aby nabízeli vysoce bezpečný výrobek a jeho bezpečnost udržovali. Členské státy se rovněž vyzývají k tomu, aby ve vhodných případech zdrojový kód na základě otevřené licence zpřístupnily. Otevřená licence umožňuje společnosti, včetně uživatelů a vývojářů, zdrojový kód měnit a opětovně ho použít.

(12) Aby se zajistilo, že evropský rámec digitální identity bude otevřen inovacím a technologickému rozvoji a obstojí v budoucnosti, měly by být členské státy vybízeny k tomu, aby společně zřizovaly zkušební prostředí (tzv. pískoviště) pro testování inovativních řešení v kontrolovaném a bezpečném prostředí, zejména za účelem zlepšení funkčnosti, ochrany osobních údajů, bezpečnosti a interoperability řešení a zahrnutí technických odkazů a právních požadavků do budoucích aktualizací. Toto prostředí by mělo podporovat začlenění evropských malých a středních podniků, začínajících podniků a samostatných inovátorů a výzkumných pracovníků.

(13) Nařízení (EU) 2019/1157[9] posiluje zabezpečení průkazů totožnosti prostřednictvím posílených bezpečnostních prvků, a to do srpna 2021. Členské státy by měly zvážit proveditelnost oznamování v rámci systémů elektronické identifikace s cílem rozšířit přeshraniční dostupnost prostředků pro elektronickou identifikaci.

(14) 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 č. 910/2014.

(15) 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 by měly podporovat spolupráci členských států v oblasti bezpečnosti a interoperability jejich oznámených systémů elektronické identifikace.

(16) Členské státy by měly k zajištění souladu s požadavky tohoto nařízení a příslušných prováděcích aktů 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 systémech certifikace, které mají být zřízeny na úrovni Unie podle nařízení (EU) 2019/881, na podporu jejich tvrzení o sladění systémů nebo jejich částí s požadavky nařízení o interoperabilitě a bezpečnosti oznámených systémů elektronické identifikace.

[9] 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).

(17a) Používání jedinečných a trvalých identifikátorů vydaných členskými státy nebo generovaných evropskou peněženkou digitální identity, spolu s použitím osobních identifikačních údajů, má zásadní význam pro zajištění toho, aby mohla být ověřena totožnost uživatele, zejména ve veřejném sektoru a je-li to vyžadováno vnitrostátním právem nebo právem Unie. Toto nařízení by mělo zajistit, aby se evropskou peněženkou digitální identity zajistil mechanismus umožňující párování záznamů, a to i prostřednictvím kvalifikovaných elektronických potvrzení atributů, a aby bylo možné zahrnout do souboru osobních identifikačních údajů jedinečné a trvalé identifikátory. Jedinečný a trvalý identifikátor může sestávat z jednoho nebo z více vnitrostátních či identifikačních údajů, které mohou být specifické pro dané odvětví pod podmínkou, že slouží k jedinečné identifikaci uživatele v celé Unii. Evropská peněženka digitální identity by rovněž měla poskytovat mechanismus, který umožní používat identifikátory specifické pro spoléhající se strany v těch případech, kdy použití jedinečného a trvalého identifikátoru vyžaduje vnitrostátní právo nebo právo Unie. Ve všech případech by měl mechanismus, který má usnadňovat párování záznamů a používání jedinečných a trvalých identifikátorů, zajišťovat, aby byl uživatel chráněn před zneužitím osobních údajů podle tohoto nařízení a platného práva Unie, zejména nařízení (EU) 2016/679, a to i před rizikem profilování a sledování souvisejícím s používáním evropské peněženky digitální identity.

(17aa) Je nezbytné zohlednit potřeby uživatelů, a tím podpořit poptávku po evropských peněženkách digitální identity. Je třeba ukazovat smysluplné případy použití a on-line služby, které evropské peněženky digitální identity využívají. 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 založené na evropských peněženkách 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.

(18) V souladu se směrnicí (EU) 2019/882[10] by osoby se zdravotním postižením měly mít možnost používat evropské peněženky digitální identity, služby vytvářející důvěru a produkty koncových uživatelů používané při poskytování těchto služeb na stejném základě jako ostatní uživatelé.

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

(20) Poskytování a využívání služeb vytvářejících důvěru nabývá na významu v kontextu mezinárodního obchodu a spolupráce. Mezinárodní partneři EU vytvářejí důvěryhodné rámce inspirované nařízením (EU) č. 910/2014. S cílem usnadnit uznávání těchto služeb a jejich poskytovatelů se proto mohou prováděcími právními předpisy stanovit 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, a to jako doplněk možnosti vzájemného uznávání služeb vytvářejících důvěru a poskytovatelů usazených v Unii a ve třetích zemích v souladu s článkem 218 Smlouvy. 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 v tomto nařízení, by měl být rovněž zajištěn soulad s příslušnými ustanoveními směrnice XXXX/XXXX (směrnice o bezpečnosti sítí a informací 2 (dále jen „směrnice NIS2“)) a nařízení (EU) 2016/679, jakož i používání důvěryhodných seznamů jako základních prvků pro budování důvěry.

[10] 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).

(21) Toto nařízení by mělo vycházet z aktů Unie zajišťujících spravedlivé trhy otevřené hospodářské soutěži v digitálním odvětví. Nařízení vychází zejména z nařízení (EU) 2022/1925, které zavádí pravidla pro poskytovatele hlavních služeb platforem určené jako strážci přístupu a mimo jiné strážcům přístupu zakazuje v souvislosti se službami nabízenými podnikatelskými uživateli využívajícími hlavní služby platforem tohoto strážce přístupu vyžadovat od podnikatelských uživatelů, aby používali identifikační službu strážce přístupu, nabízeli ji nebo s ní zajistili interoperabilitu. Ustanovení čl. 6 odst. 7 nařízení (EU) 2022/1925 vyžaduje, aby strážci přístupu umožnili podnikatelským uživatelům a poskytovatelům doplňkových služeb přístup ke stejným funkcím operačního systému, hardwaru nebo softwaru, které jsou k dispozici nebo používány při poskytování doplňkových služeb strážcem přístupu, a interoperabilitu s nimi. Podle čl. 2 odst. 15 aktu o digitálních trzích představují identifikační služby druh doplňkových služeb. Podnikatelští uživatelé a poskytovatelé doplňkových služeb by proto měli mít přístup k takovým funkcím hardwaru nebo softwaru, jako jsou zabezpečené prvky v chytrých telefonech, a měli by s nimi být interoperabilní prostřednictvím evropských peněženek digitální identity nebo prostředků pro elektronickou identifikaci oznámených členskými státy.

(22) 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 XXXX/XXXX (směrnice NIS 2) jsou služby vytvářející důvěru povinny přijmout vhodná technická a organizační opatření podle směrnice XXXX/XXXX (směrnice NIS 2), 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 se směrnicí XXXX/XXXX (směrnice NIS 2). Pokud jde o oznamování incidentů by měli poskytovatelé služeb vytvářejících důvěru hlásit jakékoli 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 došlo v souvislosti s identifikací osob. Požadavky na řízení kybernetických bezpečnostních rizik a oznamovací povinnosti podle směrnice XXXXXX [směrnice NIS 2] 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 XXXX/XXXX (směrnice NIS 2) 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. Žádnými požadavky podle tohoto nařízení není dotčena povinnost oznamovat porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679.

(23) Náležitá pozornost by se měla věnovat zajištění účinné spolupráce mezi orgány v oblasti bezpečnosti sítí a informací a orgány eIDAS. V případech, kdy se orgán dohledu podle tohoto nařízení liší od příslušných orgánů určených podle směrnice XXXX/XXXX [směrnice NIS 2], by tyto orgány měly úzce a včas spolupracovat formou výměny příslušných informací s cílem zajistit účinný dohled nad poskytovateli služeb vytvářejících důvěru a jejich dodržování požadavků stanovených v tomto nařízení a směrnici XXXX/XXXX [směrnice NIS 2]. Orgány dohledu by podle tohoto nařízení měly být zejména oprávněny požádat příslušný orgán podle směrnice XXXXX/XXXX [směrnice NIS 2] 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 o NIS 2, nebo po nich požadovat nápravu nedodržování pravidel.

(24) 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 celoevropské služby elektronického doporučeného doručování. Aby bylo zajištěno, že údaje využívající kvalifikovanou službu elektronického doporučeného doručování budou doručeny správnému adresátovi, měly by kvalifikované služby elektronického doporučeného doručování s plnou jistotou zajistit identifikaci adresáta, přičemž pokud jde o identifikaci odesílatele, postačovala by vysoká úroveň důvěry. Poskytovatelé kvalifikovaných služeb elektronického doporučeného doručování by měli být členskými státy vybízeni k tomu, aby jejich služby byly interoperabilní s kvalifikovanými službami elektronického doporučeného doručování poskytovanými jinými kvalifikovanými poskytovateli služeb vytvářejících důvěru s cílem zajistit snadnou převoditelnost elektronických registrovaných dat mezi dvěma nebo více kvalifikovanými poskytovateli služeb vytvářejících důvěru a prosazovat spravedlivé postupy na vnitřním trhu.

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

(26) Mělo by být možné vydávat a zpracovávat důvěryhodné digitální atributy a přispívat ke snižování administrativní zátěže, což by občany a ostatní rezidenty motivovalo využívat je při svých soukromých a veřejných transakcích. Občané a ostatní rezidenti 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.

(27) Každý subjekt, který shromažďuje, vytváří a vydává potvrzené atributy, jako jsou diplomy, licence či rodné listy, by měl mít možnost stát se poskytovatelem elektronického potvrzení atributů. Spoléhající se strany by měly elektronická potvrzení atributů používat jako rovnocenná potvrzením v tištěné podobě. Elektronickému potvrzení atributů by proto neměly být upírány právní účinky proto, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické potvrzení atributů. Za tímto účelem by měly být stanoveny obecné požadavky, které zajistí, aby kvalifikované elektronické potvrzení atributů mělo rovnocenný právní účinek jako zákonně vydaná potvrzení v tištěné podobě. 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.

(28) Široká dostupnost a použitelnost evropských peněženek digitální identity vyžaduje jejich přijetí soukromými poskytovateli služeb. Soukromé spoléhající se strany poskytující služby v oblasti dopravy, energetiky, bankovnictví, finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, vzdělávání nebo telekomunikací by měly akceptovat používání evropských peněženek digitální identity k poskytování služeb, u nichž se na základě vnitrostátních právních předpisů nebo právních předpisů Unie či smluvního závazku vyžaduje silná autentizace uživatele. V zájmu snazšího používání a přijímání evropské peněženky digitální identity by měly být zohledněny obecně uznávané odvětvové normy a specifikace. V případech, kdy velmi rozsáhlé on-line platformy ve smyslu článku 25.1 nařízení [odkaz na nařízení o aktu o digitálních službách] vyžadují, aby se uživatelé pro přístup k on-line službám autentizovali, by tyto platformy měly být povinny použití evropské peněženky digitální identity na dobrovolnou žádost uživatele akceptovat. Uživatelé by neměli mít povinnost používat peněženku k přístupu k soukromým službám, ale pokud si to přejí, měly by rozsáhlé on-line platformy za tímto účelem evropskou peněženku digitální identity akceptovat, přičemž by měla být dodržena zásada minimalizace údajů. Vzhledem k významu velmi rozsáhlých on-line platforem a k jejich dosahu, vyjádřenému zejména počtem příjemců služby a hospodářských transakcí, je to nezbytné v zájmu zvýšení ochrany uživatelů před podvody a zajištění vysoké úrovně ochrany údajů. 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 samoregulační kodexy chování na úrovni Unie (dále jen „kodexy chování“). 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 rozsáhlé platformy a kteří pro autentizaci uživatelů využívají služeb elektronické identifikace poskytovaných třetími stranami. Kodexy chování by měly být vypracovány do dvanácti měsíců od přijetí tohoto nařízení. Po 24 měsících od zavedení těchto ustanovení by Komise měla posoudit jejich účinnost z hlediska dostupnosti a použitelnosti evropských peněženek digitální identity pro uživatele.

