

Brusel 3. června 2021
(OR. en)

9471/21

**Interinstitucionální spis:
2021/0136(COD)**

**TELECOM 242
COMPET 457
MI 432
DATAPROTECT 156
JAI 670
IA 108
CODEC 826**

NÁVRH

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	3. června 2021
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	COM(2021) 281 final
Předmět:	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu

Delegace naleznou v příloze dokument COM(2021) 281 final.

Příloha: COM(2021) 281 final



EVROPSKÁ
KOMISE

V Bruselu dne 3.6.2021
COM(2021) 281 final

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**

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Tato důvodová zpráva je připojena k návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (dále jen „nařízení eIDAS“)¹. Právní nástroj má za cíl pro přeshraniční užití:

- poskytovat přístup k vysoce zabezpečeným a důvěryhodným řešením v oblasti elektronické identity,
- zajistit, aby se veřejné a soukromé služby mohly spoléhat na důvěryhodná a zabezpečená řešení v oblasti digitální identity,
- zajistit, aby fyzické a právní osoby byly motivovány k používání řešení v oblasti digitální identity,
- zajistit, aby tato řešení byla spojena s řadou atributů a umožňovala cílené sdílení údajů o totožnosti omezených na potřeby konkrétní požadované služby,
- poskytovat přijetí kvalifikovaných služeb vytvářejících důvěru v EU a rovné podmínky pro jejich poskytování.

Na trhu vzniká nové prostředí, kde se pozornost přesunuje z poskytování a používání nepružných digitálních identit na poskytování zvláštních atributů souvisejících s těmito identitami a na spoléhání se na ně. Zvyšuje se poptávka po řešeních v oblasti elektronické identity, která jsou schopná toto zajistit a jež povedou ke zvýšení efektivity a vysoké úrovně důvěry v celé EU, a to jak v soukromém, tak ve veřejném sektoru, a které vycházejí z potřeby identifikovat a autentizovat uživatele s vysokou úrovní záruky.

Hodnocení nařízení eIDAS² ukázalo, že stávající nařízení tyto nové požadavky trhu neřeší, a to zejména kvůli jeho přirozeným omezením na veřejný sektor, omezeným možnostem a složitosti připojení soukromých poskytovatelů on-line služeb k systému, nedostatečné dostupnosti oznámených řešení elektronické identifikace ve všech členských státech a nedostatečné pružnosti při podpoře různých případů použití. Kromě toho řešení v oblasti identity, která nespádají do oblasti působnosti nařízení eIDAS, jako jsou řešení nabízená poskytovateli sociálních médií a finančními institucemi, vyvolávají obavy o ochranu soukromí a údajů. Nemohou účinně reagovat na nové požadavky trhu a postrádají přeshraniční dosah, aby byla schopná řešit zvláštní odvětvové potřeby v případech, kdy je identifikace citlivá a vyžaduje vysoký stupeň jistoty.

Od vstupu části nařízení o elektronické identifikaci v platnost v září 2018 oznámilo alespoň jeden systém elektronické identifikace pouze čtrnáct členských států. V důsledku toho má pouze 59 % obyvatel EU přístup k důvěryhodným a bezpečným přeshraničním systémům elektronické identifikace. Pouze sedm systémů je zcela mobilních a reaguje na současná očekávání uživatelů. Vzhledem k tomu, že ne všechny technické uzly zajišťující propojení s rámcem interoperability eIDAS jsou plně funkční, je přeshraniční přístup omezen;

¹ Úř. věst. L 257/73, 28.8.2014.

² [po přijetí přidat odkaz]

prostřednictvím sítě eIDAS je přeshraničně dostupných jen velmi málo on-line veřejných služeb, které jsou dostupné vnitrostátně.

Nabídnutím evropského rámce digitální identity založeného na revizi stávajícího rámce by alespoň 80 % občanů mělo mít do roku 2030 možnost využívat k přístupu ke klíčovým veřejným službám řešení v oblasti digitální identifikace. Kromě toho by bezpečnost a kontrola poskytované evropským rámcem digitální identity měly občanům a obyvatelům poskytnout plnou důvěru v to, že evropský rámec digitální identity poskytne všem prostředky ke kontrole toho, kdo má přístup ke svému digitálnímu dvojčeti a k jakým přesně údajům. To bude rovněž vyžadovat vysokou úroveň bezpečnosti, pokud jde o všechny aspekty poskytování digitální identity, včetně vydávání evropské peněženky digitální identity, a infrastruktury pro shromažďování, uchovávání a sdělování údajů o digitální identitě.

Současný rámec eIDAS se dále nevztahuje na poskytování elektronických atributů, jako jsou lékařská osvědčení nebo odborné kvalifikace, což ztěžuje celoevropské právní uznávání těchto pověření v elektronické podobě. Nařízení eIDAS navíc neumožňuje uživatelům omezit sdílení údajů o totožnosti na to, co je nezbytně nutné pro poskytování služby.

I když hodnocení nařízení eIDAS ukazuje, že rámec pro poskytování služeb vytvářejících důvěru byl spíše úspěšný, přičemž poskytoval vysokou úroveň důvěry a zajišťoval přijímání a využívání většiny služeb vytvářejících důvěru, pro dosažení úplné harmonizace a přijetí je třeba učinit více. Co se týče kvalifikovaných certifikátů pro autentizaci internetových stránek, musí mít občané možnost se na ně spolehnout a těžit z bezpečných a důvěryhodných informací o tom, kdo za internetovými stránkami stojí, čímž se omezí podvody.

V reakci na dynamiku trhů a technologický vývoj tento návrh dále rozšiřuje stávající seznam služeb vytvářejících důvěru v rámci eIDAS o tři nové kvalifikované služby vytvářející důvěru, a to poskytování služeb elektronické archivace, elektronických účetních knih a správu prostředků pro dálkové vytváření elektronických podpisů a pečeti.

Tento návrh rovněž nabízí harmonizovaný přístup k bezpečnosti pro občany, kteří se spoléhají na evropskou digitální identitu, jež je zastupuje on-line, a pro poskytovatele on-line služeb, kteří se budou moci plně spolehnout na řešení v oblasti digitální identity a přijmout je nezávisle na tom, kde byla vydána. Tento návrh znamená posun pro vydavatele řešení v oblasti evropské digitální identity a poskytuje společnou technickou architekturu, referenční rámec a společné normy, které mají být vypracovány ve spolupráci s členskými státy. Harmonizovaný přístup je nezbytný, aby se zabránilo tomu, že vývoj nových řešení v oblasti digitální identity v členských státech způsobí další roztržičnost vyvolanou používáním odlišných vnitrostátních řešení. Harmonizovaný přístup rovněž posílí jednotný trh, neboť umožní občanům, dalším rezidentům a podnikům identifikovat se v on-line prostředí bezpečným, pohodlným a jednotným způsobem v celé EU, pokud jde o přístup k veřejným i soukromým službám. Uživatelé by se mohli spolehnout na zdokonalený ekosystém pro elektronickou identitu a služby vytvářející důvěru uznávané a přijímané všude v Unii.

S cílem zabránit roztržičnosti a překážkám způsobeným rozdílnými normami Komise přijme doporučení současně s tímto návrhem. Toto doporučení stanoví postup na podporu společného přístupu, který členskými státy a dalším příslušným zúčastněným stranám z veřejného a soukromého sektoru umožní v úzké koordinaci s Komisí pracovat na vytvoření sady nástrojů s cílem vyhnout se rozdílným přístupům a zabránit ohrožení budoucího provádění evropského rámce digitální identity.

