21.2.2024 A9-0038/ 001-001

POZMĚŇOVACÍ NÁVRHY 001-001
které předložil Výbor pro průmysl, výzkum a energetiku

Zpráva
Romana Jerković **A9-0038/2023**
Rámec pro evropskou digitální identitu

Návrh nařízení (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Pozměňovací návrh 1

POZMĚŇOVACÍ NÁVRHY EVROPSKÉHO PARLAMENTU*

k návrhu Komise

2021/0136 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

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

* Pozměňovací návrhy: nový text či text nahrazující původní znění je označen tučně a kurzivou, vypuštění textu je označeno symbolem ▌.

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

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

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

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

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Sdělení Komise ze dne 19. února 2020 nazvané „Formování digitální budoucnosti Evropy“[2] 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.

(2) Evropská rada ve svých závěrech ze zasedání konaného ve dnech 1. až 2. října 2020[3] vyzvala Komisi, aby navrhla vytvořit celounijní rámec bezpečné veřejné elektronické identifikace 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.

(2a) Politický program Digitální dekáda 2030 stanoví digitální cíl rámce Unie, který by měl vést k tomu, aby byla do roku 2030 v širokém měřítku zavedena důvěryhodná, dobrovolná, digitální identita kontrolovaná uživatelem, která bude uznávána v celé Unii a která každému uživateli umožní mít svá data a přítomnost na internetu pod kontrolou.

▌

(3a) Prohlášení Komise ze dne 26. ledna 2022 nazvané „Evropské prohlášení o digitálních právech a zásadách digitální dekády“ zdůrazňuje právo každého občana na přístup k digitálním technologiím, produktům a službám, které jsou bezpečné a zabezpečené a chrání soukromí již od návrhu. To znamená také zajištění

---

1 Úř. věst. C, , s .
2 COM(2020)0067.
3 https://www.consilium.europa.eu/cs/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

toho, aby všem lidem žijícím v Unii byla nabídnuta dostupná, bezpečná a důvěryhodná digitální identita, která umožňuje přístup k široké škále on-line i off-line služeb chráněných před veškerými kybernetickými hrozbami, včetně krádeže identity nebo manipulace s ní. V prohlášení Komise se rovněž uvádí, že každý má právo na ochranu svých osobních údajů na internetu. Toto právo zahrnuje kontrolu toho, jak jsou údaje využívány a s kým jsou sdíleny.

(3b) Občané Unie by měli mít právo na digitální identitu, která je pod jejich výhradní kontrolou a která jim umožňuje vykonávat jejich občanská práva v digitálním prostředí a podílet se na digitální ekonomice. Evropská digitální identita by měla být právně uznávána v celé Unii.

(4) Harmonizovanější přístup k digitální identifikaci by měl snížit rizika a náklady současné roztříštěnosti, jejíž příčinou je používání odlišných vnitrostátních řešení ***nebo skutečnost, že v některých členských státech tato řešení zcela chybí,*** a posílí jednotný trh tím, že umožní občanům, dalším rezidentům ve smyslu vnitrostátních právních předpisů ***a právním subjektům*** identifikovat se ***a autentizovat se*** v on-line ***a offline*** prostředí v celé Unii ***bezpečným, důvěryhodným, uživatelsky vstřícným,*** pohodlným***, dostupným a harmonizovaným*** způsobem. Každý by měl mít bezpečný přístup k veřejným a soukromým službám založeným na zdokonaleném ekosystému služeb vytvářejících důvěru a na ověřených dokladech totožnosti a ***elektronických*** potvrzeních atributů, jako je ***akademická kvalifikace,*** vysokoškolský titul ***nebo jiné vzdělání či profesní kvalifikace, které jsou*** právně uznávané a přijímané všude v Unii, ***nebo licence či pověření k zastupování společnosti, přičemž by měl být vytvořen jednotný soubor pravidel pro poskytovatele elektronických potvrzení, který zajistí rovné podmínky***. Cílem rámce pro evropskou digitální identitu je dosáhnout přechodu od spoléhání se pouze na vnitrostátní řešení v oblasti digitální identity k poskytování elektronických potvrzení atributů platných ***a právně uznávaných v celé Unii***. Poskytovatelé elektronických potvrzení atributů by měli těžit z jasného a jednotného souboru pravidel a orgány veřejné správy by měly být schopny spolehnout se na ***vysoce zabezpečené*** elektronické dokumenty***, které jsou přijímané v celé Unii***. ***Pokud jde o elektronickou identifikaci pro veřejné služby s velmi vysokými bezpečnostními požadavky na identifikaci, měly by mít členské státy možnost stanovit, že notáři a další odborníci, jimž byly svěřeny zvláštní pravomoci ve veřejném zájmu, mohou***

uplatňovat další kontroly totožnosti na dálku stanovené v souladu se zásadou proporcionality prostřednictvím vnitrostátních právních předpisů.

(5) S cílem podpořit konkurenceschopnost evropských podniků by měli mít poskytovatelé on-line ***i off-line*** služeb možnost využívat řešení v oblasti digitální identity uznávaná v celé Unii, bez ohledu na to, v kterém členském státě byla vydána, a čerpat tak výhody vyplývající 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. ***Harmonizovaný rámec digitální identity má potenciál vytvářet ekonomickou hodnotu poskytováním snadnějšího přístupu ke zboží a službám, výrazným snížením provozních nákladů spojených s postupy identifikace a autentizace, například při přijímání nových zákazníků, omezením škod souvisejících s kyberkriminalitou, jako jsou krádeže identity, krádeže údajů a podvody on-line, a podporou digitální transformace mikropodniků a malých a středních podniků v Unii.***

(5a) Plně harmonizovaný rámec digitální identity by přispěl k vytvoření digitálně integrovanější Unie, odstranil by digitální překážky mezi členskými státy a umožnil občanům Unie a rezidentům Unie využívat výhod digitalizace a zároveň by zvýšil transparentnost a ochranu jejich práv.

(5b) S cílem podpořit digitalizaci služeb veřejného sektoru členských států a zajistit rozsáhlé využívání evropského rámce digitální identity a evropské peněženky digitální identity by toto nařízení mělo podporovat používání zásady „jen jednou“, aby se snížila administrativní zátěž, podpořila přeshraniční mobilita občanů a podniků a podpořil rozvoj interoperabilních služeb elektronické veřejné správy v celé Unii. Přeshraniční uplatňování zásady „pouze jednou“ by mělo znamenat, že by občané a podniky neměli mít povinnost poskytovat stejné údaje orgánům veřejné moci více než jednou a že by mělo být rovněž možné používat tyto údaje pouze na žádost uživatele pro účely splnění přeshraničních online postupů. Provádění tohoto nařízení a zásady „pouze jednou“ by mělo být v souladu se všemi platnými pravidly pro ochranu údajů, včetně zásady minimalizace údajů, přesnosti, omezení uchovávání, integrity a důvěrnosti, nezbytnosti, přiměřenosti a omezení účelu. Zásada „pouze jednou“ by se měla uplatňovat s výslovným souhlasem uživatele.

(6) ***Fyzické a právnické osoby, které vlastní osobní identifikační údaje, by měly být považovány za subjekty digitální identity.*** Zpracovávání osobních údajů při provádění tohoto nařízení se řídí nařízením (EU) 2016/679[1], ***nařízením (EU) 2018/1725[2] a směrnicí Evropského parlamentu a Rady 2002/58/ES[3].*** 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. ***Toto nařízení dále upřesňuje uplatňování zásad účelového omezení, minimalizace údajů a záměrné a standardní ochrany údajů pro konkrétní případy použití, aniž by bylo dotčeno nařízení (EU) č. 2016/679.***

(6a) Evropské peněženky digitální identity by měly mít zabudovanou funkci přehledu řízení ochrany soukromí, aby byla zajištěna vyšší míra transparentnosti a aby měli uživatelé větší kontrolu nad svými údaji. Tato funkce by měla poskytovat snadný a uživatelsky přívětivý přehled o všech spoléhajících se stranách, s nimiž uživatel sdílel údaje, včetně atributů, a o druhu údajů sdílených s každou spoléhající se stranou. Měla by uživateli umožnit sledovat všechny transakce provedené prostřednictvím evropské peněženky digitální identity, a to alespoň pokud jde o následující údaje: čas a datum transakce, identifikace protistrany, požadované údaje a sdílené údaje. Tyto informace by měly být uloženy, i když transakce nebyla uzavřena. Nemělo by být možné vyvrátit pravost informací obsažených v historii transakce. Taková funkce by měla být standardně nastavena jako aktivní. Uživatelé by měli mít možnost snadno požádat spoléhající se stranu o okamžité vymazání osobních údajů podle článku 17 nařízení (EU) 2016/679 a snadno podat příslušnému vnitrostátnímu orgánu, v němž je spoléhající se strana usazena,

---

1 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.

2 ***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).***

3 ***Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Úř. věst. L 201, 31.7.2002, s. 37).***

oznámení v případě, že obdrží protiprávní nebo nevhodnou žádost o údaje, bez nutnosti opustit evropskou peněženku digitální identity.

(6b) Důkaz s nulovou znalostí umožňuje na základě kryptografických algoritmů ověřit tvrzení, aniž by byla odhalena data, která ho dokazují. Evropská peněženka digitální identity by měla umožnit ověření tvrzení odvozených z identifikace osobních údajů nebo potvrzení atributů bez nutnosti poskytnout zdrojové údaje, aby bylo zachováno soukromí uživatele evropské peněženky digitální identity.

(7) Je nezbytné stanovit harmonizované podmínky pro vytvoření rámce pro evropské peněženky digitální identity vydávané ***přímo členským státem, na základě pověření členského státu nebo uznané členským státem, který by měl umožnit všem občanům Unie a rezidentům Unie*** ve smyslu vnitrostátních právních předpisů ***bezpečně požadovat, přijímat, uchovávat, kombinovat a selektivně sdílet údaje týkající se*** jejich identity ***a požadovat výmaz svých osobních údajů uživatelsky přívětivým způsobem a*** pod výhradní kontrolou uživatele. ***Všechny údaje by měly být standardně uloženy na zařízení uživatele, pokud si uživatel výslovně nezvolí jinou možnost. Toto nařízení by mělo odrážet sdílené hodnoty a prosazovat základní práva, silné etické aspekty, právní záruky a odpovědnost, a chránit tak demokratickou společnost a občany.*** Technologie používané k dosažení těchto cílů by měly být vyvinuty s cílem dosáhnout nejvyšší úrovně ***soukromí a*** bezpečnosti, pohodlí uživatele***, dostupnosti*** a široké použitelnosti ***a bezproblémové interoperability***. Členské státy by měly všem svým státním příslušníkům a rezidentům zajistit rovný přístup k digitální identifikaci ***a její dobrovolné užívání***. ***Členské státy by neměly přímo ani nepřímo omezovat přístup k veřejným službám či službám financovaným z veřejných prostředků fyzickým ani právním osobám, které se rozhodnou evropskou peněženku digitální identity nevyužívat, a pro tyto jednotlivce by měly vytvářet a zajišťovat bezplatnou dostupnost alternativních řešení. Soukromé spoléhající se strany, které evropskou peněženku digitální identity využívají k poskytování služeb, by neměly tyto služby odpírat spotřebitelům, kteří evropské peněženky digitální identity pro přístup ke svým službám nepoužívají, ani pro ně vytvářet nevýhodné podmínky.***

(7a) Pokud evropskou peněženku digitální identity vydává přímo členský stát, je za vydání a správu evropské peněženky digitální identity přímo odpovědný dotčený příslušný orgán, přičemž využívá vlastních zdrojů. Pokud je evropská peněženka

digitální identity vydávána na základě pověření členského státu, dotčený příslušný orgán pověří konkrétní organizaci, aby vydala a spravovala evropskou peněženku digitální identity jejím jménem na základě zadávacího řízení založeného na transparentním, otevřeném a spravedlivém výběrovém řízení, jehož se mohou zúčastnit všechny zúčastněné strany, přičemž nejlepší uchazeč je vybrán na základě konkrétních objektivních kritérií a procesu hodnocení. Pokud je evropská peněženka digitální identity vydávána a spravována nezávisle, ale je uznávána členským státem, dotčený příslušný orgán vybere konkrétní organizaci, která již vyvinula evropskou peněženku digitální identity, která je v souladu s tímto nařízením. Není nutné, aby evropskou peněženku digitální identity vydával a spravoval tentýž subjekt.

(8) V zájmu zajištění souladu s právem Unie nebo vnitrostátními právními předpisy, jež jsou v souladu s právem Unie, by ***spoléhající se strany měly*** svůj záměr využívat evropské peněženky digitální identity ***zaregistrovat v členském státě, v němž jsou usazeny***. To členským státům umožní chránit uživatele před podvody a zabránit neoprávněnému používání údajů o totožnosti a elektronických potvrzení atributů a také zajistit, aby zpracování citlivých údajů, jako jsou údaje o zdravotním stavu, mohlo být ověřeno spoléhajícími se stranami v souladu s ***právními předpisy*** Unie nebo vnitrostátními právními předpisy. ***Postupy registrace a schvalování by měly být nákladově efektivní a přiměřené riziku. Registrace by měla zahrnovat údaje, které má spoléhající se strana v úmyslu požadovat, zamýšlené použití a důvody potřeby těchto údajů, a to pro každou jednotlivou kategorii služeb poskytovaných spoléhající se stranou. Spoléhající se strany by měly svou žádost odůvodnit v souladu se zásadami minimalizace údajů.***

(9) Všechny evropské peněženky digitální identity by měly uživatelům umožnit přeshraniční elektronickou identifikaci a autentizaci on-line a offline pro přístup k široké škále veřejných a soukromých služeb. Aniž jsou dotčeny výsady členských států s ohledem na identifikaci jejich státních příslušníků a rezidentů, mohou evropské peněženky digitální identity rovněž sloužit institucionálním potřebám orgánů veřejné správy, mezinárodních organizací a orgánů, institucí a jiných subjektů Unie. 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, bude důležité použití offline. Evropské

peněženky digitální identity, spoléhající se na „vysokou“ úroveň záruky ***při prokazování totožnosti***, by měly využít potenciál, který nabízejí řešení odolná proti neoprávněným zásahům, jako jsou zabezpečené prvky, aby byly v souladu s bezpečnostními požadavky podle tohoto nařízení. ***Při zapojování do evropských peněženek digitální identity by uživatelé měli bezplatně a standardně získat kvalifikovaný elektronický podpis bez nutnosti absolvovat další administrativní nebo technické postupy.*** ▌ V zájmu zjednodušení a snížení nákladů pro osoby a podniky v celé ***Unii,*** mimo jiné umožněním pravomocí k zastupování a elektronických mandátů, by členské státy měly vydávat evropské peněženky digitální identity založené na společných normách ***a technických specifikacích*** s cílem zajistit bezproblémovou interoperabilitu ***a přiměřené zvýšení úrovně bezpečnosti IT a posílit odolnost proti kybernetickým útokům, a tím výrazně snížit potenciální rizika probíhající digitalizace pro občany a podniky***. Pouze příslušné orgány členských států mohou při zjišťování totožnosti osoby poskytnout vysoký stupeň spolehlivosti, a tedy poskytnout ujištění, že osoba, která uvádí nebo uplatňuje určitou totožnost, je skutečně osobou, kterou tvrdí, že je. ***Vydávání evropských peněženek*** digitální identity se proto musí spoléhat na právní identitu občanů, ostatních rezidentů nebo právnických osob. ***Spoléhání se na právní identitu by uživatelům evropské peněženky digitální identity nemělo bránit v přístupu ke službám prostřednictvím pseudonymů, pokud nebyl pro účely autentizace stanoven právní požadavek uvádět právní identitu.*** Důvěru v evropské peněženky digitální identity by posílila skutečnost, že vydávající strany ***a správci*** jsou povinni zavést vhodná technická a organizační opatření k zajištění ***nejvyšší*** úrovně bezpečnosti odpovídající rizikům, která představují pro práva a svobody fyzických osob, v souladu s nařízením (EU) 2016/679.