(29) Výběrové sdělování je koncept, který opravňuje vlastníka údajů zveřejnit pouze určité části většího souboru údajů, aby přijímající subjekt získal pouze ty informace, které jsou vyžadovány, např. aby uživatel poskytl spoléhající se straně pouze údaje, které jsou nezbytné pro poskytování služby požadované uživatelem. Evropská peněženka digitální identity by měla výběrové sdělování atributů spoléhajícím se stranám technicky umožňovat. Tyto výběrově sdělované atributy, včetně případů, kdy byly původně součástí několika odlišných elektronických potvrzení, mohou být následně kombinovány a předloženy spoléhajícím se stranám. Tento prvek by se měl stát základním koncepčním prvkem, čímž se zvýší uživatelská přívětivost a ochrana osobních údajů, včetně minimalizace údajů.

(30) 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 vnitrostátními právními předpisy nebo právními předpisy Unie 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. Vhodné mechanismy mohou zahrnovat využívání konkrétních zprostředkovatelů nebo technických řešení v souladu s vnitrostátními právními předpisy, které umožňují přístup k autentickým zdrojům. Zajištěním dostupnosti mechanismu, který umožní ověřování atributů na základě autentických zdrojů, by se mělo usnadnit, aby kvalifikovaní poskytovatelé služeb vytvářejících důvěru poskytující kvalifikované elektronické potvrzování atributů plnili své povinnosti stanovené tímto nařízením. Příloha VI obsahuje seznam kategorií atributů, u nichž by členské státy měly 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. Členské státy by se měly dohodnout na zvláštních atributech, které do těchto kategorií spadají.

(31) Díky bezpečné elektronické identifikaci a potvrzování atributů by mělo mít odvětví finančních služeb k dispozici dodatečnou flexibilitu a řešení, která umožní identifikaci zákazníků a výměnu zvláštních atributů nezbytných ke splnění například požadavků na hloubkovou kontrolu klienta podle nařízení o boji proti praní peněz [odkaz bude přidán po přijetí návrhu] a požadavků přiměřenosti vyplývajících z právních předpisů na ochranu investorů, nebo k podpoře plnění požadavků na silnou autentizaci klienta k identifikaci pro účely on-line přihlášení se k účtu a zahájení transakcí v oblasti platebních služeb.

(31a) V zájmu zajištění jednotnosti certifikačních postupů v celé EU by Komise měla vydat pokyny pro certifikaci a opětovnou certifikaci prostředků pro vytváření kvalifikovaných elektronických podpisů a prostředků pro vytváření kvalifikovaných elektronických pečetí, včetně jejich platnosti a časových omezení. Toto nařízení nebrání členským státům v tom, aby veřejným nebo soukromým subjektům, které prostředky pro vytváření kvalifikovaných elektronických podpisů již certifikovaly, povolily platnost certifikace dočasně prodloužit, pokud by opětovná certifikace téhož prostředku nemohla být provedena v zákonem stanovené lhůtě z jiného důvodu, než je narušení bezpečnosti nebo bezpečnostní incident, a aniž je dotčena příslušná certifikační praxe.

(32) Služby autentizace internetových stránek poskytují uživatelům vysokou úroveň záruky, že dané stránky reprezentují skutečný a legitimní subjekt bez ohledu na to, která platforma se k jejich zobrazení využívá. Tyto služby přispívají k budování důvěry v podnikání on-line a jeho důvěryhodnosti a ke snižování počtu podvodů na internetu. Využívání služeb autentizace internetových stránek internetovými stránkami by mělo být dobrovolné. Aby se však autentizace internetových stránek stala prostředkem ke zvyšování důvěry, zlepšení uživatelské zkušenosti a k podpoře růstu na vnitřním trhu, mělo by toto nařízení pro poskytovatele služeb autentizace internetových stránek a jejich služby stanovit minimální povinnosti v oblasti bezpečnosti a odpovědnosti. Za tímto účelem by poskytovatelé internetových prohlížečů měli zajistit podporu a interoperabilitu s kvalifikovanými certifikáty pro autentizaci internetových stránek podle nařízení (EU) č. 910/2014. Měli by uznávat kvalifikované certifikáty pro autentizaci internetových stránek a umožnit, aby se certifikované údaje o totožnosti koncovému uživateli zobrazovaly v prostředí prohlížeče na základě specifikací stanovených v souladu s tímto nařízením. Uznáním kvalifikovaného certifikátu pro autentizaci internetových stránek jako kvalifikovaného certifikátu vydaného kvalifikovaným poskytovatelem služeb vytvářejících důvěru by se mělo zajistit, že je možné údaje o totožnosti obsažené v certifikátu autentizovat a ověřit v souladu s tímto nařízením. Tím by neměla být dotčena možnost, aby poskytovatelé internetových prohlížečů řešili závažné neshody související s narušením bezpečnosti a ztrátou integrity jednotlivých certifikátů a přispívali tak k on-line bezpečnosti koncových uživatelů. Za účelem zvýšení ochrany občanů 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.

(33) Mnoho členských států zavedlo vnitrostátní požadavky na služby poskytující bezpečnou a důvěryhodnou digitální archivaci, aby bylo možné dlouhodobě uchovávat elektronické údaje 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 rámec 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 na dokumenty vytvořené elektronicky i na tištěné dokumenty, které byly naskenovány a digitalizovány. V případě potřeby by tato ustanovení měla umožnit přenos uchovávaných elektronických dat na různá média nebo jejich převedení do různých formátů za účelem prodloužení jejich trvanlivosti a čitelnosti i po uplynutí doby technické platnosti a zároveň v co největší možné míře minimalizovat ztráty a změny. Pokud elektronická data předložená digitální 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 údajů dat na dobu jejich uchovávání, případně s využitím jiných kvalifikovaných elektronických služeb vytvářejících důvěru stanovených tímto nařízením. K vytváření důkazů o uchovávání v případech, kdy se používají elektronické podpisy, elektronické pečetě nebo elektronická časová razítka, by se měly používat kvalifikované elektronické služby vytvářející důvěru. V případech, kdy nejsou služby elektronické archivace tímto nařízením harmonizovány, mohou členské státy v souladu s právem Unie zachovat nebo zavést vnitrostátní předpisy týkající se těchto služeb, jako jsou zvláštní ustanovení umožňující určité odchylky pro služby integrované do organizace a používané výhradně pro „interní archivaci“ v rámci této organizace. Toto nařízení by nemělo rozlišovat mezi dokumenty vytvořenými elektronicky a fyzickými dokumenty, které byly digitalizovány.

(33a) Národní archivy a paměťové instituce jsou jakožto organizace zabývající se ochranou dokumentárního dědictví ve veřejném zájmu obvykle pověřeny prováděním svých činností podle vnitrostátního práva a nemusí nutně poskytovat služby vytvářející důvěru ve smyslu tohoto nařízení. Pokud tyto instituce takové služby neposkytují, není jejich fungování tímto nařízením dotčeno.

(34) Elektronické účetní knihy představují pořadí elektronických datových záznamů, které zajišťuje jejich integritu a přesnost jejich chronologického řazení. Účelem elektronických účetních knih je vytvořit chronologickou posloupnost datových záznamů, aby se zabránilo kopírování digitálních aktiv a jejich prodeji několika různým příjemcům. Elektronické účetní knihy lze například použít pro digitální záznamy vlastnictví v rámci celosvětového obchodu, financování dodavatelského řetězce, digitalizaci práv duševního vlastnictví nebo komodit, jako je elektřina. Ve spojení s dalšími technologiemi mohou přispět k nalezení řešení pro účinnější a transformační veřejné služby, jako je elektronické hlasování, přeshraniční spolupráce celních orgánů, přeshraniční spolupráce akademických institucí nebo zaznamenávání vlastnictví nemovitostí v decentralizovaných katastrech nemovitostí. Kvalifikované elektronické účetní knihy vytvářejí právní předpoklad pro jedinečné a přesné sekvenční chronologické pořadí a integritu datových záznamů v účetní knize. Specifické atributy elektronických účetních knih, tj. postupné chronologické řazení datových záznamů, odlišuje elektronické účetní knihy od ostatních služeb vytvářejících důvěru, jako jsou elektronická časová razítka a služby elektronického doporučeného doručování. Konkrétně ani časové razítkování digitálních dokumentů, ani jejich předávání prostřednictvím služeb elektronického doporučeného doručování by bez dalších technických nebo organizačních opatření nemohly dostatečně zabránit tomu, aby bylo stejné digitální aktivum zkopírováno a opakovaně prodáno různým stranám. Proces vytváření a aktualizace elektronické účetní knihy závisí na typu používané účetní knihy (centralizovaná nebo distribuovaná).

(35) Aby se zabránilo roztříštěnosti vnitřního trhu by měl být zřízen celoevropský právní rámec, který by umožnil přeshraniční uznávání služeb vytvářejících důvěru pro účely zaznamenávání údajů do kvalifikovaných elektronických účetních knih. Poskytovatelům služeb vytvářejících důvěru pro elektronické účetní knihy by měla být uložena povinnost kontrolovat postupné zaznamenávání údajů do účetní knihy. Toto nařízení platí bez ohledu na jakékoli právní povinnosti, které uživatelé elektronických účetních knih případně musí dodržovat podle právních předpisů Unie a vnitrostátních právních předpisů. Například případy použití, které zahrnují zpracování osobních údajů, by měly být v souladu s nařízením (EU) 2016/679. Případy použití, které zahrnují kryptoaktiva, by měly být slučitelné se všemi platnými finančními pravidly, například se směrnicí o trzích finančních nástrojů[11], směrnicí o platebních službách[12], směrnicí o elektronických penězích[13], jakož i s možnými budoucími právními předpisy o trzích s kryptoaktivy a s pravidly pro boj proti praní peněz, která by mohla být zahrnuta do nařízení týkajícího se převodů finančních prostředků[14] a mohla by vyžadovat, aby poskytovatelé služeb souvisejících s kryptoaktivy ověřovali totožnost uživatelů elektronických účetních knih s cílem dodržovat mezinárodní normy pro boj proti praní peněz.

---

11 Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnice 2002/92/ES, Úř. věst. L 173, 12.6.2014, s. 349.

12 Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES, Úř. věst. L 337, 23.12.2015, s. 35.

13 Směrnice Evropského parlamentu a Rady 2009/110/ES ze dne 16. září 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností, o změně směrnic 2005/60/ES a 2006/48/ES a o zrušení směrnice 2000/46/ES, Úř. věst. L 267, 10.10.2009, s. 7.

14 Viz návrh Komise ze dne 20. července 2021 na přepracování nařízení Evropského parlamentu a Rady (EU) 2015/847 ze dne 20. května 2015 o informacích doprovázejících převody peněžních prostředků, COM/2021/422 final.