- **Soulad s platnými předpisy v této oblasti politiky**

Tento návrh vychází ze současného nařízení eIDAS, z úlohy členských států jako poskytovatelů právní identity a z rámce pro poskytování elektronických služeb vytvářejících důvěru v Evropské unii. Návrh doplňuje ostatní nástroje politiky na úrovni EU, jejichž cílem je převést výhody vnitřního trhu do digitálního světa, zejména zvyšováním možností občanů získat přístup k přeshraničním službám, a je s těmito nástroji plně v souladu. V tomto ohledu návrh provádí politický mandát udělený Evropskou radou³ a předsedkyní Evropské komise⁴, který poskytuje celoevropský rámec pro veřejnou elektronickou identitu, jenž zajistí, aby všichni občané či obyvatelé měli přístup k bezpečné evropské elektronické identitě, kterou lze použít kdekoli v EU k identifikaci a autentizaci pro přístup ke službám ve veřejném a soukromém sektoru, což občanům umožní kontrolovat, jaké údaje jsou sdělovány a jak jsou využívány.

- **Soulad s ostatními politikami Unie**

Návrh je v souladu s prioritami digitální transformace stanovenými ve strategii Formování digitální budoucnosti Evropy⁵ a podpoří dosažení cílů uvedených ve sdělení „Digitální dekáda“⁶. Veškeré zpracovávání osobních údajů podle tohoto nařízení by mělo být prováděno v plném souladu s obecným nařízením o ochraně osobních údajů (dále jen „nařízení GDPR“)⁷. Toto nařízení navíc zavádí zvláštní ochranná opatření na ochranu údajů.

V zájmu zajištění vysoké úrovně bezpečnosti je návrh rovněž v souladu s politikami Unie týkajícími se kybernetické bezpečnosti⁸. Návrh byl vypracován tak, aby snížil roztržitost při uplatňování obecných požadavků na kybernetickou bezpečnost na poskytovatele služeb vytvářejících důvěru, kteří jsou regulováni nařízením eIDAS.

Tento návrh je navíc v souladu s ostatními odvětvovými politikami, které se opírají o používání elektronických identit, elektronických potvrzení atributů a dalších služeb vytvářejících důvěru. Patří sem nařízení o jednotné digitální bráně⁹, požadavky, které musí být splněny ve finančním sektoru v souvislosti s bojem proti praní peněz a proti financování terorismu, iniciativy na sdílení údajů o sociálním zabezpečení, digitálního řidičského průkazu nebo budoucích digitálních cestovních dokladů, a další iniciativy zaměřené na snížení administrativní zátěže pro občany a podniky, které plně spoléhají na možnosti, jež digitální transformace nabízí ve veřejném i soukromém sektoru. Peněžanka dále umožní kvalifikované elektronické podpisy, které mohou usnadnit politickou účast¹⁰.

³ <https://www.consilium.europa.eu/media/45913/021020-euco-final-conclusions-cs.pdf>

⁴ Projev o stavu Unie ze dne 16. září 2020, viz https://ec.europa.eu/commission/presscorner/detail/cs/SPEECH_20_1655

⁵ Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Formování digitální budoucnosti Evropy.

⁶ Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Digitální kompas 2030: Evropské pojetí digitální dekády.

⁷ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Úř. věst. L 119, 4.5.2016, s. 1).

⁸ https://ec.europa.eu/commission/presscorner/detail/cs/IP_20_2391

⁹ Nařízení Evropského parlamentu a Rady (EU) 2018/1724 ze dne 2. října 2018, kterým se zřizuje jednotná digitální brána pro poskytování přístupu k informacím, postupům a k asistenčním službám a službám pro řešení problémů (Úř. věst. L 295, 21.11.2018, s. 1).

¹⁰ Akční plán pro evropskou demokracii, COM/2020/790 final.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Cílem této iniciativy je podpořit transformaci Unie směrem k jednotnému digitálnímu trhu. S rostoucí digitalizací přeshraničních veřejných a soukromých služeb, které využívají řešení v oblasti digitální identity, existuje riziko, že v současném právním rámci budou občané i nadále čelit překážkám a nebudou schopni plně využívat on-line služeb v celé EU a chránit své soukromí. Existuje také riziko, že nedostatky současného právního rámce pro služby vytvářející důvěru by zvýšily roztržičnost a snížily důvěru, pokud by byly ponechány na členských státech. Jako příslušný právní základ této iniciativy je proto určen článek 114 SFEU.

• Subsidiarita (v případě nevýlučné pravomoci)

Občané a podniky by měli mít prospěch z dostupnosti vysoce bezpečných a důvěryhodných řešení v oblasti digitální identity, která lze použít v celé EU, a z přenositelnosti elektronických potvrzení atributů spojených s identitou. Nedávný technologický vývoj, poptávka na trhu a poptávka uživatelů vyžadují dostupnost uživatelsky přívětivějších přeshraničních řešení, která umožňují přístup k on-line službám v celé EU, což nařízení eIDAS ve své současné podobě nabídnout nemůže.

Uživatelé si také stále více zvykají na globálně dostupná řešení, například při přijímání řešení pro jednotné přihlašování poskytovaného většími platformami sociálních médií pro přístup k on-line službám. Členské státy nemohou samy řešit problémy, které toto přináší s ohledem na tržní sílu velkých poskytovatelů, což vyžaduje interoperabilitu a důvěryhodné elektronické identifikace na úrovni EU. Elektronická potvrzení atributů vydaná a přijatá v jednom členském státě, jako je elektronické zdravotní osvědčení, navíc často nejsou právně uznávána a přijímána v jiných členských státech. To vytváří riziko, že členské státy budou i nadále vyvíjet roztržičná vnitrostátní řešení, která nemohou fungovat přeshraničně.

Co se týče poskytování služeb vytvářejících důvěru, ačkoli jsou do značné míry regulovány a fungují v souladu se stávající právní činností, vnitrostátní postupy rovněž vytvářejí riziko zvýšené roztržičnosti.

Zásah na úrovni EU je v konečném důsledku nejvhodnější k tomu, aby občanům a podnikům poskytl prostředky k přeshraniční identifikaci a k výměně atributů a údajů osobních identit za použití vysoce bezpečných a důvěryhodných řešení v oblasti digitální identity, a to v souladu s pravidly EU v oblasti ochrany údajů. To vyžaduje důvěryhodnou a bezpečnou elektronickou identifikaci a regulační rámec, který je spojí s atributy a údaji na úrovni EU. Jedině zásah na úrovni EU může stanovit harmonizované podmínky, které zajišťují kontrolu uživatelů a přístup k přeshraničním digitálním on-line službám, a rámec interoperability, jenž on-line službám usnadňuje spoléhat se na používání bezpečných řešení v oblasti digitální identity bez ohledu na to, kde v EU byla vydána nebo kde má občan bydliště. Jak se do značné míry odráží v přezkumu nařízení eIDAS, je nepravděpodobné, že by vnitrostátní zásah byl stejně účinný a účelný.

• Proporcionalita

Tato iniciativa je přiměřená sledovaným cílům a poskytuje vhodný nástroj pro stanovení nezbytné struktury interoperability pro vytvoření ekosystému digitální identity EU založeného na právních identitách vydaných členskými státy a na poskytování kvalifikovaných a nekvalifikovaných atributů digitální identity. Jasným způsobem přispívá k cíli zlepšit jednotný digitální trh prostřednictvím harmonizovanějšího právního rámce. Harmonizované evropské peněženky digitální identity, které mají členské státy vydávat na základě společných technických norem, rovněž představují společný přístup EU, z něhož budou mít prospěch uživatelé a strany spoléhající se na dostupnost bezpečných přeshraničních řešení v oblasti elektronické identity. Tato iniciativa se zabývá omezeními současné infrastruktury pro

interoperabilitu v oblasti elektronické identifikace založené na vzájemném uznávání různých vnitrostátních systémů elektronické identifikace. S ohledem na stanovené cíle je tato iniciativa považována za dostatečně přiměřenou a náklady jsou považovány za pravděpodobně úměrné potenciálním přínosům. Navrhované nařízení povede k finančním a administrativním nákladům, které ponесou členské státy jako vydavatelé evropských peněženek digitální identity a poskytovatelé služeb vytvářejících důvěru a on-line služeb. Tyto náklady by však pravděpodobně převážily významné potenciální přínosy pro občany a uživatele vyplývající přímo z nárůstu přeshraničního uznávání a přijímání elektronické identity a služeb atributů.