(9a) Evropské peněženky digitální identity by měly zahrnovat funkci pro vytváření svobodně zvolených pseudonymů spravovaných uživateli jako formu autentizace pro přístup k poskytovaným on-line službám, včetně služeb poskytovaných velmi velkými online platformami ve smyslu nařízení Evropského parlamentu a Rady (EU) 2022/2065[1].

---

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

(9b) Členské státy by měly vypracovat harmonizované přístupy, které osobám s omezenou způsobilostí k právům a právním úkonům, jako jsou nezletilí a osoby bez právní způsobilosti, umožní využívat evropské peněženky digitální identity, služby vytvářející důvěru a produkty pro koncové uživatele.

(9c) Fyzické a právnické osoby by měly mít možnost udělit souhlas s tím, aby určité úkony prováděly jejich jménem evropské peněženky digitální identity třetích stran, například prostřednictvím plné moci nebo přenesení pravomoci k provedení konkrétních transakcí uděleného konkrétním zaměstnancům nebo subdodavatelům společnosti nebo rodičům v případě nezletilých dětí.

(10) V zájmu dosažení vysoké úrovně bezpečnosti a důvěryhodnosti stanoví toto nařízení požadavky na evropské peněženky digitální identity. Soulad evropských peněženek digitální identity s těmito požadavky by měl být certifikován akreditovanými subjekty veřejného nebo soukromého sektoru určenými členskými státy. Využívání systému certifikace založeného na dostupnosti norem společně dohodnutých s členskými státy by mělo zajistit vysokou úroveň důvěryhodnosti a interoperability. Certifikace by se měla opírat zejména o příslušné evropské systémy certifikace kybernetické bezpečnosti zřízené podle nařízení (EU) 2019/881[6]. Touto certifikací by neměla být dotčena certifikace týkající se zpracování osobních údajů podle nařízení (ES) 2016/679.

(10a) Klíčovými prvky pro vytvoření sociální důvěry v tento rámec jsou transparentnost evropských peněženek digitální identity a odpovědnost jejich vydavatelů. Všichni vydavatelé evropských peněženek digitální identity by měli zveřejnit zdrojové kódy pro účely jejich kontroly, zejména pokud jde o soukromí a bezpečnost. Vydavatelé a správci evropských peněženek digitální identity by měli podléhat podobným kontrolám a závazkům, jaké mají kvalifikovaní poskytovatelé služeb vytvářejících důvěru.

(11) Evropské peněženky digitální identity by měly zajišťovat nejvyšší úroveň bezpečnosti osobních údajů používaných k ***identifikaci a*** autentizaci bez ohledu na to, zda jsou

---

6 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.

tyto údaje uchovávány lokálně***, v decentralizované účetní knize*** nebo v rámci řešení založených na cloudu, a to se zohledněním různých úrovní rizika. ***Podmínkou pro používání evropské peněženky digitální identity by nemělo být*** používání biometrických údajů ***k identifikaci a*** autentizaci, ***a to bez ohledu na požadavek silného ověření uživatele***. ***Biometrické údaje používané pro účely autentizace fyzické osoby v souvislosti s tímto nařízením by bez výslovného souhlasu uživatele neměly být uchovávány v cloudu.*** Jedním ze způsobů identifikace poskytujících vysokou úroveň spolehlivosti je používat ▌ biometrické údaje, ▌ pokud se používají v kombinaci ***se znalostním faktorem autentizace.*** Jelikož biometrické údaje představují jedinečné vlastnosti osoby, ***nemělo by být používání*** biometrických údajů ***povinné***. ***Použití biometrických údajů by rovněž mělo být omezeno na konkrétní scénáře podle článku 9 nařízení (EU) 2016/679 a*** vyžaduje organizační a bezpečnostní opatření úměrná riziku, které takové zpracování může představovat pro práva a svobody fyzických osob, a v souladu s nařízením 2016/679. ***Ukládání informací z evropské peněženky digitální identity v cloudu by mělo být volitelnou funkcí, která bude aktivní pouze po výslovném souhlasu uživatele. Pokud jsou evropské peněženky digitální identity vydávány na osobním elektronickém zařízení uživatele, měl by být jejich kryptografický materiál, je-li to technicky možné, uložen v zabezpečených prvcích evropské peněženky digitální identity.***

(11a) Evropské peněženky digitální identity by měly být bezpečné již od fáze návrhu. Měly by zavést pokročilé bezpečnostní prvky na ochranu před krádeží identity, krádeží dat, odepřením služby a jakoukoli jinou kybernetickou hrozbou. Jejich součástí by měly být nejmodernější metody šifrování a ukládání, které jsou přístupné pouze uživateli a dekódovatelné pouze jím, a zavedení šifrované komunikace mezi koncovými body s jinými evropskými peněženkami digitální identity a spoléhajícími se stranami. Kromě toho by evropské peněženky digitální identity měly vyžadovat bezpečné výslovné a aktivní potvrzení použití pro operace.

(11b) Používání evropských peněženek digitální identity a ukončení jejich používání je právem a volbou uživatelů. Členské státy by měly vytvořit jednoduchý, uživatelsky vstřícný, rychlý a bezpečný postup, který uživatelům umožní požádat o okamžité zrušení platnosti evropských peněženek digitální identity. V situacích, kdy uživatelé zařízení vlastní, by tato funkce měla být koncipována jako integrovaný prvek

evropské peněženky digitální identity. Je třeba zavést uživatelsky přívětivý a rychlý mechanismus na dálku pro případy, kdy uživatelé zařízení nemají k dispozici, jako je krádež nebo ztráta. V případě úmrtí uživatele nebo ukončení činnosti právnické osoby by měl být vytvořen mechanismus, který orgánu odpovědnému za vypořádání dědictví fyzické osoby nebo majetku právnické osoby umožní požádat o okamžité ukončení činnosti evropské peněženky digitální identity.

(11c) V zájmu podpory zavádění evropských peněženek digitální identity a širšího využívání digitálních identit by členské státy měly nejen ukázat přínosy příslušných služeb, ale také ve spolupráci se soukromým sektorem, výzkumnými pracovníky a akademickou obcí vypracovat programy odborné přípravy zaměřené na posílení digitálních dovedností svých občanů a rezidentů, zejména pro zranitelné skupiny, jako jsou osoby se zdravotním postižením, starší osoby a osoby bez digitálních dovedností.

(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 pískoviště pro testování inovativních řešení v kontrolovaném***, časově omezeném*** 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 podpořit začlenění evropských malých a středních podniků, začínajících podniků a samostatných inovátorů a výzkumných pracovníků***, ale i příslušných zúčastněných stran z odvětví, a zároveň zlepšit dodržování předpisů a zabránit tomu, aby byla na trh uváděna řešení, která porušují právní předpisy Unie v oblasti ochrany údajů a bezpečnosti IT***.

(13) Nařízení ***Evropského parlamentu a Rady*** (EU) č. 2019/1157[7] posiluje zabezpečení průkazů totožnosti prostřednictvím posílených bezpečnostních prvků do srpna 2021. Členské státy by měly zvážit proveditelnost oznamování v rámci systémů elektronické

[7] 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).

identifikace s cílem rozšířit přeshraniční dostupnost prostředků pro elektronickou identifikaci.

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

(15) Zjednodušení stávajících postupů oznamování a vzájemného hodnocení zabrání různorodým přístupům 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 provedené akreditovanými subjekty posuzování shody nebo dobrovolné systémy certifikace bezpečnosti informačních a komunikačních technologií, jako jsou systémy certifikace, které mají být zřízeny na úrovni Unie podle nařízení (EU) 2019/881, na podporu tvrzení o sladění systémů nebo jejich částí s požadavky nařízení o interoperabilitě a bezpečnosti oznámených systémů elektronické identifikace.

(17) Poskytovatelé služeb používají identifikační údaje poskytnuté souborem osobních identifikačních údajů dostupných ze systémů elektronické identifikace podle nařízení (EU) č. 910/2014, aby k uživateli z jiného členského státu přiřadili jeho právní identitu. Navzdory použití souboru údajů eIDAS však zajištění přesné shody v mnoha případech vyžaduje dodatečné informace o uživateli a zvláštní postupy jednoznačné identifikace na vnitrostátní úrovni. ***V zájmu zajištění vysoké úrovně důvěryhodnosti a bezpečnosti osobních údajů fyzických osob by měla být zvážena různá technická řešení, včetně použití nebo kombinace různých kryptografických technik, jako jsou kryptograficky ověřitelné identifikátory.*** S cílem dále podporovat použitelnost prostředků pro elektronickou identifikaci ***a uplatňování zásady „pouze jednou“*** by toto nařízení mělo vyžadovat, aby členské státy přijaly zvláštní opatření k zajištění

správné shody totožnosti v procesu elektronické identifikace ***výhradně pro přeshraniční přístup k veřejným službám, který vyžaduje identifikaci uživatele ze zákona***. ***Tento požadavek by zejména neměl být chápán jako výzva k vytvoření centralizovaného registru totožnosti v Unii pro fyzické osoby, spoléhat by se mělo na decentralizované vnitrostátní rejstříky.*** Použití ***osobních identifikačních údajů nebo kombinace osobních identifikačních údajů, včetně použití jedinečných a trvalých identifikátorů vydaných členskými státy nebo generovaných evropskou peněženkou digitální identity, je důležité pro zajištění toho, aby mohla být ověřena totožnost uživatele. Vnitrostátními právními předpisy by mělo být možné vyžadovat používání jedinečných a trvalých identifikátorů, které jsou specifické pro konkrétní odvětví nebo spoléhající se strany. Evropské peněženky digitální identity by měly být schopny tyto identifikátory uchovávat a zveřejňovat, pokud o to uživatel požádá***. Za stejným účelem by toto nařízení mělo rozšířit povinný minimální soubor údajů a vyžadovat používání jedinečného a trvalého elektronického identifikátoru ***právnických osob*** v souladu s právem Unie ▌.

(17a) Při přeshraničním přístupu k veřejným a soukromým službám by mělo být možné ověřit a identifikovat uživatele evropské peněženky digitální identity. Přijímající členské státy by měly mít možnost jednoznačně identifikovat uživatele na jejich žádost v případech, kdy je identifikace uživatele vyžadována právními předpisy, a přistoupit k porovnání totožnosti. V zájmu zajištění vysoké úrovně důvěryhodnosti a bezpečnosti osobních údajů by měla být zvážena různá technická řešení, včetně použití nebo kombinace různých nejmodernějších kryptografických technik a technologií, jako jsou kryptograficky ověřitelné identifikátory, jedinečné digitální pseudonymy vytvořené uživatelem, decentralizovaná identita a identifikátory specifické pro danou doménu.

(18) V souladu se směrnicí ***Evropského parlamentu a Rady*** (EU) 2019/882[8] 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.

[8] 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).

(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 právem Unie nebo vnitrostátním právem. Neměly by jím být dotčeny ani vnitrostátní požadavky na formu týkající se veřejných rejstříků, zejména obchodních rejstříků a katastrů nemovitostí.

(20) Poskytování a využívání služeb vytvářejících důvěru nabývá pro mezinárodní obchod a spolupráci na významu. Mezinárodní partneři EU vytvářejí důvěryhodné rámce inspirované nařízením (EU) č. 910/2014. S cílem usnadnit uznávání těchto služeb a jejich poskytovatelů proto mohou prováděcí právní předpisy stanovit podmínky, za nichž by důvěryhodné rámce třetích zemí mohly být považovány za rovnocenné s důvěryhodným rámcem pro kvalifikované služby vytvářející důvěru a 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.

(21) ***Vydavatelé evropských peněženek digitální identity potřebují přístup ke specifickým hardwarovým a softwarovým prvkům chytrých telefonů, jako jsou části operačního systému, zabezpečený hardware (zabezpečený prvek, SIM atd.), NFC, Bluetooth, Wi-Fi Aware a biometrické senzory. Tyto prvky jsou pod kontrolou operačních systémů a výrobců zařízení. Toto nařízení by proto mělo vycházet z aktů Unie zajišťujících spravedlivé trhy otevřené hospodářské soutěži v digitálním odvětví.*** Zejména vychází z ***čl. 6 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2022/1925[1]***, ***který vyžaduje, aby poskytovatelé hlavních služeb platforem, kteří byli určeni jako*** strážci, ***bezplatně umožnili podnikatelským uživatelům a alternativním poskytovatelům služeb poskytovaných společně s hlavními službami platforem nebo na jejich podporu účinnou interoperabilitu se stejným operačním systémem, hardwarem nebo softwarovými prvky a přístup k nim pro účely interoperability, bez ohledu na to, zda jsou tyto prvky součástí operačního systému nebo jsou dostupné tomuto strážci nebo jím používané při poskytování těchto služeb.***

---

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

(21a) Cílem tohoto nařízení je usnadnit vytváření evropských peněženek digitální identity, jejich výběr a možnost přechodu mezi nimi. Aby se předešlo zakonzervování stávajícího stavu, měli by vydavatelé evropských peněženek digitální identity na žádost uživatele peněženky zajistit účinnou přenositelnost údajů, včetně nepřetržitého přístupu ke službám v reálném čase, a neměli by mít možnost používat smluvní, ekonomické nebo technické překážky, které by bránily účinnému přechodu mezi různými evropskými peněženkami digitální identity nebo od něj odrazovaly.