(36) K tomu, aby se zabránilo roztříštěnosti a překážkám v důsledku rozdílných norem a technických omezení a aby se zajistil koordinovaný postup, který zabrání tomu, aby bylo provádění budoucího evropského rámce digitální identity ohroženo, je nezbytné zavést úzkou a strukturovanou spolupráci mezi Komisí, členskými státy a soukromým sektorem. K dosažení tohoto cíle by členské státy měly spolupracovat v rámci stanoveném v doporučení Komise XXX/XXXX [soubor nástrojů pro koordinovaný přístup k evropskému rámci digitální identity][15] s cílem určit soubor nástrojů pro evropský rámec digitální identity. Soubor nástrojů by měl zahrnovat komplexní technickou architekturu a referenční rámec, soubor společných norem a technických referencí a soubor pokynů a popis osvědčených postupů zahrnujících alespoň všechny aspekty funkcí a interoperability evropských peněženek digitální identity, včetně elektronických podpisů, a kvalifikované služby vytvářející důvěru pro potvrzování atributů, jak je stanoveno v tomto nařízení. V této souvislosti by členské státy měly rovněž dosáhnout dohody o společných prvcích obchodního modelu a struktuře poplatků evropských peněženek digitální identity s cílem usnadnit jejich přijímání, zejména malými a středními podniky v přeshraničním kontextu. Obsah souboru nástrojů by se měl vyvíjet souběžně s diskusí a procesem přijetí evropského rámce digitální identity a měl by odrážet výsledek této diskuse a tohoto procesu.

(36a) 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 vedou k přesvědčení, že nekvalifikované služby vytvářející důvěru nabízené tímto poskytovatelem jsou kvalifikované.

[15] [po přijetí vložit odkaz]

(36b) Toto nařízení by mělo zajistit harmonizovanou úroveň kvality, důvěryhodnosti a bezpečnosti kvalifikovaných služeb vytvářející důvěru bez ohledu na místo, 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 mimo Unii, pokud poskytne záruky, jimiž zajistí, aby mohly být činnosti dohledu a audity vymáhány tak, jako by tyto operace byly prováděny v Unii. Nelze-li soulad s nařízením plně zajistit, měly by mít orgány dohledu možnost přijmout přiměřená a odůvodněná opatření, včetně odnětí statusu kvalifikované služby vytvářející důvěru.

(36c) V zájmu zajištění právní jistoty ohledně platnosti zaručených elektronických podpisů založených na kvalifikovaných certifikátech je nezbytné upřesnit prvky zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, které by měla posoudit spoléhající se strana, jež ověření daného podpisu provádí.

(36d) Poskytovatelé služeb vytvářejících důvěru by měli používat šifrovací algoritmy odrážející stávající osvědčené postupy a důvěryhodné provádění těchto algoritmů, aby zajistili bezpečnost a spolehlivost svých služeb vytvářejících důvěru.

(36e) Toto nařízení by mělo kvalifikovaným poskytovatelům služeb vytvářejících důvěru stanovit povinnost ověřovat totožnost fyzické nebo právnické osoby, které je kvalifikovaný certifikát vydáván, na základě různých harmonizovaných metod platných v celé EU. Metoda může spočívat v použití prostředků pro elektronickou identifikaci, které splňují požadavky „značné“ úrovně záruky v kombinaci s dalšími harmonizovanými postupy na dálku, čímž se zajistí identifikace osoby s vysokou mírou spolehlivosti.

(36f) Vydavatelé evropských peněženek digitální identity a vydavatelé oznámených prostředků pro elektronickou identifikaci jednající v rámci obchodní nebo profesní činnosti, která využívá hlavních služeb platforem nabízených strážcem přístupu za účelem nebo v průběhu poskytování zboží a služeb koncovým uživatelům , by měli být považováni za podnikatelské uživatele v souladu s čl. 2 bodem 21 nařízení (EU) 2022/1925. Strážci přístupu by proto měli mít povinnost bezplatně zajistit účinnou interoperabilitu se stejnými funkcemi operačního systému, hardwaru nebo softwaru jako jsou ty, které má k dispozici nebo používá při poskytování vlastních doplňkových a podpůrných služeb a hardwaru, a zajistit k nim přístup pro účely interoperability. Tím by se mělo vydavatelům evropských peněženek digitální identity a vydavatelům oznámených prostředků pro elektronickou identifikaci umožnit se prostřednictvím rozhraní nebo podobných řešení propojit s příslušnými prvky stejně účinně, jako je tomu u vlastních služeb nebo hardware strážce přístupu.

(36g) Aby bylo toto nařízení v souladu se současným vývojem a aby byly dodržovány 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, které se na vnitřním trhu objevily.

(37) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1525 byl konzultován evropský inspektor ochrany údajů[16].

(38) Nařízení (EU) 910/2014 by proto mělo být odpovídajícím způsobem změněno,

PŘIJALY TOTO NAŘÍZENÍ:

Článek 1

Nařízení (EU) 910/2014 se mění takto:

[16] 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).

1) Článek 1 se nahrazuje tímto:

„Toto nařízení má za cíl zajistit řádné fungování vnitřního trhu a současně poskytovat odpovídající úroveň bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru. Za těmito účely toto nařízení:

aa) stanoví podmínky, za nichž členské státy poskytují a uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému elektronické identifikace jiného členského státu;

ab) stanoví podmínky, za nichž členské státy poskytují a uznávají 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, elektronické ověřování platnosti elektronických podpisů, elektronických pečetí a jejich certifikátů, elektronické ověřování platnosti certifikátů pro autentizaci internetových stránek, elektronické uchovávání elektronických podpisů, elektronických pečetí a jejich certifikátů, elektronickou archivaci, elektronické potvrzování atributů, správu prostředků pro vytváření kvalifikovaných elektronických podpisů a pečetí na dálku a pro elektronické účetní knihy;“.

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 není dotčeno vnitrostátní právo ani právo Unie týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy nebo požadavků pro konkrétní odvětví týkajících se formy.“;

3) Článek 3 se mění takto:

(X) bod 1 se nahrazuje tímto:

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

a) bod 2 se nahrazuje tímto:

„2) „prostředkem pro elektronickou identifikaci“ hmotná či nehmotná jednotka, včetně evropských peněženek digitální identity, obsahující osobní identifikační údaje, která se používá k autentizaci pro účely on-line služby nebo případně offline služby;“;

aa) bod 3 se nahrazuje tímto:

„3) „osobními identifikačními údaji“ soubor údajů, vydaných v souladu s právními předpisy Unie nebo vnitrostátními právními předpisy, umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující fyzickou či právnickou osobu;“;

b) bod 4 se nahrazuje tímto:

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

ba) bod 5 se nahrazuje tímto:

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

bb) vkládá se nový bod 5a, který zní:

„5a) „uživatelem“ fyzická či právnická osoba nebo fyzická osoba zastupující fyzickou či právnickou osobu, která využívá služeb vytvářejících důvěru nebo prostředků pro elektronickou identifikaci poskytovaných podle tohoto nařízení;“;

c) bod 14 se nahrazuje tímto:

„14) „certifikátem pro elektronický podpis“ elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby;“;

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;

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

b) ve vytváření elektronických podpisů nebo elektronických pečetí;

c) v ověřování platnosti elektronických podpisů nebo elektronických pečetí;

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

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

f) ve vydávání elektronických potvrzení atributů;

fa) v ověřování platnosti elektronického potvrzení atributů;

g) ve vytváření elektronických časových razítek;

ga) v ověřování platnosti elektronických časových razítek;

gb) v poskytování služeb elektronického doporučeného doručování;

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

h) v elektronické archivaci elektronických údajů; nebo

i) v zaznamenávání elektronických údajů do elektronické účetní knihy;“;

da) bod 18 se nahrazuje tímto:

18) „subjektem posuzování shody“ subjekt vymezený v čl. 2 bodě 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 provádět certifikaci evropských peněženek digitální identity nebo prostředků pro elektronickou identifikaci;“;

e) 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;“;

f) vkládají se nové body 23a a 23b, které znějí:

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

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

g) bod 29 se nahrazuje tímto:

„29) „certifikátem pro elektronickou pečeť“ elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí s určitou právnickou osobou a potvrzuje název této osoby;“;

h) bod 41 se nahrazuje tímto:

„41) „ověřováním platnosti“ postup ověření a potvrzení, že data v elektronické podobě jsou v souladu s požadavky tohoto nařízení platná;“;

i) doplňují se nové body 42 až 55b, které znějí:

„42) „evropskou peněženkou digitální identity“ prostředek pro elektronickou identifikaci, který uživateli umožňuje uchovávat a vyhledávat údaje o totožnosti, včetně osobních identifikačních údajů, elektronických potvrzení atributů spojených s jeho totožností, poskytovat je na požádání spoléhajícím se stranám a používat je pro autentizaci, on-line a případně offline, pro službu v souladu s článkem 6a; a umožňuje podepisovat kvalifikovanými elektronickými podpisy a pečetit kvalifikovanými elektronickými pečetěmi;

43) „atributem“ rys, vlastnost, právo nebo povolení fyzické nebo právnické osoby nebo předmětu;

44) „elektronickým potvrzováním atributů“ potvrzování v elektronické podobě, které umožňuje ověřování atributů;

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

45a) „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 45da a splňujících požadavky stanovené v příloze VII;

46) „autentickým zdrojem“ registr nebo systém, za který odpovídá subjekt veřejného sektoru nebo soukromý subjekt a který obsahuje a poskytuje atributy fyzické nebo právnické osoby a je považován za primární zdroj těchto informací nebo je v souladu s právem Unie nebo vnitrostátními právními předpisy včetně správní praxe uznán za autentický;

47) „elektronickou archivací“ služba zajišťující přijímání, uchovávání, vyhledávání a výmaz elektronických údajů s cílem zaručit jejich trvanlivost a čitelnost, jakož i zachovat jejich integritu, důvěrnost a důkaz původu po celou dobu uchovávání;

48) „kvalifikovanou službou elektronické archivace“ služba elektronické archivace, která splňuje požadavky stanovené v článku 45ga;

49) „značkou důvěry EU pro peněženku digitální identity“ ověřitelné, jednoduché, rozpoznatelné a jasné označení toho, že evropská peněženka digitální identity byla poskytnuta v souladu s tímto nařízením;

50) „silným ověřením uživatele“ ověření založené na použití nejméně dvou navzájem nezávislých faktorů pro ověření z různých kategorií, kterým může být znalost (něco, co ví pouze uživatel), držení (něco, co má v držení pouze uživatel) nebo inherence (něco, čím uživatel je), přičemž nesplněním jednoho z nich není ovlivněna spolehlivost ostatních a postup je koncipován tak, aby byla chráněna důvěrnost ověřovacích údajů;

53) „účetní knihou“ pořadí elektronických datových záznamů, které zajišťuje jejich integritu a přesnost jejich chronologického řazení;

53a) „elektronickou účetní knihou“ elektronická účetní kniha, která splňuje požadavky stanovené v článku 45i;

54) „osobními údaji“ veškeré informace ve smyslu čl. 4 bodu 1 nařízení (EU) 2016/679;

55) „párováním záznamů“ postup, při němž jsou osobní identifikační údaje, prostředky osobní identifikace, kvalifikované elektronické potvrzení atributů nebo potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem porovnávány nebo propojeny se stávajícím účtem patřícím téže osobě;

55a) „jedinečným a trvalým identifikátorem“ identifikátor, který může sestávat buď z jednoho nebo z více vnitrostátních či odvětvových identifikačních údajů a který je spojen s jediným uživatelem v rámci daného systému a je trvalý v čase;

55b) „datovým záznamem“ elektronická data zaznamenaná pomocí souvisejících metadat (nebo atributů) podporujících zpracování těchto údajů;

55c) „používáním evropských peněženek digitální identity offline“ se rozumí interakce mezi uživatelem a spoléhající se stranou na fyzickém místě, přičemž peněženka nemusí mít pro účely interakce prostřednictvím sítí elektronických komunikací přístup k dálkovým systémům.“

„Článek 5

Pseudonymy v elektronických transakcích

Aniž jsou dotčeny právní účinky, které vnitrostátní právo přiznává pseudonymům, není používání pseudonymů v elektronických transakcích zakázáno.“

5) V kapitole II se před článek 6a vkládá nadpis, který zní:

„ODDÍL I

Evropská peněženka digitální identity“.