Nákladům vyplývajícím z vytvoření nových norem pro poskytovatele služeb vytvářejících důvěru a poskytovatele on-line služeb a přizpůsobení se jim se nelze vyhnout, má-li být dosaženo cíle použitelnosti a přístupnosti. Cílem této iniciativy je využít investice, které již členské státy vložily do svých vnitrostátních systémů identity, a navázat na ně. Kromě toho jsou dodatečné náklady, které návrh vytváří, určeny na podporu harmonizace a odůvodněny očekáváním, že z dlouhodobého hlediska sníží administrativní zátěž a náklady na dodržování předpisů. Náklady spojené s přijímáním atributů pro autentizaci digitální identity v regulovaných odvětvích lze rovněž považovat za nezbytné a přiměřené, pokud podporují celkový cíl a poskytují prostředky, kterými regulovaná odvětví mohou plnit právní povinnosti legálně identifikovat uživatele.

- **Volba nástroje**

Volba nařízení jako právního nástroje je odůvodněna potřebou zajistit pro uplatňování evropské digitální identity jednotné podmínky na vnitřním trhu prostřednictvím harmonizovaného rámce, jehož cílem je vytvořit bezproblémovou interoperabilitu a poskytnout evropským občanům a společnostem v celé Unii veřejné a soukromé služby s vysoce bezpečnou a důvěryhodnou elektronickou identifikací.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

- **Hodnocení *ex post* / kontroly účelnosti platných právních předpisů**

V rámci procesu přezkumu vyžadovaného článkem 49 nařízení eIDAS bylo provedeno hodnocení fungování nařízení eIDAS. Hlavním zjištěním hodnocení s ohledem na elektronickou identitu je, že nařízení eIDAS nedosáhlo svého potenciálu. Byl oznámen pouze omezený počet elektronických identifikací, čímž bylo omezeno pokrytí oznámených systémů elektronické identifikace na přibližně 59 % obyvatelstva EU. Přijímání oznámených elektronických identifikací na úrovni členských států i na úrovni poskytovatelů služeb je mimoto omezené. Rovněž se zdá, že pouze několik služeb přístupných prostřednictvím vnitrostátní elektronické identifikace je připojeno k vnitrostátní infrastruktuře eIDAS. Hodnotící studie také zjistila, že stávající oblast působnosti a zaměření nařízení eIDAS na systémy elektronické identifikace oznámené členskými státy EU a na umožnění přístupu k on-line veřejným službám se jeví jako příliš omezené a nedostatečné. Převážná většina potřeb v oblasti elektronické identity a dálkové autentizace zůstává v soukromém sektoru, zejména v oblastech, jako jsou bankovníctví, telekomunikace a provozovatelé platforem, od nichž zákon vyžaduje, aby ověřovali totožnost svých zákazníků. Přidaná hodnota nařízení eIDAS s ohledem na elektronickou identitu je omezena vzhledem k jeho nízkému pokrytí, přijímání a používání.

Problémy uvedené v tomto návrhu souvisejí s nedostatkem současného rámce eIDAS a se zásadními kontextovými změnami týkajícími se trhů, společenského a technologického vývoje, které vyvolávají potřeby nových uživatelů a trhu.

- **Konzultace se zúčastněnými stranami**

Otevřená veřejná konzultace byla zahájena dne 24. července 2020 a ukončena dne 2. října 2020. Komise obdržela celkem 318 příspěvků. Komise rovněž obdržela 106 odpovědí na cílený průzkum zúčastněných stran. Členské státy rovněž shromáždily stanoviska při různých dvoustranných a mnohostranných setkáních a v rámci průzkumů organizovaných od začátku roku 2020. To zahrnuje zejména průzkum zástupců členských států sítě pro spolupráci v rámci nařízení eIDAS z července a srpna 2020 a různé specializované semináře. Komise rovněž vedla hloubkové rozhovory se zástupci průmyslu a na dvoustranných schůzkách se setkala se zúčastněnými stranami z řad podniků z různých odvětví (např. elektronický obchod, zdravotnictví, finanční služby, telekomunikační operátoři, výrobci zařízení atd.).

Velká většina respondentů v otevřené veřejné konzultaci uvítala vytvoření jednotné a všeobecně přijímané digitální identity založené na právní identitě vydané členskými státy. Členské státy do značné míry podporují potřebu posílit současné nařízení eIDAS, které občanům umožňuje přístup k veřejným i soukromým službám, a uznávají potřebu zřídit službu vytvářející důvěru a umožňující vydávání a přeshraniční používání elektronických potvrzení atributů. Členské státy celkově zdůraznily potřebu vybudovat evropský rámec digitální identity na základě zkušeností a síly vnitrostátních řešení s cílem nalézt synergie a těžit z uskutečněných investic. Mnoho zúčastněných stran poukázalo na to, jak pandemie COVID-19 prokázala hodnotu bezpečné a vzdálené identifikace pro všechny, co se týče přístupu k veřejným a soukromým službám. Pokud jde o služby vytvářející důvěru, většina subjektů souhlasí s tím, že současný rámec je úspěšný, k další harmonizaci některých postupů týkajících se identifikace na dálku a vnitrostátního dohledu však byla zapotřebí určitá dodatečná opatření. Zúčastněné strany s převážně vnitrostátní zákaznickou základnou vyjádřily o přidané hodnotě evropského rámce digitální identity více pochybností.

Peněženky digitální identity vnímá veřejný a soukromý sektor stále více jako nejvhodnější nástroj umožňující uživatelům vybrat si, kdy a s kterým soukromým poskytovatelem služeb sdílet různé atributy, v závislosti na případě užití a bezpečnosti potřebné pro příslušnou transakci. Digitální identity založené na digitálních peněženkách bezpečně uložených na mobilních zařízeních byly identifikovány jako hlavní aktivum v hledání řešení schopného obstát v budoucnosti. Soukromý trh (např. Apple, Google, Thales) i vlády se tímto směrem již ubírají.

- **Sběr a využití výsledků odborných konzultací**

Návrh vychází z informací shromážděných v rámci konzultací se zúčastněnými stranami pro účely posouzení dopadů a hodnotících zpráv nařízení eIDAS s ohledem na povinnosti související s přezkumem stanovené v článku 49 nařízení eIDAS. Se zástupci členských států a odborníky byla zorganizována řada setkání.

- **Posouzení dopadů**

K tomuto návrhu bylo provedeno posouzení dopadů. Dne 19. března 2021 vydal Výbor pro kontrolu regulace negativní stanovisko s několika připomínkami. Po revidovaném opětovném předložení dne 5. května 2021 vydal výbor kladné stanovisko.

Komise zkoumá různé možnosti politiky za účelem dosažení obecného cíle této iniciativy, kterým je zajistit řádné fungování vnitřního trhu, zejména ve vztahu k poskytování a používání vysoce zabezpečených a důvěryhodných řešení v oblasti elektronické identity.

Posouzení dopadů zkoumá základní scénář, možnosti politiky a jejich dopady u tří zvažovaných možností politiky. Každá možnost představuje volbu k politickému zvážení na základě úrovně ambicí. První možnost představuje nízkou úroveň ambicí a soubor opatření, jejichž hlavním cílem je posílit efektivnost a účinnost současného nařízení eIDAS. Zavedením povinného oznamování vnitrostátních elektronických průkazů totožnosti a zefektivněním stávajících nástrojů dostupných k dosažení vzájemného uznávání je první možnost založena na uspokojení potřeb občanů tím, že se spoléhá na dostupnost různých vnitrostátních systémů elektronické identifikace, jejichž cílem je stát se interoperabilními.