(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 o bezpečnosti sítí a informací 2) jsou služby vytvářející důvěru povinny přijmout vhodná technická a organizační opatření podle směrnice XXXX/XXXX (směrnice o bezpečnosti sítí a informací 2), jako jsou opatření zaměřená na selhání systémů, lidské chyby, 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 o bezpečnosti sítí a informací 2). S ohledem na hlášení incidentů by měli poskytovatelé služeb vytvářejících důvěru oznamovat jakékoli incidenty, které mají na poskytování jejich služeb významný dopad, včetně těch, které byly způsobeny krádeží nebo ztrátou zařízení či 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 [bezpečnost sítí a informací 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 o bezpečnosti sítí a informací 2) měly nadále uplatňovat zavedené vnitrostátní postupy nebo pokyny týkající se provádění požadavků na bezpečnost a podávání zpráv 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) Zajištění účinné spolupráce mezi orgány v oblasti bezpečnosti sítí a informací a eIDAS by se měla věnovat náležitá pozornost. V případech, kdy se orgán dohledu podle tohoto nařízení liší od příslušných orgánů určených podle směrnice XXXX/XXXX [bezpečnost sítí a informací 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 [bezpečnost sítí a informací 2]. Orgány dohledu by podle tohoto nařízení zejména měly být oprávněny požádat příslušný orgán podle směrnice XXXXX/XXXX [bezpečnost sítí a informací 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 bezpečnosti sítí a informací 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 budou moci nabízet nové panevropské služby elektronického doporučeného doručování a zajistit, aby identifikace příjemců byla zajištěna s vyšší úrovní spolehlivosti než identifikace odesílatele.

I

(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 ve 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 své údaje o sociálním zabezpečení nebo budoucí digitální cestovní doklady v přeshraničním kontextu.

(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 a měl by být odpovědný za zrušení tohoto potvrzení v případě padělání, krádeže totožnosti nebo jakéhokoliv vydání na základě

zneužívající žádosti. Spoléhající se strany by měly používat elektronická potvrzení atributů jako rovnocenná potvrzením v tištěné podobě. ***Spoléhající se strany by ovšem měly i nadále akceptovat zákonně vydaná potvrzení atributů v listinné podobě jako alternativu k elektronickému potvrzení atributů.*** Elektronickému potvrzení atributů by ▌ neměly být upírány právní účinky ***pouze*** 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. ***Komise a členské státy by měly zapojit profesní organizace do vymezení atributů, které se jich týkají.***

(28) Široká dostupnost a použitelnost evropských peněženek digitální identity vyžaduje jejich přijetí ***soukromými osobami i*** soukromými poskytovateli služeb ***a jejich důvěru v tyto peněženky***. Soukromé spoléhající se strany poskytující služby ***například*** v oblasti dopravy, energetiky, bankovnictví a finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, ▌ telekomunikací ***nebo vzdělávání*** by měly akceptovat používání evropských peněženek digitální identity k poskytování služeb, u nichž ***právní předpisy Unie nebo*** vnitrostátní právní předpisy ▌ vyžadují silnou autentizaci uživatele k on-line identifikaci. ***Informace požadované od uživatele prostřednictvím evropské peněženky digitální identity by měly být nezbytné a přiměřené pro zamýšlené použití spoléhající se stranou a měly by se řídit zásadou minimalizace údajů a zajistit transparentnost ohledně toho, jaké údaje jsou sdíleny a za jakým účelem.*** V případech, kdy velmi velké on-line platformy ve smyslu článku 25.1 nařízení ***(EU) 2022/2065*** vyžadují, aby se uživatelé autentizovali pro přístup k on-line službám, měly by být tyto platformy povinny přijmout na dobrovolnou žádost uživatele evropskou peněženku digitální identity. Uživatelé by neměli mít povinnost používat evropskou peněženku digitální identity k přístupu k soukromým službám ***a neměli by být omezováni ani znevýhodňováni z důvodu, že peněženku nepoužívají,*** ale pokud si to přejí, měly by ***velmi velké*** on-line platformy za tímto účelem evropskou peněženku digitální identity

přijmout, přičemž by měla být dodržena zásada minimalizace údajů ***a právo uživatelů na použití svobodně zvoleného pseudonymu.*** Vzhledem k významu velmi velkých on-line platforem a k jejich dosahu, vyjádřenému zejména počtem příjemců služby a hospodářských transakcí, je nezbytné zvýšit ochranu uživatelů před podvody a zajistit vysokou úroveň 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“). Kodexy chování by měly usnadnit široké přijímání prostředků pro elektronickou identifikaci, včetně evropských peněženek digitální identity, těmi poskytovateli služeb, kteří nejsou kvalifikováni jako velmi velké platformy a kteří pro autentizaci uživatelů využívají služby elektronické identifikace třetích stran. Měly by být vypracovány do dvanácti měsíců od přijetí tohoto nařízení. ▌

(29) Evropská peněženka digitální identity by měla technicky umožnit výběrové sdělování atributů spoléhajícím se stranám ***bezpečným a uživatelsky vstřícným způsobem, což by měl být jeden z jejích klíčových rysů a přínosů***. ***Měla by rovněž zajistit, aby nebyly sdělovány žádné atributy stranám, které nejsou zaregistrovány jako strany oprávněné je obdržet***. Tento prvek by se měl stát základním konstrukčním prvkem, čímž se posílí pohodlí a ochrana osobních údajů, včetně minimalizace zpracování osobních údajů***, zejména standardní ochrana soukromí již ve výchozím nastavení***. ***Mechanismy pro validaci evropské peněženky digitální identity, selektivní zveřejňování a autentizace uživatelů za účelem přístupu k on-line službám by měly zachovávat soukromí, a bránit tak sledování uživatele a dodržovat zásadu omezení účelu, z níž vyplývá právo na pseudonymitu, a to s cílem zajistit, aby uživatel nemohl být identifikován několika spoléhajícími se stranami. Technická architektura a provádění evropské peněženky digitální identity by měly být plně v souladu s nařízením (EU) 2016/679. Decentralizovaná povaha evropské peněženky digitální identity by navíc měla umožnit samopodepisování (self-signing) a odvolatelnost atributů a identifikátorů***.

(29a) Pokud zvláštní pravidla práva Unie nebo vnitrostátního práva nevyžadují, aby se uživatelé identifikovali, mělo by být používání služeb pod pseudonymem povoleno

a nemělo by být členskými státy omezeno, například uložením obecné povinnosti poskytovatelům služeb omezit pseudonymní využívání jejich služeb.

(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 ***právními předpisy Unie nebo*** vnitrostátními právními předpisy ▌pro účely bezpečné výměny potvrzených atributů mezi poskytovateli služeb v oblasti identifikace nebo potvrzování atributů a spoléhajícími se stranami.

(31) Bezpečná elektronická identifikace a potvrzování atributů by měly odvětví finančních služeb nabídnout 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 pro přihlášení k účtu a ***pro zahájení*** transakcí v oblasti platebních služeb.

(31a) Toto nařízení by mělo stanovit zásadu, že právní účinky elektronického podpisu nelze zpochybnit z důvodu, že je v elektronické podobě nebo že nesplňuje požadavky na kvalifikovaný elektronický podpis. Právní účinky elektronických podpisů by však měly být vymezeny vnitrostátním právem, s výjimkou požadavků stanovených v tomto nařízení, podle nichž má být právní účinek kvalifikovaného elektronického podpisu rovnocenný právnímu účinku vlastnoručního podpisu. Při určování právních účinků elektronických podpisů by členské státy měly zohlednit zásadu proporcionality mezi soudní hodnotou písemnosti, která má být podepsána, a úrovní bezpečnosti a nákladů, které elektronický podpis vyžaduje. V zájmu zvýšení dostupnosti a používání elektronických podpisů se členské státy vyzývají, aby zvážily používání pokročilých elektronických podpisů v každodenních transakcích, pro něž zajišťují dostatečnou úroveň bezpečnosti a důvěryhodnosti. Používání kvalifikovaných elektronických podpisů by mělo být povinné pouze tehdy, je-li vyžadována nejvyšší úroveň bezpečnosti a důvěryhodnosti.

(32) Služby autentizace internetových stránek uživatelům poskytují ***vysokou úroveň záruky ohledně identity subjektu, který za danou internetovou stránkou stojí***. Tyto služby

přispívají k budování důvěryhodnosti a důvěry v on-line obchodování, neboť uživatelé budou mít důvěru v internetové stránky, které byly autentizovány. Využívání služeb autentizace internetových stránek internetovými stránkami je dobrovolné. Aby se však autentizace internetových stránek stala prostředkem pro zvýšení důvěryhodnosti, zlepšení zkušeností uživatelů a podporu růstu na vnitřním trhu, stanoví toto nařízení pro poskytovatele služeb autentizace internetových stránek a jejich služby minimální povinnosti v oblasti bezpečnosti a odpovědnosti. Za tímto účelem by internetové prohlížeče měly zajistit podporu a interoperabilitu s kvalifikovanými certifikáty pro autentizaci internetových stránek podle nařízení (EU) č. 910/2014. Tyto prohlížeče by měly uznávat a zobrazovat kvalifikované certifikáty pro autentizaci internetových stránek, aby poskytovaly vysokou úroveň záruky a umožnily vlastníkům internetových stránek potvrdit svou totožnost coby vlastníků internetových stránek a uživatelům umožnily identifikovat vlastníky internetových stránek s vysokou mírou jistoty. Za účelem další podpory jejich používání by orgány veřejné moci v členských státech měly zvážit začlenění kvalifikovaných certifikátů pro autentizaci internetových stránek na své internetové stránky. ***V případě narušení bezpečnosti by internetové prohlížeče měly mít možnost přijmout opatření, která jsou úměrná riziku. Webové prohlížeče by měly Komisi neprodleně oznámit každé narušení bezpečnosti a opatření přijatá k nápravě takového narušení v souvislosti s jediným certifikátem nebo souborem certifikátů.***

(33) Mnoho členských států zavedlo vnitrostátní požadavky na služby poskytující bezpečnou a důvěryhodnou digitální archivaci, aby bylo možné dlouhodobě uchovávat elektronické dokumenty a související služby vytvářející důvěru. V zájmu zajištění právní jistoty a důvěry je nezbytné poskytnout právní rámec pro usnadnění přeshraničního uznávání kvalifikovaných služeb v oblasti elektronické archivace. Tento rámec by mohl rovněž přinést nové tržní příležitosti pro poskytovatele služeb vytvářejících důvěru z Unie.

I

(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***, občanskou***

společností, akademickými pracovníky a soukromým sektorem. K dosažení tohoto cíle by členské státy měly spolupracovat***. Členské státy by se měly dohodnout na*** komplexní technické architektuře a referenčním rámci, souboru společných norem a technických referencí***, včetně uznávaných platných norem,*** a souboru pokynů a popisu osvědčených postupů zahrnujících alespoň všechny aspekty funkcí a interoperability evropských peněženek digitální identity, včetně elektronických podpisů, a ***poskytovatelů*** 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. ▌

(36a) Aby byla zajištěna široká použitelnost a dostupnost, měla by být naplánována další opatření finanční podpory na podporu členských států při vydávání a správě evropských peněženek digitální identity. Za tímto účelem by Komise měla posoudit, zda jsou k dispozici dodatečné finanční prostředky Unie pro členské státy, které by požádaly o podporu při vývoji, zavádění a správě evropských peněženek digitální identity.

(36b) Aby se zajistilo širší využívání a použitelnost evropských peněženek digitální identity v celé Unii, měla by Komise při vytváření odvětvových nástrojů Unie, jako jsou evropský průkaz sociálního zabezpečení a společné evropské datové prostory, vycházet z rámce tohoto nařízení a využívat jej. Koordinace s evropským průkazem sociálního zabezpečení by měla umožnit digitální přenositelnost práv občanů na sociální zabezpečení přes hranice a ověřování jejich nároků a platnosti dokumentů. Pokud jde o společný evropský datový prostor, měly by evropské peněženky digitální identity umožňovat vyšší stupeň transparentnosti a kontroly uživatelů nad jejich údaji.

(37) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1525 byl konzultován evropský inspektor ochrany údajů[12].

---

12 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).

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

PŘIJALY TOTO NAŘÍZENÍ:

Článek 1

Nařízení (EU) 910/2014 se mění takto:

1) Článek 1 se nahrazuje tímto:

„Cílem tohoto nařízení je ***přispět k zajištění*** řádného fungování vnitřního trhu a současně poskytovat odpovídající úroveň bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru ***používaných v celé Unii***. Za těmito účely toto nařízení:

a) 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;

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, ***nekvalifikované služby elektronického doručování, kvalifikované*** služby elektronického doporučeného doručování, certifikační služby pro autentizaci internetových stránek, ▌ elektronické potvrzování atributů ***a*** správu prostředků pro vytváření elektronických podpisů a pečetí na dálku ▌ ;

d) stanoví podmínky pro vydávání***, správu a uznávání*** evropských peněženek digitální identity členskými státy ***a pro zajištění jejich interoperability a přeshraničního používání v Unii;***

da) umožňuje výkon práva na bezpečnou účast v digitální společnosti a usnadňuje všem fyzickým nebo právnickým osobám neomezený přístup k veřejným službám online v celé Unii.“;

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 vydané ***a spravované*** členskými státy a na poskytovatele služeb vytvářejících důvěru usazené v Unii.“;

b) odstavec 3 se nahrazuje tímto:

„3. Tímto nařízením není dotčeno ***právo Unie ani*** vnitrostátní právo ▌ týkající se:

a) uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy nebo

b) požadavků pro konkrétní odvětví na kvalifikované elektronické potvrzování atributů s ohledem na formu se základními právními účinky, zejména v souvislosti s přeshraničním uznáváním kvalifikovaného elektronického potvrzování atributů.“;

3) Článek 3 se mění takto:

a) ***body 2) až 6)*** se nahrazují tímto:

„2) „prostředkem pro elektronickou identifikaci“ hmotná či nehmotná jednotka, včetně evropských peněženek digitální identity nebo průkazů totožnosti podle nařízení 2019/1157, obsahující osobní identifikační údaje, která se používá k autentizaci pro účely on-line či offline služby;

3) „osobními identifikačními údaji“ soubor údajů, ***vydaných v souladu s vnitrostátním právem a*** umožňujících určit totožnost fyzické nebo právnické osoby nebo fyzické osoby zastupující právnickou osobu;

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

4a) „uživatelem“ fyzická nebo právnická osoba nebo fyzická osoba zastupující právnickou osobu, která využívá služby vytvářející důvěru, oznámené prostředky elektronické identifikace nebo evropské peněženky digitální identity;

5) „autentizací“ elektronický postup, který umožňuje ***ověřit*** původ a integritu dat v elektronické podobě;