7) Vkládají se nové články (6a, 6b, 6c a 6d), které znějí:

„*Článek 6a*

Evropské peněženky digitální identity

1. S cílem zajistit, aby všechny fyzické a právnické osoby v Unii měly bezpečný, důvěryhodný a hladký přeshraniční přístup k veřejným a soukromým službám, každý členský stát do 24 měsíců od vstupu prováděcích aktů uvedených v odstavci 11 a čl. 6c odst. 4 v platnost zajistí poskytování evropské peněženky digitální identity.

2. Evropské peněženky digitální identity jsou poskytovány:

   a) členským státem;

   b) z pověření členského státu; nebo

   c) nezávisle na členském státu, ale jsou uznávány členským státem.

3. Evropské peněženky digitální identity jsou prostředky pro elektronickou identifikaci, které uživateli umožňují transparentním a sledovatelným způsobem:

   a) bezpečně požadovat, vybírat, kombinovat, uchovávat, mazat a předkládat elektronické potvrzení atributů a osobní identifikační údaje spoléhajícím se stranám mimo jiné za účelem on-line a případně offline autentizace s cílem využívat veřejné a soukromé služby, přičemž by měla být zajištěna možnost výběrového sdělování dat;

   b) podepisovat kvalifikovanými elektronickými podpisy a pečetit kvalifikovanými elektronickými pečetěmi.

4. Evropské peněženky digitální identity zejména:

a) poskytují společný soubor rozhraní:

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

2) spoléhajícím se stranám, aby mohly požadovat osobní identifikační údaje a elektronická potvrzení atributů;

3) pro předkládání osobních identifikačních údajů nebo elektronického potvrzení atributů spoléhajícím se stranám online a případně i offline;

4) umožňující uživateli interakci s evropskou peněženkou digitální identity a zobrazení „značky důvěry EU pro peněženku evropské digitální identity“;

b) poskytovatelům služeb vytvářejících důvěru a elektronických potvrzení atributů neposkytují žádné informace o používání těchto atributů po jejich vydání;

ba) zajišťují, aby bylo možné ověřit totožnost spoléhajících se stran zavedením mechanismů autentizace v souladu s článkem 6b;

c) splňují požadavky stanovené v článku 8, pokud jde o „vysokou“ úroveň záruky, která se použije obdobně na správu a používání osobních identifikačních údajů prostřednictvím peněženky, včetně elektronické identifikace a autentizace;

e) zajišťují, aby osobní identifikační údaje uvedené v čl. 12 odst. 4 písm. d) jedinečně a trvale identifikovaly fyzickou či právnickou osobu nebo fyzickou osobu zastupující fyzickou či právnickou osobu, která je s nimi spojena;

4a. Členské státy stanoví postupy, které uživateli umožní nahlásit případnou ztrátu nebo zneužití své peněženky a požadovat její zrušení.

5. Členské státy pro evropské peněženky digitální identity poskytnou mechanismy ověření:

a) které zajistí, že je možné ověřit jejich pravost a platnost;

d) které uživateli umožní autentizovat spoléhající se strany v souladu s článkem 6b.

6. Evropské peněženky digitální identity jsou vydávány v rámci oznámeného systému elektronické identifikace s „vysokou“ úrovní záruky.

6a. Vydání evropských peněženek digitální identity, jejich používání k autentizaci a jejich zrušení je pro fyzické osoby bezplatné.

6b. Aniž je dotčen článek 6db, mohou členské státy v souladu s vnitrostátními právními předpisy stanovit dodatečné funkce evropských peněženek digitální identity, včetně interoperability se stávajícími vnitrostátními prostředky pro elektronickou identifikaci.

7. Používání evropské peněženky digitální identity a údajů v evropské peněžence digitální identity mají uživatelé plně pod kontrolou. Vydavatel evropské peněženky digitální identity neshromažďuje informace o používání peněženky, které nejsou nezbytné pro poskytování služeb peněženky, ani nekombinuje osobní identifikační údaje a jakékoli jiné uložené osobní údaje nebo údaje týkající se používání evropské peněženky digitální identity s osobními údaji z jiných služeb nabízených tímto vydavatelem nebo ze služeb třetích stran, které nejsou nezbytné pro poskytování služeb peněženky, 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 vydavatele evropské peněženky digitální identity. Pokud evropskou peněženku digitální identity poskytují soukromé strany v souladu s odst. 2 písm. b) a c), použijí se obdobně ustanovení čl. 45f odst. 4.

7a. Členské státy bez zbytečného odkladu oznámí Komisi informace o:

a) subjektu odpovědném za sestavení a vedení seznamu oznámených spoléhajících se stran, které využívají evropské peněženky digitální identity v souladu s čl. 6b odst. 2;

b) subjektech odpovědných za poskytování evropských peněženek digitální identity v souladu s čl. 6a odst. 1;

c) subjektech odpovědných za zajištění toho, aby osobní identifikační údaje byly spojeny s peněženkou v souladu s čl. 6a odst. 4 písm. e).

V oznámení rovněž poskytnou informace o mechanismu umožňujícím ověření osobních identifikačních údajů uvedených v čl. 12 odst. 4 a totožnosti spoléhajících se stran.

Informace uvedené v tomto odstavci Komise bezpečnou cestou zpřístupní veřejnosti ve formě opatřené elektronickým podpisem nebo pečetí a vhodné pro automatické zpracování.

8. Článek 11 se použije obdobně na evropskou peněženku digitální identity.

9. Ustanovení čl. 24 odst. 2 písm. b), e), g) a h) se použije obdobně na vydavatele evropské peněženky digitální identity.

10. Evropská peněženka digitální identity je zpřístupněna osobám se zdravotním postižením v souladu s požadavky na přístupnost stanovenými ve směrnici 2019/882.

11. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity technické a provozní specifikace a referenční normy pro požadavky uvedené v odstavcích 3, 4, 5 a 7a. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

11a. Komise stanoví technické a provozní specifikace, jakož i referenční normy s cílem usnadnit onboarding uživatelů týkající se evropské peněženky digitální identity za použití buď prostředků pro elektronickou identifikaci odpovídajících „vysoké“ úrovni, nebo prostředků pro elektronickou identifikaci odpovídajících „značné“ úrovni ve spojení s dalšími postupy dálkového onboardingu, které společně splňují požadavky „vysoké“ úrovně záruky. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

Článek 6b

Spoléhající se strany u evropských peněženek digitální identity

1. Pokud mají spoléhající se strany, které poskytují soukromé nebo veřejné služby, v úmyslu využívat evropské peněženky digitální identity poskytované v souladu s tímto nařízením, oznámí to členskému státu, v němž jsou spoléhající se strany usazeny.

1a. Postup oznamování je nákladově efektivní a přiměřený riziku a zajišťuje, aby spoléhající se strany poskytly alespoň informace nezbytné k autentizaci evropských peněženek digitální identity. To by mělo zahrnovat přinejmenším členský stát, v němž jsou usazeny, a název spoléhající se strany a případně její registrační číslo uvedené v úředních záznamech.

1b. Oznamovací povinností nejsou dotčeny jiné požadavky na oznamování a registraci v souladu s právem Unie nebo vnitrostátním právem, jako jsou požadavky vztahující se na zvláštní kategorie osobních údajů, které mohou vyžadovat dodatečné požadavky na povolení.

1c. Členské státy mohou spoléhající se strany od oznamovací povinnosti osvobodit, pokud právo Unie nebo vnitrostátní právo nestanoví zvláštní požadavky na oznamování nebo registraci pro účely přístupu k informacím poskytovaným prostřednictvím evropské peněženky digitální identity. Osvobozené spoléhající se strany nemají v rámci evropské peněženky digitální identity povinnost autentizace.

1d. Spoléhající se strany, které obdržely oznámení v souladu s tímto článkem, neprodleně informují členský stát o jakékoli následné změně původně poskytnutých informací.

2. Spoléhající se strany zajistí zavedení mechanismů autentizace uvedených v čl. 6a odst. 4 písm. ba).

3. Spoléhající se strany jsou odpovědné za provádění postupu autentizace osob a ověřování platnosti elektronických potvrzení atributů pocházejících z evropských peněženek digitální identity obdržených v souladu s čl. 6a odst. 4 písm. a) bod 2.

4. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 11 technické a provozní specifikace pro požadavky uvedené v odstavcích 1, 1a a 1d. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

Článek 6c

Certifikace evropských peněženek digitální identity

1. Soulad evropských peněženek digitální identity s požadavky stanovenými v čl. 6a odst. 3, 4 a 5, s požadavkem na logické oddělení stanoveným v čl. 6a odst. 7 a případně s požadavky stanovenými v čl. 6a odst. 11a certifikují subjekty posuzování shody akreditované v souladu s článkem 60 aktu o kybernetické bezpečnosti a se systémy, specifikacemi, normami a postupy uvedenými v souladu s odst. 4 písm. a), aa) a aaa) a určené členskými státy. Platnost certifikace nepřesáhne pět let a je podmíněna pravidelným dvouletým hodnocením zranitelnosti. Jsou-li zjištěna zranitelná místa a nejsou-li napravena do tří měsíců, certifikace se odejme.

2. Pokud jde o soulad s požadavky na ochranu údajů podle čl. 6a odst. 7, certifikace podle odstavce 1 může být doplněna osvědčením podle článku 42 nařízení (EU) 2016/679.

3. Soulad evropských peněženek digitální identity nebo jejich částí s příslušnými požadavky na kybernetickou bezpečnost stanovenými v čl. 6a odst. 3, 4, 5, 7 a případně 11a certifikují subjekty posuzování shody uvedené v odstavci 1 v rámci příslušných systémů certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881, jak jsou uvedeny v souladu s odst. 4 písm. a) a aa).

3a. Certifikované evropské peněženky digitální identity nepodléhají požadavkům uvedeným v článcích 7 a 9.

4. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů:

a) seznam systémů certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881 požadovaných pro certifikaci evropských peněženek digitální identity podle odstavce 3;

aa) specifikace, postupy a referenční normy pro jejich použití v rámci příslušných systémů certifikace kybernetické bezpečnosti uvedených v souladu s písmenem a);

aaa) seznam specifikací, postupů a referenčních norem, které stanoví společné požadavky na certifikaci, na něž se nevztahují příslušné systémy certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881 pro účely certifikace uvedené v odstavci 1, jejichž cílem je prokázat, že evropská peněženka digitální identity splňuje požadavky uvedené v odstavci 1;

b) technické, procedurální, organizační a provozní specifikace pro určení subjektů posuzování shody uvedených v odstavci 1 a v případě požadavků na certifikaci stanovených podle písmene aaa) pro sledování a přezkum systémů certifikace a souvisejících metod hodnocení, které tyto subjekty používají, a certifikátů a certifikačních zpráv, které vydávají.