Druhá možnost představuje střední úroveň ambicí a jejím cílem je především rozšířit možnosti bezpečné výměny údajů souvisejících s identitou, doplnit vládní elektronické identifikace a podpořit současný posun směrem ke službám v oblasti identity založeným na attributech. Cílem této možnosti by bylo uspokojit poptávku uživatelů a vytvořit novou kvalifikovanou službu vytvářející důvěru pro poskytování elektronických potvrzení atributů spojených s důvěryhodnými zdroji a vymahatelných přeshraničně. Tím by se rozšířila oblast působnosti současného nařízení eIDAS a podpořilo by se co nejvíce případů užití spoléhajících se na potřebu ověřovat atributy identity spojené s osobou s vysokou úrovní záruky.

Třetí a upřednostňovaná možnost představuje nejvyšší úroveň ambicí a jejím cílem je regulovat poskytování vysoce bezpečné osobní peněženky digitální identity vydávané členskými státy. Upřednostňovaná možnost je považována za nejvhodnější k účinnému řešení cílů této iniciativy. Za účelem úplného splnění cílů politiky vychází upřednostňovaná možnost z většiny opatření posuzovaných v rámci možnosti č. 1 (spoléhání se na právní identitu potvrzenou členskými státy a dostupnost vzájemně uznávaných prostředků pro elektronickou identifikaci) a možnosti č. 2 (elektronické potvrzení atributů právně uznávaných přeshraničně).

S ohledem na obecný rámec pro služby vytvářející důvěru úroveň ambicí vyžaduje soubor opatření, která k dosažení cílů politiky nevyžadují postupné kroky.

Nová kvalifikovaná služba vytvářející důvěru pro správu prostředků pro dálkové vytváření elektronických podpisů a pečeti by přinesla značné výhody v oblasti bezpečnosti, jednotnosti, právní jistoty a volby pro spotřebitele, a to jak v souvislosti s certifikací kvalifikovaných prostředků pro vytváření podpisů, tak ve vztahu k požadavkům, které musí kvalifikovaní poskytovatelé služeb vytvářejících důvěru spravující tyto prostředky splňovat. Nová ustanovení by posílila celkový regulační rámec a rámec dohledu pro poskytování služeb vytvářejících důvěru.

Dopady možností politiky na různé kategorie zúčastněných stran jsou podrobně vysvětleny v příloze 3 posouzení dopadů, které tuto iniciativu podporuje. Posouzení je kvantitativní i kvalitativní. Studie posouzení dopadů uvádí, že minimální kvantifikovatelné náklady lze odhadnout na 3,2 miliardy EUR nebo více, jelikož některé nákladové položky nelze kvantifikovat. Celkové vyčíslitelné přínosy byly odhadnuty na 3,9 miliardy EUR až 9,6 miliardy EUR. S ohledem na širší hospodářské dopady se očekává, že upřednostňovaná možnost bude mít pozitivní vliv na inovace, mezinárodní obchod a konkurenceschopnost, přispěje k hospodářskému růstu a povede k dodatečným investicím do řešení v oblasti digitální identity. Například se očekává, že dodatečná investice ve výši 500 milionů EUR vyvolaná legislativními změnami v rámci třetí možnosti přinese po 10 letech přínosy ve výši 1 268 milionů EUR (při 67% přijetí).

Očekává se také, že upřednostňovaná možnost bude mít pozitivní dopad na zaměstnanost a vytvoří 5 000 až 27 000 dodatečných pracovních míst během pěti let po provedení. To lze vysvětlit dodatečnými investicemi a nižšími náklady pro podniky, které se spoléhají na používání řešení v oblasti elektronické identifikace.

Očekává se, že pozitivní dopad na životní prostředí bude největší u třetí možnosti, u níž se očekává maximální zlepšení zavádění a použitelnosti elektronické identifikace, což přinese pozitivní dopady na snižování emisí v souvislosti s poskytováním veřejných služeb.

Elektronické účetní knihy poskytují uživatelům důkaz a neměnnou auditní stopu pro určování pořadí transakcí a datových záznamů, čímž zajišťují integritu údajů. Ačkoli tato služba vytvářející důvěru nebyla součástí posouzení dopadů, staví na stávajících službách vytvářejících důvěru, jelikož kombinuje časové razítkování údajů a určování jejich pořadí s jistotou ohledně původce údajů, což je podobné elektronickému podpisu. Tato služba vytvářející důvěru je nezbytná k zabránění roztržitému vnitřnímu trhu vymezením jednotného celoevropského rámce, který umožní přeshraniční uznávání služeb vytvářejících důvěru a podporujících fungování kvalifikovaných elektronických účetních knih. Integrita údajů je zase velmi důležitá pro shromažďování údajů z decentralizovaných zdrojů, pro samostatná řešení v oblasti identity, pro připisování vlastnictví digitálním aktivům, pro zaznamenávání obchodních procesů za účelem ověření dodržování kritérií udržitelnosti a pro různé případy použití na kapitálových trzích.

- **Účelnost právních předpisů a zjednodušení**

Tento návrh stanoví opatření, která se budou vztahovat na veřejné orgány, občany a poskytovatele on-line služeb. Pro orgány veřejné správy sníží administrativní náklady a náklady na dodržování předpisů a provozní náklady a pro poskytovatele on-line služeb sníží výdaje související s bezpečností. Občané budou mít prospěch z úspor plynoucích ze snížené administrativní zátěže, přičemž se budou plně spoléhat na digitální prostředky k identifikaci a možnost bezpečné přeshraniční výměny atributů digitální identity se stejnou právní hodnotou. Z úspor nákladů na dodržování předpisů budou mít rovněž prospěch poskytovatelé elektronické identity.

- **Základní práva**

Jelikož osobní údaje spadají do oblasti působnosti některých prvků nařízení, jsou opatření navržena tak, aby byla plně v souladu s právními předpisy o ochraně údajů. Návrh například zlepšuje možnosti sdílení údajů a umožňuje zveřejňování na základě vlastního uvážení. S použitím evropské peněženky digitální identity bude uživatel moci kontrolovat množství údajů poskytnutých spoléhajícím se stranám a bude informován o attributech požadovaných k poskytování konkrétní služby. Poskytovatelé služeb informují členské státy o svém záměru spoléhat se na evropskou peněženku digitální identity, která by členskými státy umožnila kontrolovat, že soubory citlivých údajů, například týkající se zdraví, jsou ze strany poskytovatelů služeb požadovány pouze v souladu s vnitrostátními právními předpisy.

4. ROZPOČTOVÉ DŮSLEDKY

K optimálnímu dosažení cílů této iniciativy je nezbytné financovat řadu akcí jak na úrovni Komise, kde se v období 2022–2027 předpokládá přidělení přibližně 60 plných pracovních úvazků, tak na úrovni členských států formou aktivní účasti v odborných skupinách a výborech spojených s prací iniciativy a složených ze zástupců členských států. Celkové finanční zdroje nezbytné k realizaci návrhu v období 2022–2027 budou činit až 30,825

milionu EUR, z toho 8,825 milionu EUR správních nákladů a až 22 milionů EUR provozních výdajů pokrytých z programu Digitální Evropa (dohoda před uzavřením). Financování přispěje na náklady spojené s údržbou, vývojem, hostingem, provozem a podporou stavebních kamenů elektronické identifikace a služeb vytvářejících důvěru. Může rovněž přispět na granty na propojení služeb s ekosystémem evropské peněženky digitální identity, vývojem a technických specifikací. Financování rovněž podpoří provádění každoročních průzkumů a studií a účinnost a efektivitu nařízení při dosahování jeho cílů. Podrobný přehled souvisejících nákladů je obsažen ve „finančním výkazu“ spojeném s touto iniciativou.