5a) „identifikací“ elektronický postup, který stanoví jednoznačný vztah mezi souborem údajů a fyzickou nebo právnickou osobou; 5b) „validací“ postup ověřování, zda elektronický podpis, elektronická pečeť, evropská peněženka digitální identity, prostředek pro elektronickou identifikaci, oprávnění spoléhající se strany, osobní identifikační údaje, elektronické potvrzení atributů nebo elektronické certifikáty pro služby vytvářející důvěru jsou platné a nebyly zrušeny;

5c) „důkazem s nulovou znalostí“ kryptografické metody, kterými může spoléhající se strana ověřit, že dané tvrzení založené na elektronickém potvrzení atributů uchovávaných v evropské digitální peněžence uživatele je pravdivé, aniž by spoléhající se straně předala jakékoli údaje týkající se těchto elektronických potvrzení atributů;

6) „spoléhající se stranou“ fyzická nebo právnická osoba, která se spoléhá na ***prostředek*** elektronické identifikace***, včetně evropské peněženky digitální identity,*** nebo službu vytvářející důvěru, ***a to buď přímo, nebo prostřednictvím zprostředkovatele, za účelem poskytování služeb***;“;

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 vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování, elektronických potvrzování atributů a certifikátů souvisejících s těmito službami;

b) ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek;

c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami;

d) v elektronické archivaci elektronických dokumentů;

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

▌';

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 ▌, které znějí:

„23a) „prostředkem pro vytváření kvalifikovaných podpisů na dálku“ prostředek pro vytváření kvalifikovaných elektronických podpisů, přičemž kvalifikovaný poskytovatel služeb vytvářejících důvěru vytváří, spravuje nebo kopíruje data pro vytváření elektronických podpisů jménem podepisující osoby;

23b) „prostředkem pro vytváření kvalifikovaných pečetí na dálku“ prostředek pro vytváření kvalifikovaných elektronických pečetí, přičemž kvalifikovaný poskytovatel služeb vytvářejících důvěru vytváří, spravuje nebo kopíruje data pro vytváření elektronických podpisů jménem pečetící osoby;“

g) bod 29 se nahrazuje tímto:

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

ga) body 38) a 39) se nahrazují tímto:

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

39) „kvalifikovaným certifikátem pro autentizaci internetových stránek“ certifikát pro autentizaci internetových stránek, ***který spojuje internetové stránky s fyzickou nebo právnickou osobou, jíž je vydán certifikát s vysokou úrovní záruky, a*** který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze IV;“

▌’

i) doplňují se nové body ▌, které znějí:

„42) „evropskou peněženkou digitální identity“ ***prostředek pro elektronickou identifikaci, který bezpečně ukládá, spravuje a ověřuje*** údaje o totožnosti ***a elektronická potvrzení atributů***, poskytuje je na požádání spoléhajícím se stranám ***a dalším uživatelům evropských peněženek digitální identity a umožňuje vytváření*** kvalifikovaných elektronických podpisů a pečetí;

43) „atributem“ prvek, rys nebo vlastnost fyzické nebo právnické osoby nebo subjektu ▌;

44) „elektronickým potvrzováním atributů“ potvrzování v elektronické podobě, které umožňuje ***předkládání a*** 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;

46) „autentickým zdrojem“ registr nebo systém, za který odpovídá subjekt veřejného sektoru nebo soukromý subjekt a který obsahuje atributy fyzické nebo právnické osoby a je považován za primární zdroj těchto informací nebo je ***v unijním a*** vnitrostátním právu uznán za autentický;

47) „elektronickou archivací“ služba zajišťující ▌uchovávání ▌elektronických údajů nebo dokumentů s cílem zaručit jejich integritu, přesnost jejich původu a právní znaky po celou dobu uchovávání;

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

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

50) „silným ověřením uživatele“ ověření založené na použití ***alespoň dvou autentizačních faktorů*** kategorizovaných jako znalost, držení a inherence uživatele, kdy nesplněním jednoho z nich není ovlivněna spolehlivost ostatních, a ověření je navrženo tak, aby byla chráněna důvěrnost ověřovacích údajů;

51) „uživatelským účtem“ mechanismus, který uživateli umožňuje přístup k veřejným nebo soukromým službám za podmínek stanovených poskytovatelem služeb;

▌

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

55) ***„porovnáním totožnosti***“ postup, při němž jsou osobní identifikační údaje nebo prostředky osobní identifikace porovnávány nebo propojeny se stávajícím účtem patřícím téže osobě;

55a) „off-line službou“ schopnost uživatele se elektronicky identifikovat a autentizovat u třetí strany pomocí technologií blízkosti bez ohledu na to, zda je zařízení připojeno k internetu, či nikoli, s cílem získat přístup k široké škále veřejných a soukromých služeb.“;

4) Článek 5 se nahrazuje tímto:

„Článek 5

Ochrana osobních údajů a použití pseudonymů v elektronických transakcích

1. Zpracování osobních údajů se provádí v souladu s nařízeními (EU) 2016/679 a (EU) 2018/1725 a případně se směrnicí 2002/58/ES prováděním zásad minimalizace údajů, účelového omezení a záměrné a standardní ochrany údajů, zejména pokud jde o technická opatření pro provádění tohoto nařízení a rámec interoperability v souladu s článkem 12 tohoto nařízení.

2. Aniž jsou dotčeny právní účinky, které vnitrostátní právo přiznává pseudonymům***, a pokud právo Unie nebo vnitrostátní právo nestanoví zvláštní pravidla, která vyžadují, aby uživatelé pro právní účely uváděli svou totožnost, je při elektronických transakcích používání pseudonymů, které si uživatel svobodně zvolí, vždy povoleno a nesmí být zakázáno nebo omezeno prostřednictvím smlouvy nebo podmínek platných pro používání služby***.

3. Pokud zvláštní předpisy Unie nebo vnitrostátní právo nevyžadují, aby se uživatelé pro právní účely identifikovali, spoléhající se strany vynaloží přiměřené úsilí na to, aby umožnily využívání svých služeb bez elektronické identifikace nebo autentizace.“;

5) V kapitole II se název nahrazuje tímto:

„ODDÍL I

ELEKTRONICKÁ IDENTIFIKACE;“

6) Článek 6 se zrušuje.

7) Vkládají se nové články ▌, které znějí:

„Článek 6a

Evropské peněženky digitální identity

1. S cílem zajistit, aby všechny fyzické a právnické osoby v Unii měly bezpečný, ***spolehlivý***, důvěryhodný a hladký přístup k přeshraničním veřejným a soukromým službám ***a zároveň plnou kontrolu nad svými údaji***, vydá každý členský stát do ***[osmnáct*** měsíců od vstupu tohoto ***pozměňujícího*** nařízení v platnost***] alespoň jednu evropskou peněženku*** digitální identity.

2. Evropské peněženky digitální identity jsou vydávány ***a spravovány jedním z následujících způsobů***:

a) ***přímo*** členským státem;

b) z pověření členského státu;

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

2a. Zdrojový kód používaný pro poskytování evropských peněženek digitální identity je otevřený zdroj a je zveřejněn za účelem kontroly a přezkumu.

3. Evropské peněženky digitální identity ***uživatelsky vstřícným způsobem*** uživateli ***umožní***:

a) bezpečně požadovat a získávat, ukládat, vybírat, kombinovat a sdílet způsobem, který je pro uživatele transparentní a sledovatelný***, a pod výhradní kontrolou uživatele*** nezbytné ▌identifikační údaje ▌za účelem on-line a offline identifikace a autentizace ***uživatele*** s cílem využívat veřejné a soukromé služby on-line;

aa) bezpečně ukládat, vybírat, kombinovat a sdílet elektronické potvrzení atributů;

ab) bezpečně vydávat a zneplatňovat elektronické potvrzení atributů vydané přímo uživatelem;

ac) vytvářet pseudonymy a ukládat je v nich lokálně v zašifrované podobě;

ad) bezpečně ověřit evropské peněženky digitální identity třetí osoby nebo spoléhající se strany navazující spojení a transparentním a sledovatelným způsobem přijímat a ověřovat identifikační údaje třetí strany a elektronické potvrzení atributů online i offline;

ae) přístup k databázi všech transakcí provedených prostřednictvím evropské peněženky digitální identity, a to na základě společného přehledu, který uživateli umožní:

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

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

iii) snadno nahlašovat příslušnému orgánu členského státu, v němž je spoléhající se strana usazena, případy, kdy obdrží nezákonnou

nebo nevhodnou žádost o údaje, bez nutnosti opustit evropskou peněženku digitální identity;

iv) zneplatňovat elektronické potvrzení atributů vydané uživatelem;

b) podepisovat kvalifikovanými elektronickými podpisy***;***

ba) stáhnout údaje, elektronické potvrzení atributů a konfigurací všech uživatelů;

bb) uplatňovat právo uživatelů na přenositelnost údajů přechodem na jinou evropskou digitální peněženku patřící stejnému uživateli.

4. Evropské peněženky digitální identity zejména:

a) poskytují společné ***protokoly a*** rozhraní:

i) pro bezpečnou komunikaci s prostředky pro elektronickou identifikaci, které s nimi souvisejí podle čl. 7 odst. 2, za účelem identifikace a autentizace uživatele;

ii) pro vydavatele elektronického potvrzení atributů k vydávání elektronického potvrzení atributů pro evropskou peněženku digitální identity uživatele;

iii) pro navázání jedinečného, soukromého a bezpečného spojení peer-to peer mezi dvěma evropskými peněženkami s digitální identitou nebo mezi evropskou peněženkou digitální identity a spoléhající se stranou;

iv) uživatelům evropských peněženek digitální identity a spoléhajícím se stranám, aby mohli požadovat, přijímat, vybírat, odesílat, autentizovat a ověřovat elektronická potvrzení atributů, osobní identifikační údaje, identifikaci spoléhajících se stran, elektronické podpisy a elektronické pečetě;

v) uživatelům evropských peněženek digitální identity a spoléhajícím se stranám, aby mohli autentizovat a ověřovat evropskou peněženku digitální identity a schválené spoléhající se strany;

vi) uživatelům evropských peněženek digitální identity nebo případně spoléhajícím se stranám, aby mohli provést důkaz s nulovou znalostí odvozený z osobních identifikačních údajů nebo elektronického potvrzení atributů;

vii) uživatelům evropských peněženek digitální identity, aby mohli přenášet svá vlastní elektronická potvrzení atributů a konfigurací do jiné evropské peněženky digitální identity, která patří témuž uživateli, nebo do zařízení ovládanému týmž uživatelem, a žádat o opětovné vydání těchto potvrzení;

b) zajišťují, ***aby byly vytvořeny technologické překážky, které budou poskytovatelům*** kvalifikovaných ***a nekvalifikovaných elektronických*** potvrzení atributů ***bránit v získání jakýchkoli informací*** o používání těchto atributů;

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

ca) v případě elektronického potvrzení atributů, jehož součástí jsou zásady zveřejňování informací, poskytují mechanismus, který zajistí, aby k přístupu byla oprávněna pouze spoléhající se strana nebo uživatel evropské peněženky digitální identity mající nezbytné elektronické potvrzení atributů;

cb) poskytují mechanismus pro zaznamenávání obdržených digitálních žádostí a digitálních transakcí kryptografickým způsobem, který zajistí, že nebude možné vyvrátit jejich pravost;

cc) poskytují mechanismus pro bezodkladné informování uživatelů o všech případech narušení bezpečnosti, které zcela nebo částečně ohrozilo jejich evropské peněženky digitální identity nebo jejich obsah, zejména pokud vedlo k pozastavení nebo zrušení platnosti jejich evropských peněženek digitální identity podle článku 10a.

▌

e) zajistí, aby osobní identifikační údaje uvedené v čl. 12 odst. 4 písm. d) ▌ identifikovaly fyzickou nebo právnickou osobu, která je s nimi spojena;

ea) poskytnou mechanismus, který uživateli evropské peněženky digitální identity umožní jednat jménem jiné fyzické nebo právnické osoby;

eb) zobrazují „značku důvěry EU pro peněženku evropské digitální identity“ pro uznávání kvalifikovaného elektronického potvrzení atributů;

ec) nabízejí standardně a bezplatně kvalifikované elektronické podpisy všem uživatelům.“;

5. Členské státy ▌ poskytnou ***bezplatné*** mechanismy ověření***, které***:

a) ▌ zajistí, že je možné ověřit ▌ pravost a platnost ***evropských peněženek digitální identity***;

b) ▌ spoléhajícím se stranám ***a uživatelům evropských peněženek digitální identity*** umožní ověřit ***pravost a*** platnost ***elektronických*** potvrzení atributů;

c) ▌ spoléhajícím se stranám, ***uživatelům evropských peněženek digitální identity*** a kvalifikovaným poskytovatelům služeb vytvářejících důvěru umožní ověřit pravost a platnost přiřazených osobních identifikačních údajů;

ca) uživatelům evropské peněženky digitální identity umožní ověřit pravost a platnost totožnosti spoléhajících se stran schválených v souladu s čl. 6b odst. 1.

5a. Členské státy poskytnou prostředky pro zrušení platnosti evropské peněženky digitální identity:

a) na výslovnou žádost uživatele;

b) pokud byla ohrožena její bezpečnost;

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

5b. Členské státy prostřednictvím komunikačních kampaní zvyšují povědomí o přínosech a rizicích evropské peněženky digitální identity. Zajistí, aby jejich občané byli v používání této peněženky dobře proškoleni.

5c. Vydavatelé evropských peněženek digitální identity zajistí, aby uživatelé mohli snadno požádat o technickou podporu a hlásit technické problémy nebo jakékoli jiné incidenty, které mají negativní dopad na poskytování služeb evropské peněženky digitální identity.

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

6a. Evropské peněženky digitální identity zajišťují bezpečnost již od fáze návrhu. Evropské peněženky digitální identity mají nezbytné bezpečnostní funkce na nejmodernější úrovni, jako jsou mechanismy umožňující šifrovat a uchovávat údaje způsobem, který je přístupný pouze uživateli a dekódovatelný pouze jím, a zavádějí šifrovanou komunikaci mezi koncovými body se spoléhajícími se stranami a jinými evropskými peněženkami digitální identity. Nabízejí odolnost vůči zdatným útočníkům, zajišťují důvěrnost, integritu a dostupnost svého obsahu, včetně osobních identifikačních údajů a elektronických potvrzení atributů, a vyžadují bezpečné, výslovné a aktivní potvrzení jejich provozu uživatelem.

6b. Vydávání a používání evropských peněženek digitální identity je pro všechny fyzické i právnické osoby bezplatné.