5. Členské státy sdělí Komisi názvy a adresy veřejných nebo soukromých subjektů uvedených v odstavci 1. Komise tyto informace zpřístupní členským státům.

6. Prováděcí akty uvedené v odstavci 4 se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 6d

Zveřejnění seznamu certifikovaných evropských peněženek digitální identity

1. Členské státy bez zbytečného odkladu informují Komisi o evropských peněženkách digitální identity, které byly poskytnuty podle článku 6a a certifikovány subjekty uvedenými v čl. 6c odst. 1. Rovněž bez zbytečného odkladu informují Komisi o zrušení certifikace.

2. Na základě obdržených informací Komise sestavuje, zveřejňuje a aktualizuje strojově čitelný seznam certifikovaných evropských peněženek digitální identity.

3. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 11, formáty a postupy použitelné pro účely odstavců 1 a 2. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

Článek 6da

Narušení bezpečnosti evropských peněženek digitální identity

1. Pokud jsou evropské peněženky digitální identity vydané podle článku 6a nebo mechanismy ověření uvedené v čl. 6a odst. 5 písm. a), d) nebo e) porušeny nebo částečně ohroženy způsobem, který ovlivňuje jejich spolehlivost nebo spolehlivost ostatních evropských peněženek digitální identity, vydavatel dotčených peněženek bez zbytečného odkladu vydávání a používání evropské peněženky digitální identity pozastaví. Členský stát, v němž byly dotčené peněženky poskytnuty, bez zbytečného odkladu informuje členské státy a Komisi. Vydavatel dotčených peněženek nebo členský stát odpovídajícím způsobem informuje spoléhající se strany a uživatele.

2. Pokud bylo narušení nebo ohrožení bezpečnosti uvedené v odstavci 1 napraveno, vydavatel peněženky vydávání a používání evropské peněženky digitální identity obnoví. Členský stát, v němž byly dotčené peněženky poskytnuty, bez zbytečného odkladu informuje členské státy a Komisi. Vydavatel dotčených peněženek nebo členský stát bez zbytečného odkladu informuje spoléhající se strany a uživatele.

3. Není-li porušení nebo ohrožení uvedené v odstavci 1 napraveno do tří měsíců od pozastavení, dotčený členský stát dotyčnou evropskou peněženku digitální identity stáhne a odpovídajícím způsobem informuje ostatní členské státy a Komisi. Je-li to odůvodněno závažností porušení, je evropská peněženka digitální identity stažena bez zbytečného odkladu.

4. Komise bez zbytečného odkladu zveřejní v Úředním věstníku Evropské unie odpovídající změny v seznamu uvedeném v článku 6d.

5. Do šesti měsíců od vstupu tohoto nařízení v platnost Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 11, dále upřesní opatření uvedená v odstavcích 1, 2 a 3. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

Článek 6db

Přeshraniční využívání peněženek evropské digitální identity

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

2. Pokud vnitrostátní právo nebo právo Unie vyžadují od soukromých spoléhajících se stran poskytujících služby – s výjimkou mikropodniků a malých podniků vymezených v doporučení Komise 2003/361/ES – silnou autentizaci uživatele k on-line identifikaci nebo pokud smluvní závazek vyžaduje silnou autentizaci uživatele, a to i v oblasti dopravy, energetiky, bankovnictví, finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, vzdělávání nebo telekomunikací, soukromé spoléhající se strany nejpozději do 12 měsíců po datu poskytnutí evropských peněženek digitální identity podle čl. 6a odst. 1 a výhradně na dobrovolnou žádost uživatele začnou přijímat rovněž evropské peněženky digitální identity poskytnuté v souladu s tímto nařízením s ohledem na minimální údaje nezbytné pro konkrétní on-line službu, pro kterou se autentizace uživatele požaduje.

3. V případech, kdy velmi rozsáhlé on-line platformy ve smyslu článku 25 odst. 1 nařízení [odkaz na nařízení o aktu o digitálních službách] vyžadují, aby se uživatelé pro přístup k on-line službám autentizovali, přijímají za účelem autentizace uživatele rovněž evropské peněženky digitální identity poskytnuté v souladu s tímto nařízením výhradně 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 podporuje a usnadňuje vytvoření kodexů chování s cílem přispět k široké dostupnosti a použitelnosti evropských peněženek digitální identity v oblasti působnosti tohoto nařízení. Tyto kodexy chování usnadňují přijímání prostředků pro elektronickou identifikaci, včetně evropských peněženek digitální identity, které spadají do oblasti působnosti tohoto nařízení, zejména ze strany poskytovatelů služeb využívajících pro autentizaci uživatelů služby elektronické identifikace poskytované třetími stranami. Komise usnadní vypracování těchto kodexů chování v úzké spolupráci se všemi příslušnými zúčastněnými stranami a vyzve poskytovatele služeb, aby dokončili vypracování kodexů chování do dvanácti měsíců od přijetí tohoto nařízení a s účinností je zavedli do osmnácti měsíců od přijetí tohoto nařízení.

5. Komise do dvaceti čtyř měsíců od zavedení evropských peněženek digitální identity posoudí, zda by na základě důkazů prokazujících poptávku, dostupnost a použitelnost evropské peněženky digitální identity měli být k přijímání evropské peněženky digitální identity výhradně na dobrovolnou žádost uživatele povinni další soukromí poskytovatelé on-line služeb. Kritéria hodnocení zahrnují rozsah uživatelské základny, přeshraniční přítomnost poskytovatelů služeb, technologický rozvoj, vývoj způsobů využívání a poptávku spotřebitelů.

8) Před článek 7 se vkládá nadpis, který zní:

„ODDÍL II

SYSTÉMY ELEKTRONICKÉ IDENTIFIKACE“;

9) V článku 7 se úvodní věta nahrazuje tímto:

„Podle čl. 9 odst. 1 oznámí členské státy, které tak dosud neučinily, do 24 měsíců od vstupu prováděcích aktů uvedených v čl. 6a odst. 11 a čl. 6c odst. 4 v platnost alespoň jeden systém elektronické identifikace zahrnující nejméně jeden identifikační prostředek s „vysokou“ úrovní záruky. Systém elektronické identifikace je způsobilý pro oznámení podle čl. 9 odst. 1, jsou-li splněny všechny tyto podmínky:“;

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

„2. Komise zveřejní v Úředním věstníku Evropské unie seznam systémů elektronické identifikace, které byly oznámeny podle odstavce 1 tohoto článku, a základní informace o těchto systémech.

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

12) Vkládá se nový článek 11a, který zní:

„Článek 11a

Porovnávání záznamů

1. Používají-li se k autentizaci oznámené prostředky pro elektronickou identifikaci nebo evropské peněženky digitální identity, zajistí členské státy porovnávání záznamů, pokud jednají jako spoléhající se strany.

2. Členské státy pro účely poskytnutí evropské peněženky digitální identity zahrnou do minimálního souboru osobních identifikačních údajů uvedeného v čl. 12 odst. 4 písm. d) alespoň jeden jedinečný a trvalý identifikátor v souladu s právem Unie a vnitrostátními právními předpisy s cílem uživatele na jeho žádost identifikovat v případech, kdy je identifikace uživatele vyžadována právními předpisy.

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

2aa. Členské státy mohou v souladu s vnitrostátními právními předpisy stanovit, že uživatel evropské peněženky digitální identity musí mít možnost požádat, aby byl jedinečný a trvalý identifikátor zahrnutý do minimálního souboru osobních identifikačních údajů a spojený s peněženkou v souladu s čl. 6a odst. 4 písm. e) nahrazen jiným jedinečným a trvalým identifikátorem vydaným členským státem.

3. Do šesti měsíců od vstupu tohoto nařízení v platnost Komise prostřednictvím prováděcího aktu dále upřesní opatření uvedená v odstavci 1. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

3a. Do šesti měsíců od vstupu tohoto nařízení v platnost Komise prostřednictvím prováděcího aktu podrobně popíše opatření uvedená v odstavci 2 a 2aa. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

13) Článek 12 se mění takto:

Spolupráce a interoperabilita

a) v odstavci 3 se zrušuje písmeno d);

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

„d) odkazu na minimální soubor osobních identifikačních údajů nezbytných k jedinečné a trvalé identifikaci fyzické osoby, právnické osoby nebo fyzické osoby zastupující fyzické nebo právnické osoby;“;

ba) v odstavci 5 se doplňuje se písmeno c), které zní:

„c) podobného přístupu k on-line službám akceptujícím používání evropských peněženek digitální identity poskytovaných v souladu s tímto nařízením;“;

c) v odstavci 6 se písmeno a) nahrazuje tímto:

„a) výměnu informací, zkušeností a osvědčených postupů v oblasti systémů elektronické identifikace, a zejména v oblasti technických požadavků týkajících se interoperability, porovnávání záznamů a úrovní záruky;“;

ca) v odstavci 6 se doplňuje písmeno e), které zní:

„e) výměnu informací, zkušeností a osvědčených postupů a vydávání pokynů ohledně možných způsobů koncepce, rozvoje a provádění on-line služeb za účelem využívání evropské digitální peněženky“

14) Vkládají se nové články 12a a 12b, které znějí:

„Článek 12a

Certifikace systémů elektronické identifikace

1. Soulad systémů elektronické identifikace, které mají být oznámeny, s požadavky stanovenými v tomto nařízení se certifikuje za účelem prokázání souladu těchto systémů nebo jejich částí s požadavky stanovenými v čl. 8 odst. 2, pokud jde o úrovně záruky systémů elektronické identifikace v rámci příslušného systému certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881 nebo jeho částí, pokud se certifikát kybernetické bezpečnosti nebo jeho části vztahují na požadavky stanovené v čl. 8 odst. 2, pokud jde o úrovně záruky systémů elektronické identifikace. Platnost certifikace nepřesáhne pět let pod podmínkou pravidelného hodnocení zranitelnosti každé dva roky. Jsou-li zjištěna zranitelná místa a nejsou-li napravena do tří měsíců, certifikace se odejme.

   Certifikaci provádějí akreditované veřejné nebo soukromé subjekty posuzování shody určené členskými státy a v souladu s nařízením (ES) č. 765/2008.

2. Vzájemné hodnocení systémů elektronické identifikace uvedené v čl. 12 odst. 6 písm. c) se nevztahuje na systémy elektronické identifikace nebo na část těchto systémů certifikovaných v souladu s odstavcem 1.

2a. Bez ohledu na odstavec 2 tohoto článku mohou členské státy požadovat od oznamujícího členského státu doplňující informace o systémech elektronické identifikace nebo jejich částech certifikovaných podle odstavce 2 tohoto článku.