5. OSTATNÍ PRVKY

• Plány provádění a způsoby sledování, hodnocení a podávání zpráv

Dopady budou sledovány a hodnoceny v souladu s pokyny pro zlepšování právní úpravy, které se týkají provádění a uplatňování navrhovaného nařízení. Ujednání týkající se sledování tvoří důležitou součást návrhu, zejména s ohledem na nedostatky současného rámce pro podávání zpráv, jak ukazuje hodnotící studie. Kromě požadavků na podávání zpráv uvedených v navrhovaném nařízení, jejichž cílem je zajistit lepší databázi dat a analýz, bude rámec monitorování sledovat: 1) do jaké míry byly provedeny nezbytné změny v souladu s přijatými opatřeními; 2) zda byly provedeny nezbytné změny příslušných vnitrostátních systémů; 3) zda byly dodrženy nezbytné změny povinností regulovaných subjektů v oblasti dodržování předpisů. Za shromažďování údajů na základě předem stanovených ukazatelů budou odpovědné Evropská komise (1, 2 a 3) a příslušné vnitrostátní orgány (2 a 3).

Co se týče uplatňování navrhovaného nástroje, Evropská komise a příslušné vnitrostátní orgány prostřednictvím každoročních průzkumů posoudí: 1) přístup k prostředkům pro elektronickou identifikaci pro všechny občany EU; 2) přeshraniční uznávání a přijímání systémů elektronické identifikace ve vyšší míře; 3) opatření na podporu přijetí soukromým sektorem a rozvoje nových služeb v oblasti digitální identity.

Evropská komise bude shromažďovat kontextové informace prostřednictvím každoročních průzkumů týkajících se: 1) velikosti trhu s digitální identitou; 2) výdajů na veřejné zakázky spojených s digitální identitou; 3) podílu podniků poskytujících své služby on-line; 4) podílu on-line transakcí vyžadujících silnou identifikaci zákazníka; 5) podílu občanů EU využívajících soukromé a veřejné služby on-line.

• Podrobné vysvětlení konkrétních ustanovení návrhu

Návrh nařízení v článku 6a požaduje, aby členský stát vydal evropskou peněženku digitální identity v rámci oznámeného systému elektronické identifikace podle společných technických norem po povinném posouzení souladu a dobrovolné certifikaci v rámci evropského rámce pro certifikaci kybernetické bezpečnosti, jak stanoví akt o kybernetické bezpečnosti. Návrh obsahuje ustanovení, která zajistí, aby fyzické a právnické osoby měly možnost bezpečně požadovat a získávat, ukládat, kombinovat a používat osobní identifikační údaje a elektronická potvrzení atributů za účelem on-line a offline autentizace a umožnění přístupu ke zboží a veřejným a soukromým službám on-line pod kontrolou uživatele. Tímto osvědčením není dotčeno nařízení GDPR v tom smyslu, že operace zpracování osobních údajů související s evropskou peněženkou digitální identity mohou být certifikovány pouze podle článků 42 a 43 nařízení GDPR.

Návrh obsahuje v článku 6b zvláštní ustanovení o požadavcích na spoléhající se strany, pokud jde o předcházení podvodům, a o zajištění autentizace osobních identifikačních údajů a elektronických potvrzení atributů pocházejících z evropské peněženky digitální identity.

Za účelem zpřístupnění více prostředků pro elektronickou identifikaci pro přeshraniční použití a zlepšení účinnosti procesu vzájemného uznávání oznámených systémů elektronické identifikace se v článku 7 stanoví povinnost oznamovat alespoň jeden systém elektronické identifikace ze strany členských států. Kromě toho se v článku 11a doplňují ustanovení pro usnadnění jedinečné identifikace, aby byla zajištěna jedinečná a trvalá identifikace fyzických osob. Týká se to případů, kdy je identifikace vyžadována právními předpisy, například v oblasti zdraví, v oblasti financí za účelem plnění povinností při boji proti praní peněz nebo pro soudní účely. Za tímto účelem budou členské státy muset do minimálního souboru osobních identifikačních údajů zahrnout jedinečný a trvalý identifikátor. Možnost členských států spoléhat se na certifikaci k zajištění souladu s nařízením, a tím nahradit proces vzájemného hodnocení, zlepšuje účinnost vzájemného uznávání.

Oddíl 3 obsahuje nová ustanovení o přeshraničním spoléhání se na evropskou peněženku digitální identity s cílem zajistit, aby se uživatelé mohli spolehnout na používání evropské peněženky digitální identity k přístupu k on-line službám poskytovaným subjekty veřejného sektoru a soukromými poskytovateli služeb, kteří vyžadují použití silného ověření uživatele.

V kapitole III o službách vytvářejících důvěru se mění článek 14 o mezinárodních aspektech s cílem umožnit Komisi přijímat prováděcí rozhodnutí potvrzující rovnocennost požadavků uplatňovaných na služby vytvářející důvěru, které jsou zřízeny ve třetích zemích, a služeb, které poskytují, kromě používání dohod o vzájemném uznávání v souladu s článkem 218 Smlouvy o fungování EU.

Co se týče obecných ustanovení vztahujících se na služby vytvářející důvěru, včetně kvalifikovaných poskytovatelů služeb vytvářejících důvěru, články 17, 18, 20, 21 a 24 se mění tak, aby byly v souladu s pravidly vztahujícími se na bezpečnost sítí a informací v EU. Pokud jde o metody, které mají kvalifikovaní poskytovatelé služeb vytvářejících důvěru používat k ověření totožnosti fyzických nebo právnických osob, jimž jsou kvalifikované certifikáty vydávány, byla ustanovení o používání prostředků identifikace na dálku harmonizována a vyjasněna, aby se zajistilo uplatňování stejných pravidel v celé EU.

Kapitola III představuje nový článek 29a, který definuje požadavky na kvalifikovanou službu správy prostředků pro vytváření elektronických podpisů na dálku. Nová kvalifikovaná služba vytvářející důvěru by byla přímo propojena a vycházela by z opatření, na která se v posouzení dopadů odkazuje a která jsou v něm posuzována, zejména z opatření týkajících se „harmonizace procesu certifikace pro elektronické podpisy na dálku“ a dalších opatření vyžadujících harmonizaci postupů dohledu ze strany členských států.

Aby bylo zajištěno, že uživatelé mohou zjistit, kdo za internetovými stránkami stojí, mění se článek 45 tak, aby od poskytovatelů internetových prohlížečů požadoval usnadnění používání kvalifikovaných certifikátů pro autentizaci internetových stránek.

Kapitola III představuje tři nové oddíly.

Nový oddíl 9 obsahuje ustanovení o právních účincích elektronických potvrzení atributů, jejich používání ve vymezených odvětvích a požadavcích na kvalifikovaná potvrzení atributů. V zájmu zajištění vysoké úrovně důvěryhodnosti se do článku 45d vkládá ustanovení o ověřování atributů podle autentických zdrojů. Aby se zajistilo, že uživatelé evropské peněženky digitální identity budou mít prospěch z dostupnosti elektronických potvrzení atributů a že tato potvrzení budou vydána evropské peněženke digitální identity, vkládá se do článku 45e požadavek. Článek 45f místo toho obsahuje dodatečná pravidla pro poskytování elektronického potvrzení služeb atributů, včetně ochrany osobních údajů.

Nový oddíl 10 umožňuje poskytování kvalifikovaných služeb v oblasti elektronické archivace na úrovni EU. Článek 45g o kvalifikovaných službách v oblasti elektronické archivace

doplňuje články 34 a 40 o kvalifikovaných službách uchovávání kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečeti.