7. ***Na technický rámec evropské peněženky digitální identity se vztahují tyto zásady:***

   a) evropskou peněženku digitální identity ***a údaje uživatele, včetně autocertifikace,*** má uživatel plně pod kontrolou;

   b) evropská peněženka digitální identity používá pro architekturu identity decentralizované prvky;

   c) soubor prostředků pro elektronickou identifikaci, atributů a certifikátů obsažených v evropské peněžence digitální identity musí být bezpečně uložen výhradně na zařízeních pod kontrolou uživatele, ledaže dá

uživatel svobodný souhlas s ukládáním na zařízeních třetích stran nebo s možností založenou na cloudu;

e) ***evropská peněženka digitální identity umožňuje bezpečné spojení mezi uživatelem a spoléhajícími se stranami;***

f) ***technická architektura evropské peněženky digitální identity brání vydavateli evropské peněženky digitální identity, členskému státu nebo jakékoli jiné straně v tom, aby shromažďovali nebo získávali prostředky pro elektronickou identifikaci, atributy, elektronické dokumenty obsažené v evropské peněžence digitální identity a informace o používání evropské peněženky digitální identity uživatelem, s výjimkou případů, kdy o to uživatel používající zařízení, která má pod kontrolou, požádá, a výměna informací prostřednictvím evropské peněženky digitální identity neumožňuje poskytovatelům elektronického potvrzování atributů, aby sledovali, propojovali, dávali do vzájemného vztahu nebo jinak získávali informace o transakcích nebo chování uživatelů;***

g) ***k jedinečným a trvalým identifikátorům mají spoléhající se strany přístup pouze v případě, že identifikaci uživatele vyžadují právní předpisy Unie nebo vnitrostátní právní předpisy;***

h) ***členské státy zajistí, aby příslušné informace o evropské peněžence digitální identity byly veřejně dostupné;***

i) osobní údaje týkající se poskytování evropské peněženky digitální identity jsou uchovávány fyzicky a logicky odděleně od jakýchkoli jiných uchovávaných údajů***;***

j) pokud evropskou peněženku digitální identity poskytují soukromé strany v souladu s odst. 1 písm. b) a c), použijí se obdobně ustanovení čl. 45f odst. 4***;***

k) ***pokud potvrzení atributů nevyžaduje identifikaci uživatele, provede se důkaz s nulovou znalostí;***

l) správcem pro účely nařízení (EU) 2016/679 v souvislosti se zpracováním osobních údajů v evropské peněžence digitální identity je vydavatel evropské peněženky digitální identity;

m) evropská peněženka digitální identity poskytne mechanismus pro podávání a vyřizování stížností, který uživatelům umožní přímo informovat dozorový úřad podle tohoto nařízení a dozorové úřady zřízené podle nařízení (EU) 2016/679, pokud spoléhající se strana požaduje nepřiměřené množství údajů, které není v souladu s registrovaným zamýšleným použitím těchto údajů.

7a. Používání evropských peněženek digitální identity je dobrovolné. Pro fyzické a právnické osoby, které nepoužívají evropskou peněženku digitální identity, nesmí být v žádném případě omezen ani znevýhodněn přístup k veřejným a soukromým službám, přístup na trh práce ani svoboda podnikání. Přístup k veřejným a soukromým službám musí být i nadále možný za použití jiných stávajících prostředků identifikace a autentizace.

I

9. Ustanovení čl. 24 odst. 2 písm. b), ***d)***, e), ***f), fa), fb)***, g) a h) se použije obdobně na členské státy, ***které přímo vydávají a spravují*** evropské peněženky digitální identity.

10. Evropská peněženka digitální identity je zpřístupněna osobám se zdravotním postižením v souladu s požadavky na přístupnost stanovenými v příloze I směrnice ***(EU)*** 2019/882 ***a v Úmluvě Organizace spojených národů o právech osob se zdravotním postižením[1] a rovněž osobám se zvláštními potřebami, včetně starších osob a osob s omezeným přístupem k digitálním technologiím nebo osob s nedostatečnou digitální gramotností.***

11. Do ***... [***šest měsíců od vstupu tohoto ***pozměňujícího*** nařízení v platnost***]*** stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky

[1] ***Schválena rozhodnutím Rady 2010/48/ES ze dne 26. listopadu 2009 o uzavření Úmluvy Organizace spojených národů o právech osob se zdravotním postižením Evropským společenstvím (Úř. věst. L 23, 27.1.2010, s. 35).***

digitální identity ▌ referenční normy pro požadavky uvedené ***v tomto článku***. ***Uvedený*** prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

11a. Do ... [šest měsíců ode dne vstupu tohoto pozměňujícího nařízení v platnost] přijme Komise akt v přenesené pravomoci v souladu s článkem 47 za účelem doplnění tohoto nařízení stanovením technických a provozních specifikací pro požadavky uvedené v tomto článku.

Článek 6b

Spoléhající se strany u evropských peněženek digitální identity

1. Pokud ***má spoléhající se strana*** v úmyslu spoléhat se na evropské peněženky digitální identity ***při poskytování veřejných nebo soukromých služeb, zaregistruje se*** v členském státě, v němž je spoléhající se strana usazena***. Při registraci uvede spoléhající se strana ve vztahu ke každé jednotlivé poskytované službě informace o údajích, které hodlá požadovat, zamýšlené použití požadovaných údajů a důvody žádosti. Spoléhající se strana oznámí členskému státu bez zbytečného odkladu jakoukoli změnu oznámených informací.***

1a. Spoléhající se strany, které mají v úmyslu zpracovávat zvláštní kategorie osobních údajů, jako jsou údaje o zdravotním stavu nebo biometrické údaje uvedené v článku 9 nařízení (EU) 2016/679, vyžadují předchozí souhlas příslušných orgánů v členském státě, v němž hodlají poskytovat své služby. Spoléhající se strany, které tento souhlas obdrží, zajistí, aby zpracování osobních údajů bylo prováděno v souladu s čl. 6 odst. 1 nařízení (EU) 2016/679.

1b. Odstavci 1 a 1a nejsou dotčeny požadavky na schválení ex ante stanovené právními předpisy Unie nebo vnitrostátními právními předpisy pro poskytování konkrétních služeb.

1c. Členské státy informace uvedené v odstavci 1 zveřejní na internetu spolu s identitou každé spoléhající se strany a jejich kontaktními údaji.

1d. Členské státy zavedou kontroly ex post s cílem ověřit, zda jsou žádosti o údaje přiměřené a úměrné deklarovanému záměru a zda je dodržena zásada minimalizace údajů.

1e. Evropský sbor pro rámec digitální identity zřízený podle článku 46c nebo kterýkoli členský stát zruší povolení spoléhajících se stran v případě nezákonného nebo podvodného použití evropské peněženky digitální identity nebo toto povolení pozastaví, dokud nebudou zjištěné nesrovnalosti napraveny.

2. Členské státy zavedou ▌ společný mechanismus ***pro identifikaci a autentizaci spoléhajících se stran a ověřování oznámených souborů údajů podle čl. 6a odst. 4 písm. ca) a cb)***.

2a. Pokud spoléhající se strany hodlají spoléhat na evropské peněženky digitální identity vydané v souladu s tímto nařízením, musí se před uskutečněním jakékoli jiné formy transakce autentizovat a identifikovat vůči uživateli evropské peněženky digitální identity.

3. Spoléhající se strany jsou odpovědné za provádění postupu autentizace ***a ověření*** osobních identifikačních údajů a elektronického potvrzování atributů pocházejících z evropských peněženek digitální identity. ***Spoléhající se strany souhlasí s používáním pseudonymů, pokud identifikace uživatele není vyžadována právem Unie nebo vnitrostátním právem.***

3a. Zprostředkovatelé, kteří jednají jménem spoléhajících se stran, se považují za spoléhající se strany a nezískávají údaje o obsahu transakce.

4. ***Do ... [***šest měsíců ode dne vstupu tohoto ***pozměňujícího*** nařízení v platnost***] přijme*** Komise ***akty v přenesené pravomoci v souladu s článkem 47 za účelem doplnění tohoto nařízení stanovením*** technických a provozních specifikací pro požadavky uvedené ***v tomto článku v souladu s čl. 6a odst. 11a.***

Článek 6c

Certifikace evropských peněženek digitální identity

1. Evropské peněženky digitální identity, které byly certifikovány nebo pro něž bylo vydáno prohlášení o shodě v rámci systému kybernetické bezpečnosti podle nařízení (EU) 2019/881 a na něž byly zveřejněny odkazy v Úředním věstníku Evropské unie, se považují za vyhovující požadavkům týkajícím se kybernetické bezpečnosti stanoveným v článku 6a ***tohoto nařízení,*** pokud se na tyto požadavky vztahuje certifikát kybernetické bezpečnosti nebo prohlášení

o shodě či jejich části. ***Jsou-li k dispozici příslušné evropské systémy certifikace kybernetické bezpečnosti, evropská peněženka digitální identity nebo její části jsou certifikovány v souladu s těmito systémy.***

2. Soulad s požadavky stanovenými v čl. 6a odst. 3, 4 a 5 týkajícími se operací zpracování osobních údajů, které provádí vydavatel evropských peněženek digitální identity, je certifikován podle nařízení (EU) 2016/679.

2a. Jsou-li k dispozici příslušné evropské systémy certifikace funkčnosti a interoperability, evropská peněženka digitální identity nebo její části jsou certifikovány v souladu s těmito systémy. U těchto systémů certifikace existuje předpoklad shody s požadavky na funkčnost a interoperabilitu stanovenými v článku 6a. Neexistují-li systémy certifikace pro funkčnost a interoperabilitu, použijí se normy uvedené v čl. 6a odst. 11.

3. Soulad evropských peněženek digitální identity s požadavky stanovenými v článku 6a ***tohoto nařízení*** je certifikován ***subjekty posuzování shody v souladu s článkem 60 nařízení (EU) 2019/881 v případě požadavků na kybernetickou bezpečnost a subjekty pro vydávání osvědčení v souladu s článkem 43 nařízení (EU) 2016/679 v případě operací zpracování osobních údajů***.

3a. Pro účely tohoto článku evropské peněženky digitální identity nepodléhají požadavkům uvedeným v článcích 7 a 9.

4. ***Do ...[***šesti měsíců ode dne vstupu tohoto ***pozměňujícího*** nařízení v platnost***]*** stanoví Komise prostřednictvím prováděcích aktů seznam norem***, technických specifikací, postupů a dostupných unijních a vnitrostátních systémů certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881 nezbytných*** pro certifikaci evropských peněženek digitální identity ***uvedených v odstavcích 2a a 3 tohoto článku***. ***Uvedené prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2 tohoto nařízení.***

5. Členské státy sdělí Komisi názvy a adresy ▌subjektů ***posuzování shody a subjektů pro vydávání osvědčení*** uvedených v odstavci 3. Komise tyto informace zpřístupní ***všem*** členským státům.

6. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 47***, kterými doplní toto nařízení stanovením*** zvláštních kritérií ▌ uvedených v odstavci 3 ***tohoto článku***.

Článek 6d

Zveřejnění seznamu certifikovaných evropských peněženek digitální identity

1. Členské státy bez zbytečného odkladu informují Komisi o evropských peněženkách digitální identity, které byly vydány podle článku 6a a certifikovány subjekty uvedenými v čl. 6c odst. 3. Rovněž bez zbytečného odkladu informují Komisi o zrušení certifikace ***a o důvodech tohoto zrušení***.

2. Na základě obdržených informací Komise zřizuje, zveřejňuje a udržuje ***aktualizovaný strojově čitelný*** seznam certifikovaných evropských peněženek digitální identity.

3. ***Do ... [***šest měsíců od vstupu tohoto ***pozměňujícího*** 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 odstavce 1 ***tohoto článku***. ***Uvedený prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.“;***

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 ***do ...[***dvanáct měsíců od vstupu tohoto nařízení v platnost***]*** alespoň jeden systém elektronické identifikace, včetně alespoň jednoho ***prostředku pro elektronickou identifikaci s úrovní záruky „vysoká“***, ***který splňuje všechny následující podmínky:***

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

„2. Komise ***bez zbytečného odkladu*** zveřejní v Úředním věstníku Evropské unie seznam systémů elektronické identifikace, které byly oznámeny podle odstavce 1 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.“;

10a) V článku 10 se nadpis nahrazuje tímto:

„Narušení bezpečnosti ***systémů elektronické identifikace pro přeshraniční ověřování***“;

11) Vkládá se nový článek ▌, který zní:

„Článek 10a

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), b) a c) porušeny nebo částečně ohroženy způsobem, který ovlivňuje jejich spolehlivost ***a důvěrnost, integritu nebo dostupnost uživatelských dat*** nebo spolehlivost ostatních evropských peněženek digitální identity, členský stát, který je vydal, bezodkladně pozastaví vydávání evropských peněženek digitální identity, zruší jejich platnost a informuje o tom ***dotčené uživatele, jednotné kontaktní místo určené podle článku 46a, spoléhající se strany,*** ostatní členské státy a Komisi.

1a. Po oznámení narušení bezpečnosti evropské peněženky digitální identity jednotné kontaktní místo určené podle článku 46a naváže kontakt s příslušnými vnitrostátními orgány a v případě potřeby s Evropským sborem pro rámec digitální identity zřízeným podle čl. 46c, Evropským sborem pro ochranu osobních údajů, Komisí a agenturou ENISA.

2. Pokud bylo narušení nebo ohrožení bezpečnosti uvedené v odstavci 1 napraveno, vydávající členský stát obnoví vydávání a používání evropských peněženek digitální identity a bez zbytečného odkladu o tom uvědomí příslušné ***vnitrostátní orgány ostatních členských států, dotčené uživatele a spoléhající se strany, jednotné kontaktní místo určené podle článku 46a*** a Komisi.

3. ***Nedojde-li k žádnému pokusu o nápravu nebo dostatečnému pokroku v nápravě*** porušení nebo ohrožení uvedeného v odstavci 1 do tří měsíců od pozastavení nebo zrušení, dotčený členský stát dotyčnou evropskou digitální peněženku stáhne a informuje o stažení ***dotčené uživatele, jednotné kontaktní***

místo určené podle článku 46a, spoléhající se strany a ostatní členské státy a Komisi. Je-li to odůvodněno závažností porušení, je evropská peněženka digitální identity stažena neprodleně ***a příslušné rozhodnutí by mělo být odůvodněno a sděleno Komisi***.