3. Členské státy sdělí Komisi názvy a adresy veřejných nebo soukromých subjektů uvedených v odstavci 1. Komise tyto informace zpřístupní členským státům.“;

„Článek 12b

Přístup k funkcím hardwaru a softwaru

Vydavatelé evropských peněženek digitální identity a vydavatelé oznámených prostředků pro elektronickou identifikaci jednající v rámci obchodní nebo profesní činnosti a používající hlavní služby platformy ve smyslu čl. 2 odst. 2 nařízení (EU) 2022/1925 pro účely poskytování nebo v průběhu poskytování služeb evropské peněženky digitální identity a prostředků pro elektronickou identifikaci koncovým uživatelům jsou podnikatelskými uživateli v souladu s čl. 2 bodem 21 nařízení (EU) 2022/1925.“

17) V článku 13 se odstavec 1 nahrazuje tímto:

„1. Bez ohledu na odstavec 2 tohoto článku poskytovatelé služeb vytvářejících důvěru odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle tohoto nařízení“;

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 škoda podle prvního pododstavce nastala bez jeho úmyslu nebo nedbalosti.“

18) Článek 14 se nahrazuje tímto:

„Článek 14

Mezinárodní aspekty

1. Služby vytvářející důvěru poskytované poskytovateli služeb vytvářejících důvěru usazenými ve třetí zemi či zřízenými 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 na základě prováděcího rozhodnutí uzavřeného mezi Unií a třetí zemí nebo mezinárodní organizací v souladu s článkem 218 Smlouvy.

2. Prováděcí rozhodnutí a dohody uvedené v odstavci 1 zajistí, že požadavky vztahující se na kvalifikované poskytovatele služeb vytvářejících důvěru usazené ve třetí zemi nebo zřízené mezinárodní organizací a jimi poskytované služby vytvářející důvěru splňují požadavky vztahující se na poskytovatele služeb vytvářející 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 důvěryhodných služeb.

   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 organizaci, s níž je dohoda uzavřena.

3. Prováděcí rozhodnutí uvedené v odstavci 1 se přijímají přezkumným postupem podle čl. 48 odst. 2.“

19) Článek 15 se nahrazuje tímto:

„Článek 15

Přístupnost pro osoby se zdravotním postižením

Poskytování služeb vytvářejících důvěru a konečných uživatelských produktů používaných při poskytování těchto služeb je zpřístupněno osobám se zdravotním postižením v souladu s požadavky na přístupnost stanovenými ve směrnici 2019/882 o požadavcích na přístupnost u výrobků a služeb.“;

20) Článek 17 se mění takto:

a) odstavec 4 se mění takto:

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

„c) informovat příslušné vnitrostátní orgány dotčených členských států určené podle směrnice (EU) XXXX/XXXX [směrnice NIS 2] o jakémkoli závažném narušení bezpečnosti nebo ztrátě integrity, o němž se dozví při plnění svých úkolů. Pokud se závažné narušení bezpečnosti nebo ztráta integrity týká jiných členských států, orgán dohledu informuje jednotné kontaktní místo dotčeného členského státu určené podle směrnice (EU) XXXX/XXXX (směrnice NIS 2) a orgány dohledu určené podle článku 17 tohoto nařízení v ostatních dotčených členských státech. Vyrozuměný orgán dohledu informuje veřejnost nebo požádá, aby tak učinil poskytovatel služeb vytvářejících důvěru, pokud rozhodne, že zveřejnění informací o narušení bezpečnosti nebo ztrátě integrity je ve veřejném zájmu;“;

2. písmeno f) se nahrazuje tímto:

„f) spolupracovat s příslušnými dozorovými úřady zřízenými podle 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 porušeních bezpečnosti, která podle všeho představují porušení ochrany osobních údajů;“;

b) odstavec 6 se nahrazuje tímto:

„6. Do 31. března každého roku předloží každý orgán dohledu Komisi zprávu o svých hlavních činnostech v předchozím kalendářním roce.“;

c) odstavec 8 se nahrazuje tímto:

„8. Do dvanácti měsíců od vstupu tohoto nařízení v platnost přijme Komise pokyny pro provádění úkolů uvedených v odstavci 4 orgány dohledu a prostřednictvím prováděcích aktů přijatých přezkumným postupem podle čl. 48 odst. 2 vymezí formu a postupy pro podávání zpráv uvedených v odstavci 6.“;

21) Článek 18 se mění takto:

a) název článku 18 se nahrazuje tímto:

„Vzájemná pomoc a spolupráce“;

b) odstavec 1 se nahrazuje tímto:

„1. Orgány dohledu vzájemně spolupracují za účelem výměny osvědčených postupů a informací týkajících se poskytování služeb vytvářejících důvěru.“;

c) doplňují se nové odstavce 4 a 5, které znějí:

„4. Orgány dohledu a příslušné vnitrostátní orgány podle směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX [směrnice NIS 2] spolupracují a vzájemně si pomáhají s cílem zajistit, aby poskytovatelé služeb vytvářejících důvěru dodržovali požadavky stanovené v tomto nařízení a směrnici (EU) XXXX/XXXX [směrnice NIS 2]. Orgány dohledu požádají příslušný vnitrostátní orgány podle směrnice XXXX/XXXX [směrnice NIS 2] o provedení opatření dohledu s cílem ověřit, zda poskytovatelé služeb vytvářejících důvěru splňují požadavky směrnice XXXX/XXXX (směrnice NIS 2), a to požadovat po poskytovatelích služeb vytvářejících důvěru nápravu v případě nedodržování těchto požadavků, včas poskytnout výsledky veškerých činností dohledu souvisejících s poskytovateli služeb vytvářejících důvěru a informovat orgány dohledu o příslušných incidentech oznámených v souladu se směrnicí XXXX/XXXX [směrnice NIS 2].

5. Do dvanácti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů nezbytná procesní opatření pro usnadnění spolupráce mezi orgány dohledu uvedenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

21a) Vkládá se nový článek 19a, který zní:

„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. Bez ohledu na ustanovení článku 18 směrnice EU XXXX/XXX [směrnice NIS 2] tato opatření zahrnují alespoň:

i) opatření týkající se postupů registrace ke službě a onboardingu;

ii) opatření týkající se procesních nebo správních kontrol;

iii) opatření týkající se řízení a provádění služeb.

b) oznámí orgánu dohledu, identifikovatelným dotčeným fyzickým osobám, veřejnosti, pokud je to ve veřejném zájmu, a případně dalším relevantním příslušným orgánům veškerá porušení nebo narušení poskytování služby nebo provádění opatření uvedených v písm. a) bodech i), ii) a 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 nich dozvěděl.

2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické vlastnosti opatření uvedených v odstavci 1a). Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

22) 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 je potvrzením toho, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení a článku 18 směrnice (EU) XXXX/XXXX [směrnice NIS 2]. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru předloží výslednou zprávu o posouzení shody do tří pracovních dnů od jejího obdržení orgánu dohledu.“;

aa) vkládá se nový odstavec, který zní:

1a. Členské státy mohou stanovit, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru předem informují orgán dohledu o plánovaných auditech a na žádost umožní účast orgánu dohledu jako pozorovatele.

b) v odstavci 2 se poslední věta nahrazuje tímto:

„Jestliže podle všeho došlo k porušení pravidel týkajících se ochrany osobních údajů, informuje orgán dohledu bez zbytečného odkladu příslušné dozorové úřady podle nařízení (EU) 2016/679.“;

c) odstavce 3 a 4 se nahrazují tímto:

„3. Pokud kvalifikovaný poskytovatel služeb vytvářejících důvěru nesplňuje některý z požadavků stanovených tímto nařízením, orgán dohledu po něm případně požaduje, aby ve stanovené lhůtě zjednal nápravu.

Pokud tento poskytovatel nezjedná nápravu, a to ve lhůtě případně stanovené orgánem dohledu, může orgán dohledu zejména s přihlédnutím k rozsahu, délce trvání a důsledkům daného neplnění odejmout danému poskytovateli nebo jím poskytované dotčené službě status kvalifikovaného poskytovatele nebo kvalifikované služby.

3a. Pokud je orgán dohledu příslušnými vnitrostátními orgány podle směrnice (EU) XXXX/XXXX [směrnice NIS 2] informován, že kvalifikovaný poskytovatel služeb vytvářejících důvěru nesplňuje některý z požadavků stanovených v článku 18 směrnice (EU) XXXX/XXXX [směrnice NIS 2], může orgán dohledu s přihlédnutím zejména k rozsahu, délce trvání a důsledkům daného neplnění odejmout danému poskytovateli nebo jím poskytované dotčené službě status kvalifikovaného poskytovatele nebo kvalifikované služby.

3b. Pokud je orgán dohledu informován dozorovými úřady podle nařízení (EU) 2016/679, že kvalifikovaný poskytovatel služeb vytvářejících důvěru nesplňuje některý z požadavků stanovených v nařízení (EU) 2016/679, může orgán dohledu s přihlédnutím zejména k rozsahu, délce trvání a důsledkům daného neplnění odejmout danému poskytovateli nebo jím poskytované dotčené službě 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 orgán uvedený v čl. 22 odst. 3 za účelem aktualizace důvěryhodných seznamů uvedených v čl. 22 odst. 1 a příslušný vnitrostátní orgán uvedený ve směrnici XXXX [směrnice NIS 2].

4. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro následující účely:

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 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.“;

23) Článek 21 se mění takto:

„1. Pokud poskytovatelé služeb vytvářejících důvěru hodlají začít poskytovat kvalifikovanou službu vytvářející důvěru, předloží orgánu dohledu oznámení o svém záměru spolu se zprávou o posouzení shody vydanou subjektem posuzování shody, která potvrzuje splnění požadavků stanovených v tomto nařízení a v článku 18 směrnice (EU) XXXX/XXXX [směrnice NIS 2].“;

a) odstavec 2 se nahrazuje tímto:

„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.

S cílem ověřit, zda poskytovatel služeb vytvářejících důvěru splňuje požadavky stanovené v článku 18 směrnice XXXX [směrnice NIS 2], orgán dohledu požádá příslušné orgány uvedené ve směrnici XXXX [směrnice NIS 2] o provedení příslušných opatření dohledu a o poskytnutí informací o výsledku bez zbytečného odkladu a nejpozději dva měsíce od doručení této žádosti příslušnými úřady uvedenými ve směrnici XXXX [směrnice NIS 2]. Není-li ověření dokončeno do dvou měsíců od oznámení, vyrozumí příslušný úřad uvedený ve směrnici XXXX [směrnice NIS 2] orgán dozoru a uvede důvody prodlení a dobu, v níž bude ověřování dokončeno.

Dojde-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 nebo 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 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 dvanácti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů formy a postupy oznamování a ověřování pro účely odstavců 1 a 2. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

25) 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 znaky fyzické nebo právnické osoby, jíž se kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů bude vydávat.

Kvalifikovaný poskytovatel služeb vytvářejících důvěru ověří informace uvedené v prvním pododstavci přímo nebo tím, že se spolehne na třetí osobu, a to jedním z těchto způsobů:

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 kvalifikovaného elektronického potvrzení atributů nebo 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, jejíž shodu potvrdí subjekt posuzování shody;

d) fyzickou přítomností fyzické osoby nebo oprávněného zástupce právnické osoby vhodnými postupy a v souladu s vnitrostátními právními předpisy.“;

b) doplňuje se nový odstavec 1a, který zní:

„1a. Do dvanácti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů minimální technické specifikace, normy a postupy týkající se ověřování identity a atributů v souladu s odst. 1 písm. c). Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

c) odstavec 2 se mění takto:

0) písmeno a) se mění takto:

„a) informuje orgán dohledu nejméně jeden měsíc před provedením jakékoli změny v poskytování svých kvalifikovaných služeb vytvářejících důvěru nebo tak učiní alespoň do tří měsíců v případě záměru ukončit tyto činnosti. Orgán dohledu si může před tím, než udělí svolení k provedení zamýšlených změn kvalifikovaných služeb vytvářejících důvěru vyžádat doplňující informace nebo výsledek posouzení shody. 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.