Nový oddíl 11 stanoví rámec pro služby vytvářející důvěru s ohledem na vytváření a údržbu elektronických účetních knih a kvalifikovaných elektronických účetních knih. Elektronická účetní kniha kombinuje časové razítkování údajů a určování jejich pořadí s jistotou ohledně původce údajů podobnou elektronickému podpisu s dodatečným přínosem, kterým je umožnění decentralizovanější správy, jež je vhodná pro spolupráci více stran. To je důležité pro různé případy použití, které mohou být založeny na elektronických účetních knihách.

Elektronické účetní knihy pomáhají společností šetřit náklady tím, že zvyšují účinnost a bezpečnost mnohostranné koordinace a usnadňují regulační dohled. Pokud evropská regulace chybí, existuje riziko, že vnitrostátní zákonodárci stanoví odlišné vnitrostátní normy. K zabránění roztržtosti je nezbytné vymezit jednotný celoevropský rámec, který umožní přeshraniční uznávání služeb vytvářejících důvěru a podporujících fungování elektronických účetních knih. Tato celoevropská norma pro provozovatele uzlů se bude uplatňovat bez ohledu na ostatní sekundární právní předpisy EU. Používají-li se elektronické účetní knihy na podporu vydávání dluhopisů nebo kryptoaktiv či na obchodování s nimi, měly by tyto případy použití být slučitelné se všemi platnými finančními pravidly, například se směrnicí o trzích finančních nástrojů¹¹, směrnicí o platebních službách¹² a budoucím nařízením o trzích s kryptoaktivy¹³. Pokud se případy použití týkají osobních údajů, poskytovatelé služeb budou muset dodržovat nařízení GDPR.

75 % všech případů použití elektronických účetních knih se v roce 2017 týkalo bankovníctví a financí. Případy použití elektronických účetních knih jsou v současné době stále rozmanitější, přičemž 17 % případů se týká komunikace a médií; 15 % výroby a přírodních zdrojů, 10 % vládního sektoru, 8 % pojišťovnictví, 5 % maloobchodu, 6 % dopravy, 5 % veřejných služeb¹⁴.

Kapitola VI obsahuje nový článek 48b, který má zajistit shromažďování statistik o používání evropské peněženky digitální identity za účelem sledování účinnosti pozměněného nařízení.

¹¹ Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU, text s významem pro EHP, *Úř. věst. L 173, 12.6.2014, s. 349–496*.

¹² Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES, *Úř. věst. L 337, 23.12.2015, s. 35–127*.

¹³ Návrh nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937, COM/2020/593 final.

¹⁴ Gartner, Blockchain Evolution (Evoluce blockchainu), 2020.

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

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

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

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

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru¹⁵,

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

- (1) Sdělení Komise ze dne 19. února 2020 nazvané „Formování digitální budoucnosti Evropy“¹⁶ 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 2020¹⁷ 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.
- (3) Sdělení Komise ze dne 9. března 2021 nazvané „Digitální kompas 2030: Evropské pojetí digitální dekády“¹⁸ stanoví cíl rámce Unie, který do roku 2030 povede k širokému zavedení důvěryhodné identity kontrolované uživatelem, která každému uživateli umožní mít svou komunikaci a přítomnost na internetu pod kontrolou.
- (4) Harmonizovanější přístup k digitální identifikaci by měl snížit rizika a náklady současné rozříštěnosti, jejíž příčinou je používání odlišných vnitrostátních řešení, a posílí jednotný trh tím, že umožní občanům, dalším rezidentům ve smyslu vnitrostátních právních předpisů a podnikům identifikovat se v on-line prostředí v celé Unii pohodlným a jednotným způsobem. Každý by měl mít bezpečný přístup k veřejným a soukromým službám založeným na zdokonaleném ekosystému služeb vytvářejících důvěru a na ověřených dokladech totožnosti a potvrzeních atributů, jako je vysokoškolský titul právně uznávaný a přijímaný všude v Unii. Cílem rámce pro evropskou digitální identitu je dosáhnout přechodu od spoléhání se pouze na

¹⁵ Úř. věst. C, , s .

¹⁶ COM(2020) 67 final.

¹⁷ <https://www.consilium.europa.eu/cs/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/>

¹⁸ COM/2021/118 final/2

vnitrostátní řešení v oblasti digitální identity k poskytování elektronických potvrzení atributů platných na evropské úrovni. Poskytovatelé elektronických potvrzení atributů by měli těžit z jasného a jednotného souboru pravidel a orgány veřejné správy by měly být schopny spolehnout se na elektronické dokumenty v daném formátu.

- (5) S cílem podpořit konkurenceschopnost evropských podniků by měli mít poskytovatelé on-line služeb možnost využívat řešení v oblasti digitální identity uznávaná v celé Unii, bez ohledu na to, 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.
- (6) Zpracovávání osobních údajů při provádění tohoto nařízení se řídí nařízením (EU) 2016/679¹⁹. 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.
- (7) Je nezbytné stanovit harmonizované podmínky pro vytvoření rámce pro evropské peněženky digitální identity vydávané členskými státy, který by měl motivovat všechny občany Unie a ostatní rezidenty ve smyslu vnitrostátních právních předpisů k bezpečnému sdílení údajů týkajících se jejich identity uživatelsky přívětivým a pohodlným způsobem pod výhradní kontrolou uživatele. Technologie používané k dosažení těchto cílů by měly být vyvinuty s cílem dosáhnout nejvyšší úrovně bezpečnosti, pohodlí uživatele a široké použitelnosti. Členské státy by měly všem svým státním příslušníkům a rezidentům zajistit rovný přístup k digitální identifikaci.
- (8) V zájmu zajištění souladu s právem Unie nebo vnitrostátními právními předpisy, jež jsou v souladu s právem Unie, by poskytovatelé služeb měli členským státům sdělit svůj záměr využívat evropské peněženky digitální identity. 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 právem Unie nebo vnitrostátními právními předpisy.
- (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 peněženky 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, 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. Evropské peněženky digitální identity by rovněž měly uživatelům umožnit vytvářet a používat kvalifikované elektronické podpisy a pečete, které jsou přijímány v

¹⁹ 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.

celé EU. V zájmu zjednodušení a snížení nákladů pro osoby a podniky v celé EU, mimo jiné umožněním pravomocí k zastupování a elektronických mandátů, by členské státy měly vydávat evropské peněženky digitální identity založené na společných normách s cílem zajistit bezproblémovou interoperabilitu a vysokou úroveň bezpečnosti. Pouze příslušné orgány členských států mohou při zjišťování totožnosti osoby poskytnout vysoký stupeň spolehlivosti, a tedy poskytnout ujistění, že osoba, která uvádí nebo uplatňuje určitou totožnost, je skutečně osobou, kterou tvrdí, že je. Evropské peněženky digitální identity se proto musí spoléhat na právní identitu občanů, ostatních rezidentů nebo právnických osob. Důvěru v evropské peněženky digitální identity by posílila skutečnost, že vydávající strany jsou povinny zavést vhodná technická a organizační opatření k zajištění úrovně bezpečnosti odpovídající rizikům, která představují pro práva a svobody fyzických osob, v souladu s nařízením (EU) 2016/679.

- (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) 2019/881²⁰. Touto certifikací by neměla být dotčena certifikace týkající se zpracování osobních údajů podle nařízení (ES) 2016/679.
- (11) Evropské peněženky digitální identity by měly zajišťovat nejvyšší úroveň bezpečnosti osobních údajů používaných k autentizaci bez ohledu na to, zda jsou tyto údaje uchovávány lokálně, nebo v rámci řešení založených na cloudu, a to se zohledněním různých úrovní rizika. Jedním ze způsobů identifikace poskytujících vysokou úroveň spolehlivosti je používat k autentizaci biometrické údaje, zejména pokud se používají v kombinaci s jinými autentizačními prvky. Jelikož biometrické údaje představují jedinečné vlastnosti osoby, vyžaduje použití biometrických údajů organizační a bezpečnostní opatření úměrná riziku, které takové zpracování může představovat pro práva a svobody fyzických osob, a v souladu s nařízením 2016/679.
- (12) Aby se zajistilo, že evropský rámec digitální identity bude otevřen inovacím a technologickému rozvoji a obtoží v budoucnosti, měly by být členské státy vybízeny k tomu, aby společně zřizovaly pískoviště pro testování inovativních řešení v kontrolovaném a bezpečném prostředí, zejména za účelem zlepšení funkčnosti, ochrany osobních údajů, bezpečnosti a interoperability řešení a zahrnutí technických odkazů a právních požadavků do budoucích aktualizací. Toto prostředí by mělo podpořit začlenění evropských malých a středních podniků, začínajících podniků a samostatných inovátorů a výzkumných pracovníků.