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

5. ***Do ... [šest*** měsíců od vstupu tohoto ***pozměňujícího*** nařízení v platnost***]***, přijme Komise ***v souladu s článkem 47 akt v přenesené pravomoci za účelem doplnění tohoto nařízení a dalšího upřesnění*** opatření uvedených v odstavcích 1 a 3 ***tohoto článku***. “;

12) Vkládá se nový článek ▌, který zní:

„Článek 11a

Identifikace ***přeshraničního uživatele***

1. ***Při přístupu k přeshraničním veřejným službám, který vyžaduje identifikaci uživatele podle práva Unie nebo vnitrostátního práva, členské státy zajistí jednoznačné porovnání totožnosti fyzických osob za použití*** oznámených prostředků pro elektronickou identifikaci ***nebo*** evropských peněženek digitální identity. ***Členské státy stanoví technická a organizační opatření s cílem zajistit ochranu osobních údajů a zabránit profilování uživatelů.***

2. ***Za účelem identifikace fyzických osob na jejich žádost o přístup ke službám popsaným v odstavci 1 poskytnou členské státy*** minimální soubor osobních identifikačních údajů uvedený v čl. 12 odst. 4 písm. d). ***Členské státy, které mají alespoň jeden jedinečný identifikátor, vydávají na žádost uživatele*** jedinečné a trvalé identifikátory ***pro přeshraniční použití. Tyto jedinečné a trvalé identifikátory mohou být specifické pro jednotlivá odvětví nebo spoléhající se strany, pokud jednoznačně identifikují uživatele v celé Unii.***

2a. Členské státy poskytnou jeden jedinečný a trvalý identifikátor právnickým osobám používajícím prostředky pro elektronickou identifikaci nebo evropské peněženky digitální identity.

3. ***Do... [šest*** měsíců ode dne vstupu tohoto ***pozměňujícího*** nařízení v platnost***]*** přijme Komise prováděcí akt o zavedení evropských peněženek digitální identity podle čl. 6a odst. 11, ***kterým stanoví další technické specifikace, které posilují soukromí a zajistí důvěryhodnou, bezpečnou a interoperabilní přeshraniční autentizaci a identifikaci uživatelů***. ***Uvedený prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.“;***

13) Článek 12 se mění takto:

-a) nadpis se nahrazuje tímto:

„▌ Interoperabilita“;

a) v odstavci 3 se písmena c) a d) nahrazují tímto:

„c) usnadňuje zavádění ochrany a bezpečnosti dat již od návrhu;

d) zajišťuje, aby osobní údaje byly zpracovávány v souladu s nařízením (EU) 2016/679.“;

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

„d) odkazu na minimální soubor osobních identifikačních údajů nezbytných k ***jednoznačné*** identifikaci fyzické nebo právnické osoby***, které jsou v systémech elektronické identifikace k dispozici. Obecně platí, že pokud jde o osobní údaje, posuzují se rizika pro práva fyzických osob na základě čl. 25 odst. 1 nařízení (EU) 2016/679;“;***

ba) odstavec 5 se zrušuje;

c) ***odstavec 6 se zrušuje;***

ca) odstavec 7 se zrušuje;

cb) odstavec 9 se nahrazuje tímto:

„9. Prováděcí akty uvedené v ***odstavci 8*** tohoto článku se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

14) Vkládá se nový článek ▌, který zní:

„Článek 12a

Certifikace systémů elektronické identifikace

1. Soulad oznámených systémů elektronické identifikace s požadavky stanovenými v ***článcích 8 a 10*** může být certifikován ***subjekty posuzování shody*** určenými členskými státy.

2. Vzájemné hodnocení systémů elektronické identifikace uvedené v čl. 46b odst. 5 písm. c) ***tohoto nařízení*** se nevztahuje na systémy elektronické identifikace nebo na část těchto systémů certifikovaných v souladu s odstavcem 1. Členské státy mohou použít certifikát nebo prohlášení Unie o shodě vydané v souladu s příslušným evropským systémem certifikace kybernetické bezpečnosti zřízeným podle nařízení (EU) 2019/881 s cílem prokázat ***úplný nebo částečný*** soulad těchto systémů ***nebo jejich součástí*** s požadavky stanovenými v čl. 8 odst. 2 ***tohoto nařízení***, pokud jde o úrovně záruky systémů elektronické identifikace.

2a. Certifikační systém používaný k prokázání shody podle odstavce 1 zahrnuje posouzení zranitelnosti certifikovaného výrobku prováděné každé dva roky a průběžné sledování hrozeb, pokud takový systém certifikace nebyl zaveden podle nařízení (EU) 2019/881.

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

15) Za článek 12a se vkládá nový nadpis, který zní:

„ODDÍL III

PŘESHRANIČNÍ VYUŽÍVÁNÍ PROSTŘEDKŮ PRO ELEKTRONICKOU IDENTIFIKACI“.

16) vkládají se nové články ▌, které znějí:

„Článek 12b

Přeshraniční využívání peněženek evropské digitální identity

1. Pokud členské státy podle vnitrostátního práva nebo správní praxe pro přístup k on-line službě poskytované subjektem veřejného sektoru vyžadují elektronickou identifikaci s použitím prostředku pro elektronickou identifikaci

a autentizaci, přijmou rovněž evropské peněženky digitální identity vydané v souladu s tímto nařízením ***pro účely elektronické identifikace a autentizace a o jejich přijetí jasným způsobem informují potenciální uživatele služby.***

2. Pokud ***právní předpisy Unie nebo vnitrostátní právní předpisy*** vyžadují od soukromých spoléhajících se stran poskytujících služby silnou autentizaci uživatele k on-line identifikaci ▌, a to i v oblasti dopravy, energetiky, bankovnictví a finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, ***telekomunikací nebo*** vzdělávání, ***zejména s ohledem na uznávání vzdělání a odborné kvalifikace, nabízejí a*** akceptují soukromé spoléhající se strany rovněž evropské peněženky digitální identity ***a oznámené prostředky pro elektronickou identifikaci*** vydané v souladu s ***tímto nařízení pro účely identifikace a autentizace***.

3. V případech, kdy velmi ***velké*** on-line platformy ve smyslu ***článku 25 odst. 1 nařízení (EU) 2022/2065*** vyžadují, aby se uživatelé pro přístup k on-line službám autentizovali, přijímají rovněž evropské peněženky digitální identity vydané v souladu s článkem 6a, ***nikoli však výlučně, a usnadňují jejich používání, a to*** výhradně na dobrovolnou žádost uživatele a s ohledem na ***právo použít pseudonym stanovené v tomto nařízení. V tomto případě se v souvislosti s evropskou peněženkou digitální identity používají pseudonymy vygenerované uživateli. Velmi velké on-line platformy o této možnosti uživatele služby jasným způsobem informují. Pokud o to uživatel výslovně nepožádá, je zakázáno kombinovat osobní identifikační údaje a jiné osobní údaje a identifikátory spojené s evropskými peněženkami digitální identity s osobními nebo neosobními údaji z jiných služeb, které nejsou nezbytné pro poskytování autentizace nebo používání základních služeb.***

4. Komise ***ve spolupráci s členskými státy, průmyslem a příslušnými relevantními zúčastněnými stranami včetně občanské společnosti*** podpoří a usnadní vytvoření samoregulačních kodexů chování na úrovni Unie (dále jen „kodexy chování“) s cílem přispět k široké dostupnosti a použitelnosti evropských peněženek digitální identity v oblasti působnosti tohoto nařízení. Tyto kodexy chování zajistí 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 třetích stran. 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.

▌

Článek 12c

Vzájemné uznávání jiných prostředků pro elektronickou identifikaci

1. Pokud se podle vnitrostátního práva nebo správní praxe pro přístup k on-line službě poskytované subjektem veřejného sektoru v určitém členském státě vyžaduje elektronická identifikace s použitím prostředku pro elektronickou identifikaci a autentizace, je pro účely přeshraniční autentizace pro danou on-line službu ***a pro účely vzájemného uznávání*** v tomto členském státě uznán prostředek pro elektronickou identifikaci vydaný v jiném členském státě, pokud jsou splněny tyto podmínky:

   a) daný prostředek pro elektronickou identifikaci je vydán v rámci systému elektronické identifikace, který je uveden na seznamu podle článku 9;

   b) úroveň záruky daného prostředku pro elektronickou identifikaci odpovídá stejné úrovni záruky, jako je úroveň záruky požadovaná příslušným subjektem veřejného sektoru v dotčeném členském státě pro přístup k dané on-line službě, nebo vyšší úrovni, ale v každém případě ne úrovni nižší, než je „značná“ úroveň záruky;

   c) příslušný subjekt veřejného sektoru v dotčeném členském státě používá v souvislosti s přístupem k dané on-line službě „značnou“ nebo „vysokou“ úroveň záruky.

   K tomuto uznání dojde do šesti měsíců od zveřejnění seznamu uvedeného v prvním pododstavci písm. a) Komisí.

2. Pro účely přeshraniční autentizace pro on-line službu poskytovanou subjekty veřejného sektoru mohou tyto subjekty uznat prostředek pro elektronickou

identifikaci, který byl vydán v rámci působnosti systému elektronické identifikace uvedeného na seznamu podle článku 9 a který odpovídá „nízké“ úrovni záruky.“

17) V článku 13 se odstavec 1 nahrazuje tímto:

„1. Bez ohledu na odstavec 2 tohoto článku odpovídají poskytovatelé služeb vytvářejících důvěru za škody, které úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle tohoto nařízení a povinností v oblasti řízení kybernetických bezpečnostních rizik podle článku 18 směrnice XXXX/XXXX [o bezpečnosti sítí a informací 2].“

18) Článek 14 se nahrazuje tímto:

„Článek 14

Mezinárodní aspekty

1. Komise může v souladu s ***článkem 47*** přijmout ***akty v přenesené pravomoci***, kterými ***doplní toto nařízení stanovením podmínek***, za nichž lze požadavky třetí země vztahující se na poskytovatele služeb vytvářejících důvěru usazené na jejím území a na služby vytvářející důvěru, které poskytují, považovat za rovnocenné s požadavky vztahujícími se na kvalifikované poskytovatele služeb vytvářejících důvěru usazené v Unii a na kvalifikované služby vytvářející důvěru, které poskytují.

2. Pokud Komise přijala ***akt v přenesené pravomoci*** podle odstavce 1 nebo uzavřela mezinárodní dohodu o vzájemném uznávání služeb vytvářejících důvěru v souladu s článkem 218 Smlouvy, považují se služby vytvářející důvěru poskytované poskytovateli usazenými v dotčené třetí zemi za rovnocenné s kvalifikovanými službami vytvářejícími důvěru poskytovanými kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými v Unii.“

19) Článek 15 se nahrazuje tímto:

„Článek 15

Přístupnost pro osoby se zdravotním postižením ***a zvláštními potřebami***

Poskytování služeb vytvářejících důvěru a konečných uživatelských produktů používaných při poskytování těchto služeb ***probíhá v jasném a snadno***

srozumitelném jazyce a způsobem přístupným osobám se zdravotním postižením ***aosobám s funkčními omezeními, jako jsou starší lidí, a osobám s omezeným přístupem k digitálním technologiím*** v souladu s požadavky na přístupnost stanovenými v příloze I směrnice ***(EU)*** 2019/882 o požadavcích na přístupnost u výrobků a služeb ***a v Úmluvě OSN o právech osob se zdravotním postižením[1]***.“

19a) Článek 16 se nahrazuje tímto:

„Článek 16

Sankce

1. Aniž je dotčen článek 31 směrnice (EU) XXXX/XXXX [NIS 2], členské státy stanoví pravidla pro ukládání sankcí za porušení tohoto nařízení. Stanovené sankce musí být účinné, přiměřené a odrazující, ***zejména pokud se porušení dopustil malý a střední podnik.***

2. Členské státy zajistí, aby za porušení povinností stanovených v tomto nařízení, jehož se dopustil kvalifikovaný poskytovatel služeb vytvářejících důvěru, byly uloženy správní pokuty v maximální výše nejméně 10 000 000 EUR, nebo 2 % celkového celosvětového ročního obratu podniku, k němuž kvalifikovaný poskytovatel služeb vytvářejících důvěru patřil v předchozím finančním roce, podle toho, co je vyšší.

3. Členské státy zajistí, aby za porušení povinností stanovených v tomto nařízení, jehož se dopustil nekvalifikovaný poskytovatel služeb vytvářejících důvěru, byly uloženy správní pokuty v maximální výši nejméně 7 000 000 EUR, nebo 1,4 % celkového celosvětového ročního obratu podniku, k němuž nekvalifikovaný poskytovatel služeb vytvářejících důvěru patřil v předchozím finančním roce, podle toho, co je vyšší.

20) ***Články 17, 18, a 19 se zrušují.***

▌

[1] ***Schválena rozhodnutím Rady 2010/48/ES ze dne 26. listopadu 2009 o uzavření Úmluvy Organizace spojených národů o právech osob se zdravotním postižením Evropským společenstvím (Úř. věst. L 23, 27.1.2010, s. 35).***

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 potvrdí, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru i jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení a v článku 18 směrnice (EU) XXXX/XXXX [o bezpečnosti sítí a informací 2]. ***Pokud byly součásti služeb vytvářejících důvěru samostatně certifikovány v souladu s tímto nařízením, subjekt posuzování shody odpovědný za certifikaci služby vytvářející důvěru neprovádí další audity těchto součástí. Subjekt posuzování shody se namísto toho ujistí, že interakce mezi různými součástmi nebrání shodě služby vytvářející důvěru s požadavky stanovenými v tomto odstavci.*** Kvalifikovaní poskytovatelé služeb vytvářejících důvěru předloží výslednou zprávu o posouzení shody do tří pracovních dnů od jejího obdržení orgánu dohledu.“;

b) v odstavci 2 se poslední věta nahrazuje tímto:

Aniž jsou dotčeny případné další povinnosti správců nebo zpracovatelů údajů vyplývající z nařízení (EU) 2016/679, pokud existuje důvod domnívat se, že pravidla ochrany údajů mohla být porušena, vyrozumí orgán dohledu bez zbytečného odkladu dozorové úřady podle nařízení (EU) 2016/679 a vydavatele a správce evropské peněženky a poskytne jim výsledky svých auditů, jakmile jsou k dispozici.

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, ▌ orgán dohledu zejména s přihlédnutím k rozsahu, délce trvání a důsledkům daného neplnění ***odejme*** danému poskytovateli nebo jím poskytované dotčené službě status

kvalifikovaného poskytovatele nebo kvalifikované služby a případně jej ***požádá***, aby ve stanovené lhůtě splnil požadavky směrnice XXXX/XXXX [o bezpečnosti sítí a informací 2]. Orgán dohledu informuje orgán uvedený v čl. 22 odst. 3 za účelem aktualizace důvěryhodných seznamů uvedených v čl. 22 odst. 1.

Orgán dohledu vyrozumí daného kvalifikovaného poskytovatele služeb vytvářejících důvěru o odnětí statusu kvalifikovaného poskytovatele nebo kvalifikované služby.

4. Do ... [12 měsíců od vstupu tohoto ***pozměňujícího*** nařízení v platnost] určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro:

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

b) auditní požadavky vztahující se na subjekty posuzování shody při provádění 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 o posouzení shody uvedených v odstavci 1.