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

„d) před uzavřením smluvního vztahu informuje jasným, srozumitelným a jednoduše dostupným způsobem, ve veřejně dostupném prostoru a individuálně 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 pozměňování, a zajišťuje technickou bezpečnost a spolehlivost procesů, které podporují, včetně používání vhodných šifrovacích algoritmů, délek klíčů a hašovacích funkcí v systémech, produktech a v jimi podporovaných procesech;“;

2. vkládají se nová písmena fa) a fb), která znějí:

„fa) má vhodné politiky a přijímá odpovídající opatření pro řízení právních, obchodních, provozních a jiných přímých nebo nepřímých rizik poskytování kvalifikované služby vytvářející důvěru. Bez ohledu na ustanovení článku 18 směrnice EU XXXX/XXX [o bezpečnosti sítí a informací 2] tato opatření zahrnují alespoň:

i) opatření týkající se postupů registrace ke službě a onboardingu;

ii) opatření týkající se procesních nebo správních kontrol;

iii) opatření týkající se řízení a provádění služeb.“;

„fb) oznámí orgánu dohledu, identifikovatelným dotčeným fyzickým osobám, případně dalším relevantním příslušným orgánům a na žádost orgánu dozoru také veřejnosti, pokud je to ve veřejném zájmu, veškerá porušení nebo narušení poskytování služby nebo provádění opatření uvedených v písm. fa) bodech i), ii) a 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 k nim došlo.“;

3. písmena g) a h) 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;“;

4) písmeno j) se zrušuje;

d) doplňuje se nový odstavec 4a, který zní:

„4a. Odstavce 3 a 4 se odpovídajícím způsobem použijí na zrušení kvalifikovaného elektronických potvrzení atributů.“;

e) odstavec 5 se nahrazuje tímto:

„5. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace, postupy a referenční čísla norem pro požadavky uvedené v odstavci 2. Pokud jsou tyto technické specifikace, postupy a normy splněny, předpokládá se shoda s požadavky stanovenými v tomto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

f) vkládá se nový odstavec 6, který zní:

„6. Komisi je svěřena pravomoc přijímat prováděcí akty, kterými se stanoví technické vlastnosti opatření uvedených v odst. 2 písm. fa).“;

25a) Článek 26 se mění takto:

2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro zaručené elektronické podpisy. Pokud zaručený elektronický podpis těmto specifikacím a normám vyhovuje, předpokládá se shoda s požadavky pro zaručené elektronické podpisy. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

25b) Článek 27 se mění takto:

Odstavec 4 se zrušuje.

26) V článku 28 se odstavec 6 nahrazuje tímto:

„6. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro kvalifikované certifikáty pro elektronické podpisy. Pokud kvalifikovaný certifikát pro elektronický podpis těmto specifikacím a normám vyhovuje, 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 1a, který zní:

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

28) Vkládá se nový článek 29a, který zní:

„*Článek 29a*

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

1. Správu prostředků pro vytváření kvalifikovaných elektronických podpisů na dálku jako kvalifikované služby může provádět 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) může kopírovat data pro vytváření elektronických podpisů pouze pro účely zálohování a jsou-li splněny tyto požadavky:

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

ii. počet zkopírovaných souborů dat nepřesáhne minimum potřebné pro zajištění kontinuity služby;

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

2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro účely odstavce 1.“

29) V článku 30 se vkládá nový odstavec 3a, který zní:

„3a. Platnost certifikátu uvedeného v odstavci 1 nesmí překročit pět let pod podmínkou pravidelného hodnocení zranitelnosti každé dva roky. Jsou-li zjištěna zranitelná místa a nejsou-li napravena, certifikace se zruší.“

30) V článku 31 se odstavec 3 nahrazuje tímto:

„3. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů formáty a postupy použitelné pro účely odstavce 1. 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 vyhovuje specifikacím a normám uvedeným v odstavci 3, předpokládá se shoda s požadavky stanovenými v prvním pododstavci.“;

b) odstavec 3 se nahrazuje tímto:

„3. Do dvanácti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů specifikace a referenční čísla norem pro ověřování kvalifikovaných elektronických podpisů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

31a) Vkládá se nový článek 32a, který zní:

Požadavky na ověřování zaručených elektronických podpisů založených na kvalifikovaných certifikátech

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

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. Pokud ověřování platnosti zaručených elektronických podpisů založených na kvalifikovaných certifikátech vyhovuje specifikacím a normám uvedeným v odstavci 3, předpokládá se shoda s požadavky stanovenými v prvním pododstavci.

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

3. Do dvanácti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů specifikace a referenční čísla norem pro ověřování zaručených elektronických podpisů založených na kvalifikovaných certifikátech. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

31b) Článek 33 se mění takto:

„1. Kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů může poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který:“;

„2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro kvalifikovanou službu ověřování platnosti uvedenou v odstavci 1. Pokud služba ověřování platnosti kvalifikovaných elektronických podpisů vyhovuje těmto specifikacím a normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

32) Článek 34 se nahrazuje tímto:

„Článek 34

Kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů

1. Kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů může poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který používá postupy a technologie, jež jsou s to zajistit důvěryhodnost kvalifikovaného elektronického podpisu i po uplynutí doby technické platnosti.

2. Pokud postupy pro kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů vyhovují specifikacím a normám uvedeným v odstavci 3, předpokládá se shoda s požadavky stanovenými v odstavci 1.

3. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

32a) V článku 36 se doplňuje nový odstavec 2, který zní:

2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro zaručené elektronické pečetě.

Pokud zaručená elektronická pečeť těmto specifikacím a normám vyhovuje, předpokládá se shoda s požadavky pro zaručené elektronické pečetě. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

33) Článek 37 se mění takto:

Odstavec 4 se zrušuje.

34) Článek 38 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Kvalifikované certifikáty pro elektronické pečetě musí splňovat požadavky stanovené v příloze III. Pokud kvalifikovaný certifikát pro elektronickou pečeť vyhovuje specifikacím a normám uvedeným v odstavci 6, předpokládá se shoda s požadavky stanovenými v příloze III.“;

b) odstavec 6 se nahrazuje tímto:

„6. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro kvalifikované certifikáty pro elektronické pečetě. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

35) Vkládá se nový článek 39a, který zní:

„*Článek 39a*

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

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

35a) Vkládá se nový článek 40a, který zní:

„*Článek 40a*

Požadavky na ověřování zaručených elektronických pečetí založených na kvalifikovaném certifikátu

(1) Na ověřování zaručených elektronických pečetí založených na kvalifikovaném certifikátu se použije přiměřeně článek 32a.“

36) Článek 42 se mění takto:

a) doplňuje se nový odstavec 1a, který zní:

„1a. Pokud spojení data a času s daty a zdroj přesného času vyhovují specifikacím a normám uvedeným v odstavci 2, předpokládá se shoda s požadavky stanovenými v odstavci 1.“;

b) odstavec 2 se nahrazuje tímto:

„2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro spojení data a času s daty a pro zdroje přesného času. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

36a) V článku 43 se doplňuje nový odstavec 3, který zní:

2a. Kvalifikovaná služba elektronického doporučeného doručování v jednom členském státě se uznává jako kvalifikovaná služba elektronického doporučeného doručování v jakémkoli jiném členském státě.“

37) Článek 44 se mění takto:

a) doplňuje se nový odstavec 1a, který zní:

„1a. Pokud postup odesílání a přijímání dat vyhovuje specifikacím a normám uvedeným v odstavci 2, předpokládá se shoda s požadavky stanovenými v odstavci 1.“;

b) odstavec 2 se nahrazuje tímto:

„2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro postupy odesílání a přijímání dat. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

c) doplňují se nové odstavce 3 a 4, které znějí:

„3. Poskytovatelé kvalifikované služby doporučeného doručování se mohou dohodnout na interoperabilitě kvalifikovaných služeb doporučeného doručování, které poskytují. Tento rámec interoperability musí být v souladu s požadavky stanovenými v odstavci 1. Soulad musí potvrdit subjekt posuzování shody.“;

„4. Komise může prostřednictvím prováděcího aktu určit technické specifikace a referenční čísla norem s cílem usnadnit přenos dat mezi dvěma či více kvalifikovanými poskytovateli služeb vytvářejících důvěru. Technické specifikace a obsah norem musí být nákladově efektivní a přiměřené. Tento prováděcí akt se přijme přezkumným postupem podle čl. 48 odst. 2.“

38) 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 dodržení požadavků stanovených v příloze IV se provádí v souladu se specifikacemi a normami uvedenými v odstavci 4.

2. Kvalifikované certifikáty pro autentizaci internetových stránek uvedené v odstavci 1 jsou rozpoznávány internetovými prohlížeči. Pro tyto účely internetové prohlížeče zajistí, aby údaje o totožnosti poskytnuté pomocí kterékoli z metod byly zobrazeny uživatelsky přívětivým způsobem. Internetové prohlížeče zajistí podporu a interoperabilitu s kvalifikovanými certifikáty pro autentizaci internetových stránek uvedenými v odstavci 1, s výjimkou podniků, které jsou považovány za mikropodniky a malé podniky v souladu s doporučením Komise 2003/361/ES, v prvních pěti letech fungování jako poskytovatelé služeb prohlížení internetových stránek.

4. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů specifikace a referenční čísla norem pro kvalifikované certifikáty pro autentizaci internetových stránek uvedené v odstavci 1 a 2. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

39) Za článek 45 se vkládají nové oddíly 9, 10 a 11, které znějí:

„ODDÍL 9

ELEKTRONICKÉ POTVRZOVÁNÍ ATRIBUTŮ

Článek 45a

Právní účinky elektronického potvrzení atributů

1. Elektronickému potvrzení atributů nesmějí být upírány právní účinky a 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 zákonně vydaná potvrzení v tištěné podobě.

3. Kvalifikované elektronické potvrzení atributů vydané v jednom členském státě se uznává jako kvalifikované elektronické potvrzení atributů v jakémkoli jiném členském státě.

4. Potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem se ve všech členských státech uznává jako potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem.

Článek 45b

Elektronické potvrzování 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 potvrzování atributů z jiných členských států.

Článek 45c

Požadavky na kvalifikované elektronické potvrzení atributů

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

1a. Hodnocení dodržení požadavků stanovených v příloze V se provádí v souladu se specifikacemi a normami uvedenými v odstavci 4.

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

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

4. Do šesti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcího aktu o provádění evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 11, technické specifikace a referenční čísla norem pro kvalifikovaná elektronická potvrzení atributů.

Článek 45d

Ověřování atributů podle autentických zdrojů

1. Členské státy do 24 měsíců od vstupu v platnost prováděcích aktů uvedených v čl. 6a odst. 11 a čl. 6c odst. 4 zajistí, aby přinejmenším pro atributy uvedené v příloze VI, pokud se tyto atributy spoléhají na autentické zdroje v rámci veřejného sektoru, byla přijata opatření, která kvalifikovaným poskytovatelům elektronických potvrzení atributů umožní na žádost uživatele a v souladu s vnitrostátními právními předpisy nebo právními předpisy Unie tyto atributy elektronickými prostředky ověřit.

2. Do šesti měsíců od vstupu tohoto nařízení v platnost a s přihlédnutím k příslušným mezinárodním normám stanoví Komise prostřednictvím prováděcího aktu o provádění evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 11, minimální technické specifikace, normy a postupy s odkazem na katalog atributů a systémy potvrzování atributů a ověřovací postupy pro kvalifikovaná elektronická potvrzení atributů.