²⁰ 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.

- (13) Nařízení (EU) č. 2019/1157²¹ posiluje zabezpečení průkazů totožnosti prostřednictvím posílených bezpečnostních prvků do srpna 2021. Členské státy by měly zvážit proveditelnost oznamování v rámci systémů elektronické identifikace s cílem rozšířit přeshraniční dostupnost prostředků pro elektronickou identifikaci.
- (14) Postup oznamování systémů elektronické identifikace by měl být zjednodušen a urychlen s cílem podpořit přístup k pohodlným, důvěryhodným, bezpečným a inovativním řešením v oblasti autentizace a identifikace a případně podpořit soukromé poskytovatele identity, aby orgánům členského státu nabízeli systémy elektronické identifikace k oznamování jako vnitrostátní systémy elektronických průkazů totožnosti podle nařízení 910/2014.
- (15) Zjednodušení stávajících postupů oznamování a vzájemného hodnocení zabráni 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. S cílem dále podporovat použitelnost prostředků pro elektronickou identifikaci by toto nařízení mělo vyžadovat, aby členské státy přijaly zvláštní opatření k zajištění správné shody totožnosti v procesu elektronické identifikace. Za stejným účelem by toto nařízení mělo rovněž rozšířit povinný minimální soubor údajů a vyžadovat používání jedinečného a trvalého elektronického identifikátoru v souladu s právem Unie v případech, kdy je nezbytné uživatele na jeho žádost jedinečným a trvalým způsobem právně identifikovat.
- (18) V souladu se směrnicí (EU) 2019/882²² by osoby se zdravotním postižením měly mít možnost používat evropské peněženky digitální identity, služby vytvářející důvěru a produkty koncových uživatelů používané při poskytování těchto služeb na stejném základě jako ostatní uživatelé.
- (19) Toto nařízení by se nemělo vztahovat na aspekty související s uzavíráním a platností smluv nebo jiných právních povinností, pokud existují požadavky na formu stanovené vnitrostátním právem nebo právem Unie. Neměly by jím být dotčeny ani vnitrostátní

²¹ 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).

²² 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).

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) Toto nařízení by mělo vycházet z aktů Unie zajišťujících spravedlivé trhy otevřené hospodářské soutěži v digitálním odvětví. Zejména vychází z nařízení XXX/XXXX [akt o digitálních trzích], které zavádí pravidla pro poskytovatele hlavních služeb platform určené jako strážci a mimo jiné strážcům zakazuje v souvislosti se službami nabízenými podnikatelskými uživateli využívajícími hlavní služby platform tohoto strážce vyžadovat od podnikatelských uživatelů, aby používali identifikační službu strážce, nabízeli ji nebo s ní komunikovali. Ustanovení čl. 6 odst. 1 písm. f) nařízení XXX/XXXX [akt o digitálních trzích] vyžaduje, aby strážci umožnili podnikatelským uživatelům a poskytovatelům doplňkových služeb přístup ke stejným funkcím operačního systému, hardwaru nebo softwaru, které jsou k dispozici nebo používány při poskytování doplňkových služeb strážcem, a interoperabilitu s nimi. Podle čl. 2 odst. 15 [aktu o digitálních trzích] představují identifikační služby druh doplňkových služeb. Podnikatelští uživatelé a poskytovatelé doplňkových služeb by proto měli mít přístup k takovým funkcím hardwaru nebo softwaru, jako jsou zabezpečené prvky v chytrých telefonech, a měli by s nimi spolupracovat prostřednictvím evropských peněženek digitální identity nebo prostředků pro elektronickou identifikaci označených členskými státy.
- (22) S cílem zefektivnit povinnosti v oblasti kybernetické bezpečnosti uložené poskytovatelům služeb vytvářejících důvěru a umožnit těmto poskytovatelům a jejich příslušným orgánům využívat právní rámec stanovený směrnicí XXXX/XXXX (směrnice 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 tyto 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 XXXX/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.
- (25) Ve většině případů si občané a ostatní rezidenti nemohou informace týkající se jejich totožnosti, jako jsou adresy, věk a odborná kvalifikace, řidičské průkazy a jiná povolení a platební údaje, digitálně přeshraničně vyměňovat bezpečně a s vysokou úrovní ochrany údajů.
- (26) Mělo by být možné vydávat a zpracovávat důvěryhodné digitální atributy a přispívat ke snižování administrativní zátěže, což by občany a ostatní rezidenty motivovalo využívat je 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 něž 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. Společající se strany by měly používat elektronická potvrzení atributů jako rovnocenná potvrzením v tištěné podobě. Elektronickému potvrzení atributů by proto neměly být upírány právní účinky proto, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické potvrzení atributů. Za tímto účelem by měly být stanoveny obecné požadavky, které zajistí, aby kvalifikované elektronické potvrzení atributů mělo rovnocenný právní účinek jako zákonně vydaná potvrzení v tištěné podobě. Tyto požadavky by se však měly uplatňovat, aniž jsou dotčeny právní předpisy Unie nebo vnitrostátní právní předpisy vymezující dodatečné požadavky pro konkrétní odvětví, co se týče formy se základními právními účinky, a zejména případné přeshraniční uznávání kvalifikovaného elektronického potvrzení atributů.

- (28) Široká dostupnost a použitelnost evropských peněženek digitální identity vyžaduje jejich přijetí soukromými poskytovateli služeb. Soukromé spoléhající se strany poskytující služby v oblasti dopravy, energetiky, bankovníctví a finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, vzdělávání nebo telekomunikací by měly akceptovat používání evropských peněženek digitální identity k poskytování služeb, u nichž vnitrostátní právní předpisy nebo právní předpisy Unie či smluvní závazek vyžadují silnou autentizaci uživatele k on-line identifikaci. V případech, kdy velmi rozsáhlé on-line platformy ve smyslu článku 25.1 nařízení [odkaz na nařízení o aktu o digitálních službách] vyžadují, aby se uživatelé 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 peněženku k přístupu k soukromým službám, ale pokud si to přejí, měly by rozsáhlé on-line platformy za tímto účelem evropskou peněženku digitální identity přijmout, přičemž by měla být dodržena zásada minimalizace údajů. Vzhledem k významu velmi rozsáhlých on-line platforem a k jejich dosahu, vyjádřenému zejména počtem příjemců služby a hospodářských transakcí, je 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 rozsáhlé platformy a kteří pro autentizaci uživatelů využívají služby elektronické identifikace třetích stran. Měly by být vypracovány do dvanácti měsíců od přijetí tohoto nařízení. Komise by měla posoudit účinnost těchto ustanovení z hlediska dostupnosti a použitelnosti evropských peněženek digitální identity pro uživatele po 18 měsících od jejich zavedení a na základě tohoto posouzení přezkoumat ustanovení s cílem zajistit jejich přijetí prostřednictvím aktů v přenesené pravomoci.
- (29) Evropská peněženka digitální identity by měla technicky umožnit výběrové sdělování atributů spoléhajícím se stranám. Tento prvek by se měl stát základním konstrukčním prvkem, čímž se posílí pohodlí a ochrana osobních údajů, včetně minimalizace zpracování osobních údajů.
- (30) Atributy poskytované kvalifikovanými poskytovateli služeb vytvářejících důvěru jako součást kvalifikovaného potvrzování atributů by měly být ověřovány na základě autentických zdrojů buď přímo kvalifikovaným poskytovatelem služeb vytvářejících důvěru, nebo prostřednictvím určených zprostředkovatelů uznaných na vnitrostátní úrovni v souladu s vnitrostátními právními předpisy nebo právními předpisy Unie pro účely bezpečné výměny potvrzených atributů mezi poskytovateli služeb v oblasti identifikace nebo potvrzování atributů a spoléhajícími se stranami.
- (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 zahájení transakcí v oblasti platebních služeb.