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

23) Článek 21 se mění takto:

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 [o bezpečnosti sítí a informací 2], orgán dohledu požádá příslušné orgány uvedené ve směrnici XXXX [o bezpečnosti sítí a informací 2] o provedení opatření dohledu v tomto ohledu a o poskytnutí informací o výsledku do tří dnů od jejich dokončení.

Dojde-li orgán dohledu k závěru, že poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky uvedené v prvním pododstavci, 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 ... [12 měsíců od vstupu tohoto ***pozměňujícího*** nařízení v platnost] stanoví Komise prostřednictvím prováděcích aktů formáty a postupy oznamování a ověřování pro účely odstavců 1 a 2 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

23a) Článek 22 se mění takto:

a) odstavec 22 se nahrazuje tímto:

„1. Každý členský stát zřizuje, udržuje, ***pravidelně aktualizuje*** a zveřejňuje důvěryhodné seznamy obsahující informace týkající se kvalifikovaných poskytovatelů služeb vytvářejících důvěru v jeho působnosti spolu s informacemi o jimi poskytovaných kvalifikovaných službách vytvářejících důvěru.

b) vkládá se nový odstavec, který zní:

„3a. Komise v koordinaci s členskými státy a případně s agenturou ENISA vyvine harmonizovaný mechanismus pro podávání zpráv, který budou kvalifikovaní poskytovatelé služeb vytvářejících důvěru a ostatní zainteresované třetí strany používat k tomu, aby transparentním způsobem a s řádným odůvodněním napadli rozhodnutí členského státu o zařazení kvalifikovaného poskytovatele služby vytvářející důvěru na důvěryhodný seznam nebo jeho vyškrtnutí z tohoto seznamu.“;

c) *doplňuje se nový odstavec, který zní:*

„5a. Do … [šest měsíců od vstupu tohoto pozměňujícího nařízení v platnost] stanoví Komise prostřednictvím prováděcích aktů další podrobnosti týkající se postupu uvedeného v odstavci 3a. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

24) V článku 23 se vkládá nový odstavec 2a, který zní:

„2a. Odstavce 1 a 2 se použijí rovněž na poskytovatele služeb vytvářejících důvěru usazené ve třetích zemích a na služby, které poskytují, za předpokladu, že byli uznáni v Unii v souladu s článkem 14.“

25) Článek 24 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Při vydávání kvalifikovaného certifikátu nebo kvalifikovaného elektronického potvrzení atributů pro službu vytvářející důvěru ověří kvalifikovaný poskytovatel služeb vytvářejících důvěru totožnost a případně zvláštní znaky fyzické nebo právnické osoby, jíž se kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributu vydává.

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 oznámených prostředků pro elektronickou identifikaci, které splňují požadavky stanovené v článku 8, pokud jde o „vysokou“ úroveň záruky;

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

c) použitím jiných metod identifikace, které zajišťují identifikaci fyzické 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, nejsou-li k dispozici jiné prostředky.“;

b) doplňuje se nový odstavec ▌, který zní:

„1a. ***Do ... [12 měsíců od data vstupu tohoto nařízení v platnost] přijme Komise akty v přenesené pravomoci přijatých v souladu s článkem 47, kterými doplní toto nařízení*** stanovením minimálních technických specifikací, norem a postupů týkajících se ověřování identity a atributů v souladu s odst. 1 písm. c). tohoto článku.“;

c) odstavec 2 se mění takto:

1) písmeno d) se nahrazuje 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;“

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 registrace a spuštění služby;

ii) opatření týkající se procesních nebo správních kontrol;

iii) opatření týkající se řízení a provádění služeb.

fb) oznámí orgánu dohledu a případně dalším příslušným orgánům veškerá související porušení nebo narušení při 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.“;

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 elektronických potvrzení atributů.“;

e) odstavec 5 se nahrazuje tímto:

„5. b určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro požadavky uvedené v odstavci 2 ***tohoto článku***. Pokud důvěryhodné systémy a produkty vyhovují těmto normám, 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 akty v přenesené pravomoci ***v souladu s článkem 47, kterými doplní toto nařízení,*** pokud jde o dodatečná opatření uvedená v odst. 2 písm. fa) ***tohoto článku***.“

26) V článku 28 se odstavec 6 nahrazuje tímto:

„6. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro kvalifikované certifikáty pro elektronické podpisy. Pokud kvalifikovaný certifikát pro elektronický podpis vyhovuje těmto normám, 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. Data pro vytváření ***kvalifikovaných*** elektronických podpisů může jménem podepisující osoby vytvářet, spravovat a kopírovat 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 ▌, 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) kopíruje 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 ... [12 měsíců od vstupu tohoto pozměňujícího 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. Certifikát uvedený v odstavci 1 je platný po dobu pěti let pod podmínkou pravidelného hodnocení zranitelnosti každé dva roky. Jsou-li zjištěna zranitelná místa a nejsou-li napravena, certifikace se odejme.“

30) V článku 31 se odstavec 3 nahrazuje tímto:

„3. ***Do ... [12 měsíců od data vstupu tohoto pozměňujícího 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 normám uvedeným v odstavci 3, předpokládá se shoda s požadavky stanovenými v prvním pododstavci.“;

b) odstavec 3 se nahrazuje tímto:

„3. ***Do ... [12 měsíců od data vstupu tohoto pozměňujícího nařízení v platnost]*** určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro ověřování kvalifikovaných elektronických podpisů. 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 normám uvedeným v odstavci 3, předpokládá se shoda s požadavky stanovenými v odstavci 1.

3. ***Do ... [12 měsíců od data vstupu tohoto pozměňujícího nařízení v platnost]*** určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

33) Článek 37 se mění takto:

a) doplňuje se nový odstavec 2a, který zní:

„2a. Pokud zaručená elektronická pečeť vyhovuje normám uvedeným v odstavci 4, předpokládá se shoda s požadavky na zaručené elektronické pečetě uvedenými v článku 36 a v odstavci 5 tohoto článku.“;

b) odstavec 4 se nahrazuje tímto:

„4. Do ... [12 měsíců od data vstupu tohoto pozměňujícího nařízení v ***platnost]*** určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro zaručené elektronické pečetě. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

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 normám uvedeným v odstavci 6, předpokládá se shoda s požadavky stanovenými v příloze III.“;

b) odstavec 6 se nahrazuje tímto:

„6. ***Do ... [12 měsíců od vstupu data tohoto pozměňujícího nařízení v platnost]*** určí Komise prostřednictvím prováděcích aktů 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 ▌, který zní:

„Článek 39a

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

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

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 normám uvedeným v odstavci 2, předpokládá se shoda s požadavky stanovenými v odstavci 1.“;

b) odstavec 2 se nahrazuje tímto:

„2. ***Do ... [12 měsíců od data vstupu tohoto pozměňujícího nařízení v platnost]*** určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro spojení data a času s daty a zdroje přesného času. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

37) Článek 44 se mění takto:

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

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

b) odstavec 2 se nahrazuje tímto:

„2. ***Do ... [12 měsíců od data vstupu tohoto pozměňujícího nařízení v platnost]*** určí Komise prostřednictvím prováděcích aktů referenční

čísla norem pro postupy odesílání a přijímání dat. Tyto prováděcí akty se přijímají 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 ***umožňují autentizaci a identifikaci fyzických nebo právnických osob, kterým byl vydán certifikát s vysokou úrovní záruky. Kvalifikované certifikáty pro autentizaci internetových stránek musí rovněž*** splňovat požadavky stanovené v příloze IV. Kvalifikované certifikáty pro autentizaci internetových stránek se považují za vyhovující ***tomuto odstavci a*** požadavkům stanoveným v příloze IV, pokud vyhovují normám uvedeným v odstavci 3.

2. Kvalifikované certifikáty pro autentizaci internetových stránek uvedené v odstavci 1 jsou rozpoznávány internetovými prohlížeči. ***Poskytovatelům internetových prohlížečů nesmí být bráněno přijímat nezbytná a proporcionální opatření k řešení odůvodněných rizik narušení bezpečnosti, soukromí uživatelů a ztráty integrity certifikátů, jsou-li tato opatření řádně odůvodněna. V takovém případě poskytovatel webového prohlížeče neprodleně uvědomí o přijatých opatřeních Komisi, ENISA a kvalifikovaného poskytovatele služeb vytvářejících důvěru. Rozpoznávání kvalifikovaných certifikátů internetovými prohlížeči zajišťuje, že příslušné údaje o totožnosti a vydaná elektronická potvrzení atributů se zobrazují uživatelsky přívětivým a pokud možno jednotným způsobem, který odpovídá nejmodernějším postupům v oblasti přístupnosti, informovanosti uživatelů a kybernetické bezpečnosti v souladu s nejvyššími normami v odvětví.*** 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.

3. ***Do ... [12 měsíců od data vstupu tohoto pozměňujícího 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 nebo že bylo vydáno poskytovatelem služeb vytvářejících důvěru usazeným v jiném členském státě.***

2. Kvalifikované elektronické potvrzení atributů má stejný právní účinek jako zákonně vydaná potvrzení v tištěné podobě. ***Spoléhající se strany budou i nadále přijímat tato potvrzení v tištěné podobě jako alternativu k elektronickému potvrzení atributů.***

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

Elektronické potvrzování atributů ve veřejných službách

Pokud se podle vnitrostátního práva pro přístup k on-line službě poskytované subjektem veřejného sektoru vyžaduje 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 nebo subjekt veřejného

sektoru výslovně nepovolí. V takovém případě se rovněž přijímá kvalifikované elektronické potvrzování atributů z jiných členských států.

Článek 45c

Požadavky na kvalifikované potvrzení atributů

1. Kvalifikované elektronické potvrzení atributů musí splňovat požadavky stanovené v příloze V. Kvalifikované elektronické potvrzení atributů se považuje za vyhovující požadavkům stanoveným v příloze V, pokud vyhovuje normám uvedeným v odstavci 4.

2. ***Aniž je dotčen obsah atributů,*** nepodléhají kvalifikovaná elektronická potvrzení atributů žádným závazným požadavkům kromě požadavků stanovených v příloze V.

3. Pokud bylo kvalifikované potvrzení elektronických atributů po počátečním vydání zneplatněno, ztrácí okamžikem zneplatnění platnost a jeho status se nemůže v žádném případě změnit zpět. ***Pouze spoléhající se strany, s nimiž uživatel sdílel tento atribut, mají mít možnost spojit zneplatnění s těmito atributy, a to na základě šifrovacích funkcí.***

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

Článek 45d

Ověřování atributů podle autentických zdrojů

1. Členské státy 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 elektronickými prostředky ***bezplatně*** ověřit autenticitu atributu přímo porovnáním s příslušným autentickým zdrojem na vnitrostátní úrovni nebo prostřednictvím určených zprostředkovatelů uznaných na vnitrostátní úrovni v souladu s ***unijními nebo vnitrostátními právními předpisy***.

1a. Autentické zdroje mohou na žádost uživatele vydat nekvalifikované elektronické potvrzení atributů.

2. ***Do ... [6 měsíců od vstupu tohoto pozměňujícího nařízení v platnost]*** a s přihlédnutím k příslušným mezinárodním normám stanoví Komise prostřednictvím ***prováděcích aktů*** 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 kvalifikované elektronické potvrzení atributů. ***Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.***

Článek 45e

Vydávání elektronických potvrzení atributů evropským peněženkám digitální identity

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

1a. Veřejné rejstříky vydají uživateli evropské peněženky digitální identity na jeho žádost kvalifikované elektronické potvrzení atributů.

1b. Nekvalifikované potvrzení atributů může vydat kterýkoli poskytovatel důvěryhodných služeb, autentický zdroj nebo přímo evropská peněženka digitální identity.

1c. Poskytovatelé elektronických potvrzení atributů usazení v jiném členském státě, než je členský stát, který vydal a spravuje evropskou peněženku digitální identity uživatele, poskytnou tomuto uživateli možnost požadovat, získat, uchovávat a spravovat elektronické potvrzení atributů jednoduchým způsobem a bez dalších technických, správních nebo procedurálních požadavků na evropskou peněženku digitální identity vydanou a spravovanou členským státem původu.

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.

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

3. Osobní údaje týkající se poskytování kvalifikovaných služeb elektronického potvrzování atributů jsou uchovávány fyzicky a logicky odděleně od jakýchkoli jiných uchovávaných údajů.

4. Poskytovatelé kvalifikovaných služeb elektronického potvrzování atributů poskytují tyto služby v rámci samostatného právního subjektu.

ODDÍL 10

KVALIFIKOVANÉ SLUŽBY ELEKTRONICKÉ ARCHIVACE

Článek 45fa

Právní účinek služby elektronické archivace

1. Právní účinek a přípustnost údajů a dokumentů archivovaných prostřednictvím služby elektronické archivace jako právních důkazů nesmí být odmítnuty pouze z toho důvodu, že tato služba je v elektronické podobě nebo nesplňuje požadavky na kvalifikovanou službu elektronické archivace.

2. Na údaje a dokumenty archivované pomocí kvalifikované služby elektronické archivace se vztahuje domněnka týkající se integrity archivovaných údajů a dokumentů, jejich dostupnosti, sledovatelnosti, přesnosti a původu, jakož i identifikace uživatelů.

Článek 45g

Kvalifikované služby elektronické archivace

Kvalifikovanou službu elektronické archivace elektronických dokumentů může poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který používá postupy a technologie***, jež jsou s to zajistit splnění všech požadavků na kvalifikované služby elektronické archivace.***

Do *24* měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro služby elektronické archivace. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 45ga

Požadavky na kvalifikované služby elektronické archivace

1. Kvalifikované služby elektronické archivace musí splňovat tyto požadavky:

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

b) zaručují integritu, přesnost původu a právní znaky po celou dobu uchovávání;

c) zajišťují přesnost data a času procesu archivace;

2. Pokud služba elektronické archivace vyhovuje normám uvedeným v odstavci 3, předpokládá se shoda s požadavky stanovenými v odstavci 1.

3. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro postupy přijímání, ukládání, mazání a přenosu elektronických dat nebo dokumentů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

39a) vkládají se nové články, které znějí:

„Článek 46a

Vnitrostátní příslušné orgány a jednotné kontaktní místo

1. Každý členský stát zřídí jeden nebo více nových vnitrostátních příslušných orgánů, které budou plnit úkoly svěřené jim podle článku 46b, nebo k tomuto účelu určí již existující orgán.

2. Každý členský stát určí jedno vnitrostátní jednotné kontaktní místo pro evropský rámec digitální identity (jednotné kontaktní místo). Určí-li členský stát pouze jeden příslušný orgán, je tento orgán rovněž jednotným kontaktním místem pro tento členský stát.