Článek 45da

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, jenž tvoří základ kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti subjektu veřejného sektoru uvedeného v článku 3 (45a) určeného jako vydavatel podle písmenu b) přílohy VII, musí obsahovat specifický soubor certifikovaných atributů ve formě vhodné pro automatické zpracování:

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

ii) poskytující soubor dat jednoznačně identifikujících autentický zdroj uvedený v písmenu i) a

iii) identifikující vnitrostátní právní předpisy nebo právní předpisy Unie uvedené v písmenu i).

2. Členský stát, v němž jsou subjekty veřejného sektoru uvedené v článku 3 (45a) zřízeny, zajistí, aby subjekty veřejného sektoru vydávající elektronické potvrzení atributů měly rovnocennou úroveň spolehlivosti jako kvalifikovaní poskytovatelé služeb vytvářejících důvěru v souladu s článkem 24.

2a. Členské státy oznámí subjekty veřejného sektoru uvedené v článku 3 (45a) Komisi. Toto oznámení obsahuje zprávu a posouzení shody vydanou subjektem posuzování shody potvrzující splnění požadavků stanovených v odstavcích 1, 2 a 6 tohoto článku. Seznam subjektů veřejného sektoru uvedených v článku 3 (45a) Komise bezpečnou cestou zpřístupní veřejnosti ve formě opatřené elektronickým podpisem nebo pečetí a vhodné pro automatické zpracování.

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

4. Pokud elektronické potvrzení atributů vydané subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem splňuje normy uvedené v odstavci 5 tohoto článku, má se zato, že vyhovuje požadavkům stanoveným v odstavci 1 tohoto článku.

5. Do šesti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcího aktu o provádění evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 11, technické specifikace a referenční čísla norem pro elektronická potvrzení atributů vydaná subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem.

5a. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 11, formáty, postupy, specifikace a normy pro účely odstavce 2a.

6. Subjekty veřejného sektoru uvedené v článku 3 (45a) vydávající elektronické potvrzení atributů poskytují rozhraní s evropskými peněženkami digitální identity v souladu s článkem 6a.

Článek 45e

Vydávání elektronických potvrzení atributů evropským peněženkám digitální identity

Poskytovatelé kvalifikovaných elektronických potvrzení atributů poskytují rozhraní s evropskými peněženkami digitální identity v souladu s článkem 6a.

Článek 45f

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 údajů uchovávaných poskytovatelem elektronického potvrzování atributů.

4. Poskytovatelé služeb kvalifikovaného elektronického potvrzení atributů provedou za účelem poskytování těchto služeb funkční oddělení.

ODDÍL 10

SLUŽBY ELEKTRONICKÉ ARCHIVACE

Článek 45g

Právní účinek služby elektronické archivace

1. Elektronickým datům uchovávaným s použitím služby elektronické archivace nesmějí být upírány právní účinky a nesmějí být odmítána 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 uchovávaných s použitím kvalifikované služby elektronické archivace platí předpoklad integrity dat a jejich původu, a to po dobu uchovávání kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

3. Kvalifikovaná služba elektronické archivace v jednom členském státě se uznává jako kvalifikovaná služba elektronické archivace v jakémkoli jiném členském státě.

Článek 45ga

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 prodloužit životnost a čitelnost elektronických dat i po uplynutí doby technické platnosti a alespoň po zákonně či smluvně stanovenou dobu uchovávání, a současně zachovat jejich integritu a původ;

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

d) musí oprávněným spoléhajícím se stranám umožnit obdržet automatizovaným způsobem zprávu potvrzující, že u elektronických dat získaných z kvalifikovaného elektronického archivu platí předpoklad integrity dat od začátku doby uchovávání do doby jejich získání. Tato zpráva se poskytne spolehlivým a účinným způsobem a musí být opatřena kvalifikovaným elektronickým podpisem nebo kvalifikovanou elektronickou pečetí poskytovatele kvalifikované služby elektronické archivace;

2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro kvalifikované služby elektronické archivace. Pokud kvalifikovaná služba elektronické archivace těmto specifikacím a normám vyhovuje, 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 ÚČETNÍ KNIHY

Článek 45h

Právní účinky elektronických účetních knih

1. Elektronické účetní knize nesmějí být upírány právní účinky a 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 pečetě.

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

3. Kvalifikovaná elektronická účetní kniha v jednom členském státě se uznává jako kvalifikovaná elektronická účetní kniha v jakémkoli jiném členském státě.

Článek 45i

Požadavky na kvalifikované elektronické účetní knihy

1. Kvalifikované elektronické účetní knihy musí splňovat tyto požadavky:

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

   b) identifikují původ datových záznamů v účetní knize;

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

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

2. Pokud elektronická účetní kniha vyhovuje specifikacím a normám uvedeným v odstavci 3, předpokládá se shoda s požadavky stanovenými v odstavci 1.

3. Komise může prostřednictvím prováděcích aktů určit technické specifikace a referenční čísla norem pro vytváření a fungování kvalifikované elektronické účetní knihy. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

40) Vkládá se nový článek 48a, který zní:

„Článek 48a

Požadavky týkající se podávání zpráv

1. Členské státy zajistí shromažďování statistických údajů týkajících se fungování evropských peněženek digitální identity, jakmile budou na jejich území tyto peněženky poskytovány.

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 přijímají používání evropské digitální peněženky;

   c) souhrnnou zprávu včetně údajů o incidentech, jež zabránily použití evropské peněženky digitální identity.

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.“

41) Článek 49 se nahrazuje tímto:

„Článek 49

Přezkum

1. Do 36 měsíců od vstupu tohoto nařízení v platnost přezkoumá Komise uplatňování tohoto nařízení a podá zprávu Evropskému parlamentu a Radě. Komise zejména vyhodnotí působnost článku 6 a článku 6db a to, zda je s přihlédnutím ke zkušenostem s uplatňováním tohoto nařízení, jakož i k poptávce ze strany zákazníků a k technologickému, tržnímu a právnímu vývoji vhodné oblast působnosti tohoto nařízení nebo jeho konkrétní ustanovení upravit. V případě potřeby se ke zprávě přiloží návrh na změnu tohoto nařízení.

2. Hodnotící zpráva zahrnuje posouzení dostupnosti a použitelnosti evropských peněženek digitální identity, které spadají do oblasti působnosti tohoto nařízení, a posuzuje, zda by všichni soukromí poskytovatelé on-line služeb, kteří pro autentizaci uživatelů využívají služby elektronické identifikace třetích stran, měli být povinni akceptovat používání evropských peněženek digitální identity.

3. Vedle toho Komise každé čtyři roky od předložení zprávy uvedené v prvním pododstavci předloží Evropskému parlamentu a Radě zprávu o pokroku v dosahování cílů tohoto nařízení.“

42) Článek 51 se nahrazuje tímto:

„Článek 51

Přechodná opatření

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 až do 36 měsíců po vstupu tohoto nařízení v platnost.

2. Kvalifikovaná osvědčení vydaná fyzickým osobám podle směrnice 1999/93/ES se považují za kvalifikované certifikáty pro elektronické podpisy podle tohoto nařízení až do 24 měsíců po vstupu tohoto nařízení v platnost.“

2a. Správa prostředků pro vytváření kvalifikovaných 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 prostředků pro vytváření kvalifikovaných elektronických podpisů a pečetí na dálku v souladu s články 29a a 39a je i nadále akceptována, aniž je nutné do 24 měsíců od vstupu tohoto nařízení v platnost získat kvalifikovaný status pro poskytování těchto služeb souvisejících se správou.

2b. Kvalifikovaní poskytovatelé služby vytvářející důvěru, kteří kvalifikovaný status podle tohoto nařízení získají do [datum vstupu pozměňujícího nařízení v platnost], s použitím metod pro ověřování totožnosti pro účely vydávání kvalifikovaných certifikátů v souladu s čl. 24 odst. 1, předloží orgánu dohledu co nejdříve, avšak nejpozději 30 měsíců od vstupu v pozměňující nařízení v platnost, zprávu o posouzení shody dokládající soulad s čl. 24 odst. 1. Do předložení této zprávy o posouzení shody a dokončení posouzení orgánem dohledu může poskytovatel služby vytvářející důvěru nadále spoléhat na použití metod pro ověřování totožnosti stanovených v čl. 24 odst. 1 nařízení (EU) č. 910/2014.

43) Příloha I se mění v souladu s přílohou I tohoto nařízení.

44) Příloha II se nahrazuje zněním uvedeným v příloze II tohoto nařízení.

45) Příloha III se mění v souladu s přílohou III tohoto nařízení.

46) Příloha IV se mění v souladu s přílohou IV tohoto nařízení.

47) Doplňuje se nová příloha V uvedená v příloze V tohoto nařízení.

48) Doplňuje se nová příloha VI.

Článek 52

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

Za Evropský parlament Za Radu

předsedkyně předseda/předsedkyně

PŘÍLOHA I

V příloze I 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

POŽADAVKY NA KVALIFIKOVANÉ PROSTŘEDKY PRO VYTVÁŘENÍ ELEKTRONICKÝCH PODPISŮ

1. Kvalifikované prostředky pro vytváření elektronických podpisů vhodnými technickými prostředky a postupy přinejmenším zajistí, aby:

(a) byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů, která byla použita při vytváření elektronického podpisu;

(b) data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu se mohla prakticky vyskytnout pouze jednou;

(c) bylo přiměřeně zajištěno, že data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu nelze odvodit a že elektronický podpis je v současnosti dostupnými technickými prostředky spolehlivě chráněn proti padělání;

(d) měla oprávněná podepisující osoba možnost data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu spolehlivě chránit před jejich zneužitím třetí osobou.

2. Kvalifikované prostředky pro vytváření elektronických podpisů nesmějí měnit podepisovaná data ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním.

PŘÍLOHA III

V příloze III 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

V příloze IV se písmeno j) 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

POŽADAVKY NA KVALIFIKOVANÉ ELEKTRONICKÉ POTVRZENÍ ATRIBUTŮ

Kvalifikované elektronické potvrzení atributů obsahuje:

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

(f) 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:

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

– v případě fyzické osoby: jméno a příjmení osoby;

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

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

(i) označení začátku a konce doby platnosti potvrzení;

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

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

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

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

PŘÍLOHA VI

MINIMÁLNÍ SEZNAM ATRIBUTŮ

V návaznosti na článek 45d členské státy zajistí, aby byla přijata opatření, která kvalifikovaným poskytovatelům elektronických potvrzení atributů umožní na žádost uživatele elektronickými prostředky porovnáním s příslušným autentickým zdrojem na vnitrostátní úrovni nebo prostřednictvím určených zprostředkovatelů uznaných na vnitrostátní úrovni v souladu s vnitrostátními právními předpisy nebo právními předpisy Unie, pokud se tyto atributy spoléhají na autentické zdroje v rámci veřejného sektoru, ověřit autenticitu následujících atributů:

1. adresa;
2. věk;
3. pohlaví;
4. rodinný stav;
5. složení rodiny;
6. státní příslušnost nebo občanství;
7. dosažená úroveň vzdělání, tituly a osvědčení;
8. odborná kvalifikace, tituly a osvědčení;
9. veřejná povolení a osvědčení;
10. finanční údaje a údaje o společnosti.

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 přinejmenším 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 systému 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 kvalifikovaného potvrzení nebo údaj o umístění služeb, které lze využít ke zjištění platnosti potvrzení.