3. Každé jednotné kontaktní místo plní styčnou funkci pro účely přeshraniční spolupráce mezi příslušnými orgánu svého členského státu a příslušnými orgány v jiných členských státech, a případně s Komisí a s agenturou ENISA, a rovněž pro účely meziodvětvové spolupráce s jinými příslušnými orgány na vnitrostátní úrovni.

4. Členské státy zajistí, aby příslušné orgány podle odstavce 1 disponovaly nezbytnými pravomocemi a odpovídajícími zdroji pro účinné a účelné plnění úkolů jim svěřených, a tím pro splnění cílů tohoto nařízení. Členské státy zajistí, aby jimi jmenovaní zástupci v Evropské radě pro digitální identitu zřízené v souladu s článkem 46c účelně, účinně a spolehlivě spolupracovali.

5. Členské státy bez zbytečného odkladu oznámí Komisi zřízení nebo určení příslušného orgánu podle odstavce 1. Rovněž zveřejní a oznámí Komisi totožnost a úkoly jednotného kontaktního místa určeného v souladu s odstavcem 2 a případné následné změny. Komise zveřejní seznam těchto jednotných kontaktních míst.

Článek 46b

Úkoly příslušných vnitrostátních orgánů

1. Příslušné vnitrostátní orgány plní tyto úkoly:

a) monitorují a vymáhají uplatňování tohoto nařízení;

b) vykonávají dohled nad vydavateli evropských peněženek digitální identity usazenými na jejich území prostřednictvím činností předběžného a následného dohledu a zajišťují, aby vydavatelé evropských peněženek digitální identity splňovali požadavky stanovené v tomto nařízení, a přijímají nápravná opatření, pokud tomu tak není;

c) dohlížejí na údajně protiprávní nebo nevhodné jednání spoléhajících se stran usazených na jejich území, zejména pokud bylo takové chování nahlášeno prostřednictvím evropských peněženek digitální identity, a v případě potřeby uplatňují nápravná opatření;

d) vykonávají dohled nad kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými na území členského státu, který provedl

určení, prostřednictvím činností předběžného a následného dohledu, aby tito kvalifikovaní poskytovatelé služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru splňovali požadavky stanovené v tomto nařízení;

e) prostřednictvím činností následného dohledu přijímají v případě potřeby opatření ve vztahu k nekvalifikovaným poskytovatelům služeb vytvářejících důvěru usazeným na území členského státu, který provedl určení, pokud mají k dispozici informace o tom, že tito nekvalifikovaní poskytovatelé služeb vytvářejících důvěru nebo jimi poskytované služby vytvářející důvěru nesplňují požadavky stanovené v tomto nařízení;

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

g) informují příslušné vnitrostátní orgány dotčených členských států určené podle směrnice (EU) XXXX/XXXX [o bezpečnosti sítí a informací 2] o veškerých závažných případech narušení bezpečnosti nebo ztráty integrity, o nichž se dozvědí při plnění svých úkolů, a v případě, že se závažné narušení bezpečnosti nebo ztráta integrity týká jiných členských států, informují jednotné kontaktní místo dotčeného členského státu určené podle směrnice (EU) XXXX/XXXX (o bezpečnosti sítí a informací 2);

h) podávají Komisi zprávy o svých hlavních činnostech v souladu s odstavcem 2;

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

j) spolupracují s dozorovými úřady zřízenými podle nařízení (EU) 2016/679, zejména tím, že je bez zbytečného odkladu informují o výsledcích auditů kvalifikovaných poskytovatelů služeb vytvářejících důvěru, jestliže bylo prokázáno, že byla porušena pravidla týkající se ochrany osobních údajů, a o porušeních bezpečnosti, která mohou představovat porušení ochrany osobních údajů, nebo o podezření na

taková porušení, o nichž se dozvědí při plnění svých úkolů, aniž by bylo dotčeno nařízení (EU) 2016/679;

k) v souladu s články 20 a 21 udělují poskytovatelům služeb vytvářejících důvěru a jimi poskytovaným službám status kvalifikovaného poskytovatele nebo kvalifikované služby a odnímají tento status;

l) informují subjekt odpovědný za vnitrostátní důvěryhodný seznam podle čl. 22 odst. 3 o svých rozhodnutích udělit nebo odejmout status kvalifikovaného poskytovatele nebo kvalifikované služby, pokud tento subjekt není rovněž příslušným vnitrostátním orgánem;

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

n) požadují, aby poskytovatelé služeb vytvářejících důvěru a vydavatelé Evropských peněženek digitální identity napravili případné neplnění požadavků stanovených v tomto nařízení;

o) spolupracují s ostatními příslušnými vnitrostátními orgány a poskytují jim pomoc v souladu s článkem 46c.

2. Do 31. března každého roku předloží každý příslušný vnitrostátní orgán Komisi zprávu o svých hlavních činnostech v předchozím kalendářním roce.

3. Komise poskytuje každoroční zprávy uvedené v odstavci 2 Evropskému parlamentu a Radě a zveřejňuje je.

4. Do … [12 měsíců od data vstupu tohoto pozměňujícího nařízení v platnost] určí Komise prostřednictvím prováděcích aktů formáty a postupy pro účely zprávy uvedené v odst. 1 písm. h) tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

5. Do … [12 měsíců od vstupu tohoto pozměňujícího nařízení v platnost] Komise přijme prováděcí akt v souladu s článkem 47, který doplní toto nařízení dalším určením úkolů příslušných vnitrostátních orgánů uvedených v odstavci 1.

Článek 46c

Evropská rada pro rámec pro digitální identitu

1. *Zřizuje se Evropská rada pro rámec pro digitální identitu (European Digital Identity Framework Board, dále jen „EDIFB“).*
2. *EDIFB je tvořena zástupci příslušných vnitrostátních orgánů a Komise.*
3. *K účasti na zasedáních EDIFB a na její činnosti mohou být pozvány zúčastněné strany a relevantní třetí strany.*
4. *Pokud se projednávají otázky týkající se kybernetických hrozeb, oznamování narušení, certifikátů nebo norem kybernetické bezpečnosti nebo jiné otázky týkající se bezpečnosti, je k účasti pozvána agentura ENISA.*
5. *EDIFB plní tyto úkoly:*
   a) *pomáhat Komisi při přípravě legislativních návrhů a politických iniciativ v oblasti digitálních peněženek, prostředků elektronické identifikace a služeb vytvářejících důvěru;*
   b) *pomáhat Komisi při přípravě prováděcích aktů a aktů v přenesené pravomoci podle tohoto nařízení a spolupracovat s ní;*
   c) *podporovat důsledné uplatňování tohoto nařízení za účelem:*
      i) *výměny osvědčených postupů a informací týkajících se uplatňování ustanovení tohoto nařízení;*
      ii) *posuzovat příslušný vývoj v oblasti evropských peněženek digitální identity, elektronické identifikace a služeb vytvářejících důvěru;*
      iii) *pravidelně pořádat společná setkání s příslušnými zainteresovanými stranami z celé Unie za účelem projednávání činností EDIFB a shromažďování poznatků o nových výzvách v dané oblasti;*
      iv) *vydávat společné pokyny k provádění nařízení;*
      v) *za podpory agentury ENISA vyměňovat informace, zkušenosti a osvědčené postupy, pokud jde o všechny aspekty kybernetické*

bezpečnosti evropské peněženky digitální identity, systémů elektronické identifikace a služeb vytvářejících důvěru;

vi) příslušné vnitrostátní orgány podle tohoto nařízení a příslušné vnitrostátní orgány podle směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX [NIS2] spolupracují s cílem zajistit pokračování stávajících postupů a navázat na znalosti a zkušenosti získané při uplatňování nařízení eIDAS. Kromě toho spolupracují s cílem zajistit jednotné provádění směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX [NIS2];

vii) poskytovat pokyny v souvislosti s vývojem a prováděním politik pro oznamování narušení, koordinované zveřejňování zranitelných míst a společná opatření podle článků 10 a 10a;

viii) zajišťování výměny osvědčených postupů a informací v souvislosti s opatřeními tohoto nařízení a směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX [NIS2] v oblasti kybernetické bezpečnosti, pokud jde o služby vytvářející důvěru, v souvislosti s kybernetickými hrozbami, incidenty, zranitelností, iniciativami na zvyšování povědomí, školeními, cvičeními a dovednostmi, budováním kapacit, kapacitami norem a technických specifikací, jakož i normami a technickými specifikacemi;

ix) provádí koordinované hodnocení bezpečnostních rizik ve spolupráci s agenturou ENISA;

x) provádí vzájemné hodnocení systémů elektronické identifikace, na něž se vztahuje toto nařízení.

6. V rámci EDIFB mohou členské státy požádat o vzájemnou pomoc:

a) po obdržení odůvodněné žádosti příslušného vnitrostátního orgánu poskytne EDIFB tomuto příslušnému vnitrostátnímu orgánu pomoc, aby mohla být provedena jednotným způsobem, což se může týkat zejména žádostí o informace a opatření v oblasti dohledu, jako jsou žádosti o provedení inspekcí souvisejících se zprávami o posouzení

shody podle článků 20 a 21 týkajících se poskytování služeb vytvářejících důvěru;

b) v případě potřeby mohou členské státy pověřit své příslušné vnitrostátní orgány, aby prováděly společná vyšetřování, do nichž jsou zapojeni pracovníci příslušného vnitrostátního orgánu jiného členského státu. Ujednání a postupy pro tyto společné akce schválí a zavedou dotčené členské státy v souladu se svými vnitrostátními právními předpisy.

7. Do … [6 měsíců od data vstupu tohoto pozměňujícího nařízení v platnost] a poté každé dva roky vypracuje EDIFB pracovní program týkající se akcí, jež budou realizovány za účelem plnění stanovených cílů a úkolů.

8. Komise může přijmout prováděcí akty, kterými stanoví procesní pravidla nezbytná pro fungování EDIFB. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;

39b) Článek 47 se mění takto:

a) odstavce 3 a 3 se nahrazují tímto:

„2. Pravomoc přijímat akty v přenesené pravomoci uvedená v ***čl. 6a odst. 11a, čl. 6c odst. 6, čl. 24 odst. 1a a 6, čl. 30 odst. 4 a čl. 46b odst. 5*** je svěřena Komisi na dobu neurčitou od 17. září 2014.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené ***čl. 6a odst. 11a, čl. 6c odst. 6, čl. 24 odst. 1a a 6, čl. 30 odst. 4 a čl. 46b odst. 5*** kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v Úředním věstníku Evropské unie nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.“;

b) odstavec 5 se nahrazuje tímto:

„5. Akt v přenesené pravomoci přijatý podle ***čl. 6a odst. 11a, čl. 6c odst. 6, čl. 24 odst. 1a a 6, čl. 30 odst. 4 a čl. 46b odst. 5*** vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen,

nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.“;

40) Vkládá se nový článek ▌, který zní:

„Článek 48a

Požadavky týkající se podávání zpráv

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

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***, a počet případů zamítnutí žádosti poskytovatele služeb, který se chce stát spoléhající stranou, a důvody zamítnutí;***

ba) počet stížností uživatelů a počet incidentů týkajících se ochrany spotřebitelů a údajů ve vztahu k třetím stranám a kvalifikovaným službám vytvářejícím důvěru;

c) ***druh a počet*** incidentů a výpadků infrastruktury na vnitrostátní úrovni, které brání používání ***evropské peněženky digitální identity;***

ca) druh a počet bezpečnostních incidentů, podezření na narušení bezpečnosti údajů a dotčení uživatelé evropské peněženky digitální identity nebo kvalifikované služby vytvářející důvěru;

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

4. Do 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 ... [24 měsíců od data vstupu tohoto pozměňujícího nařízení]*** v platnost přezkoumá Komise uplatňování tohoto nařízení a podá zprávu Evropskému parlamentu a Radě. Komise zejména vyhodnotí, zda je s přihlédnutím ke zkušenostem s uplatňováním tohoto nařízení a k technologickému, tržnímu a právnímu vývoji vhodné upravit oblast působnosti tohoto nařízení nebo jeho konkrétní ustanovení. V případě potřeby se ke zprávě přiloží návrh na změnu tohoto nařízení.

2. Hodnotící zpráva zahrnuje posouzení dostupnosti, ***bezpečnosti*** a použitelnosti prostředků pro identifikaci, včetně evropských peněženek digitální identity, které spadají do oblasti působnosti tohoto nařízení, a posuzuje, zda by všichni soukromí poskytovatelé on-line služeb využívající pro autentizaci uživatelů služby elektronické identifikace třetích stran měli být povinni k přijímání oznámených prostředků pro elektronickou identifikaci ***a 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 [datum – Úř. věst., vložit období čtyř let 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 [datum – PO, vložit období čtyř let po vstupu tohoto nařízení v platnost].“;

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 2

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 ...

Za Evropský parlament	*Za Radu*
předsedkyně	*předseda*

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;

ia) údaj ve strojově čitelném formátu uvádějící, která z metod ověření totožnosti uvedených v čl. 1 odst. 24 byla použita při vydávání 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:

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) oprávněná podepisující osoba měla 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;

ia) údaj ve strojově čitelném formátu uvádějící, která z metod ověření totožnosti uvedených v čl. 24 odst. 1 byla použita při vydávání pečeti;“.

Příloha IV

Příloha IV se mění takto:

1) ***písmeno c) se nahrazuje tímto:***

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

ca) v případě právnických osob: alespoň název právnické osoby, jíž byl certifikát vydán, a případně registrační číslo uvedené v úředních záznamech s vysokou mírou jistoty;“;

2) Písmeno j) se nahrazuje tímto:

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

Příloha V

POŽADAVKY NA KVALIFIKOVANÉ ELEKTRONICKÉ POTVRZENÍ ATRIBUTŮ

Kvalifikované elektronické potvrzení atributů obsahuje:

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

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

- v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech,

- v případě fyzické osoby: jméno osoby;

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

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

e) označení začátku a konce doby platnosti potvrzení;

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

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

h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene f);

i) 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 právními předpisy Unie nebo*** vnitrostátními právními předpisy ▌, pokud se tyto atributy spoléhají na autentické zdroje v rámci veřejného sektoru, ověřit autenticitu následujících atributů:

1. Adresa;

2. Datum narození;

3. Pohlaví;

4. Osobní stav;

5. Složení rodiny;

6. Státní příslušnost nebo příslušnosti;

6a. ***Občanství;***

7. Vzdělání, tituly a licence;

8. Odborná kvalifikace, tituly a licence;

8a. ***Doklady prokazující aktivaci režimu ochrany a jméno pověřené osoby určené k jednání jménem fyzické osoby;***

9. Veřejná povolení a licence;

10. ***Údaje*** o společnosti.