- (32) Služby autentizace internetových stránek uživatelům poskytují jistotu, že stránky reprezentují skutečný a legitimní subjekt. 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. Měly by 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.
- (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.
- (34) Kvalifikované elektronické účetní knihy zaznamenávají data způsobem, který zajišťuje jedinečnost, autenticitu a správné pořadí dat a který je odolný proti neoprávněným zásahům. Elektronická účetní kniha kombinuje účinek časového razítkování dat s jistotou ohledně původce dat podobnou elektronickému podpisu a má dodatečný přínos, kterým je umožnění decentralizovanějších modelů správy, jež jsou vhodné pro spolupráci více stran. Vytváří například spolehlivou auditní stopu původu komodit v přeshraničním obchodu, podporuje ochranu práv duševního vlastnictví, umožňuje flexibilitu trhů s elektřinou, poskytuje základ pro pokročilá řešení v oblasti samostatné identity a podporuje účinnější a transformativnější veřejné služby. K zabránění roztržetosti vnitřního trhu je nezbytné vymezit jednotný celoevropský právní rámec, který umožní přeshraniční uznávání služeb vytvářejících důvěru pro zaznamenávání údajů do elektronických účetních knih.
- (35) Certifikace kvalifikovaných poskytovatelů služeb vytvářejících důvěru by měla poskytnout právní jistotu pro případy užití založené na elektronických účetních knihách. Tato služba vytvářející důvěru pro elektronické účetní knihy a kvalifikované elektronické účetní knihy a certifikace jako kvalifikovaný poskytovatel služeb vytvářejících důvěru pro elektronické účetní knihy by měly být bez ohledu na potřebu případů užití v souladu s právem Unie nebo vnitrostátními právními předpisy, jež jsou v souladu s právem Unie. Případy užití, které zahrnují zpracování osobních údajů, musí být v souladu s nařízením (EU) 2016/679. Případy užití, které zahrnují kryptoaktiva, by měly být slučitelné se všemi platnými finančními předpisy, například

se směrnicí o trzích finančních nástrojů²³, směrnicí o platebních službách²⁴ a budoucím nařízením o trzích s kryptoaktivy²⁵.

- (36) K tomu, aby se zabránilo roztržštěnosti a překážkám v důsledku rozdílných norem a technických omezení a aby se zajistil koordinovaný postup, který zabrání tomu, aby bylo provádění budoucího evropského rámce digitální identity ohroženo, je nezbytné zavést úzkou a strukturovanou spolupráci mezi Komisí, členskými státy a soukromým sektorem. K dosažení tohoto cíle by členské státy měly spolupracovat v rámci stanoveném v doporučení Komise XXX/XXXX [soubor nástrojů pro koordinovaný přístup k evropskému rámci digitální identity]²⁶ s cílem určit soubor nástrojů pro evropský rámec digitální identity. Soubor nástrojů by měl zahrnovat komplexní technickou architekturu a referenční rámec, soubor společných norem a technických referencí a soubor pokynů a popis osvědčených postupů zahrnujících alespoň všechny aspekty funkcí a interoperability evropských peněženek digitální identity, včetně elektronických podpisů, a kvalifikované služby vytvářející důvěru pro potvrzování atributů, jak je stanoveno v tomto nařízení. V této souvislosti by členské státy měly rovněž dosáhnout dohody o společných prvcích obchodního modelu a struktuře poplatků evropských peněženek digitální identity s cílem usnadnit jejich přijímání, zejména malými a středními podniky v přeshraničním kontextu. Obsah souboru nástrojů by se měl vyvíjet souběžně s diskusí a procesem přijetí evropského rámce digitální identity a měl by odrážet výsledek této diskuse a tohoto procesu.
- (37) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1525²⁷ byl konzultován evropský inspektor ochrany údajů.
- (38) Nařízení (EU) 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:

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

- 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;

²³ Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU, text s významem pro EHP, *Úř. věst. L 173, 12.6.2014, s. 349–496*.

²⁴ Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES, *Úř. věst. L 337, 23.12.2015, s. 35–127*.

²⁵ Návrh nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937, COM/2020/593 final.

²⁶ [po přijetí vložit odkaz]

²⁷ 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).

- b) stanoví pravidla pro služby vytvářející důvěru, zejména u elektronických transakcí;
- c) stanoví právní rámec pro elektronické podpisy, elektronické pečeti, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování, certifikační služby pro autentizaci internetových stránek, elektronickou archivaci a elektronické potvrzování atributů, správu prostředků pro vytváření elektronických podpisů a pečeti na dálku a pro elektronické účetní knihy;
- d) stanoví podmínky pro vydávání evropských peněženek digitální identity členskými státy.“

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

- b) odstavec 3 se nahrazuje tímto:

„3. Tímto nařízením není dotčeno vnitrostátní právo ani právo Unie týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se požadavků pro konkrétní odvětví s ohledem na formu se základními právními účinky.“

3) Článek 3 se mění takto:

- a) bod 2 se nahrazuje 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;“

- b) bod 4 se nahrazuje tímto:

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

- c) bod 14 se nahrazuje tímto:

„14) „certifikátem pro elektronický podpis“ elektronické potvrzení nebo soubor potvrzení, které spojují data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzují 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 pečeti 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, pečeti nebo certifikátů souvisejících s těmito službami;
 - d) v elektronické archivaci elektronických dokumentů;
 - e) ve správě prostředků pro vytváření elektronických podpisů a pečeti na dálku;
 - f) zaznamenávání elektronických údajů do elektronické účetní knihy.“;
- e) bod 21 se nahrazuje tímto:
- „21) „produktem“ technické zařízení nebo programové vybavení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb elektronické identifikace a služeb vytvářejících důvěru;“
- f) vkládají se nové body 23a a 23b, které znějí:
- „23a) „prostředkem pro vytváření 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 pečeti na dálku“ prostředek pro vytváření kvalifikovaných elektronických pečeti, přičemž kvalifikovaný poskytovatel služeb vytvářejících důvěru vytváří, spravuje nebo kopíruje data pro vytváření elektronických podpisů jménem pečetiící osoby;“
- g) bod 29 se nahrazuje tímto:
- „29) „certifikátem pro elektronickou pečeť“ elektronické potvrzení nebo soubor potvrzení, které spojují data pro ověřování platnosti elektronických pečeti s určitou právnickou osobou a potvrzují název této osoby;“
- h) bod 41 se nahrazuje tímto:
- „41) „ověřováním platnosti“ postup ověřující shodu a potvrzující platnost elektronického podpisu nebo elektronické pečeti nebo osobních identifikačních údajů nebo elektronického potvrzení atributů;“
- i) doplňují se nové body 42 až 55, které znějí:
- „42) „evropskou peněženkou digitální identity“ produkt a služba, které uživateli umožňují uchovávat údaje o totožnosti, pověření a atributy spojené s jeho totožností, poskytovat je na požádání spoléhajícím se stranám a používat je pro autentizaci, on-line i offline, pro službu v souladu s článkem 6a; a k vytváření kvalifikovaných elektronických podpisů a pečeti;

- (43) „atributem“ prvek, rys nebo vlastnost fyzické nebo právnické osoby nebo subjektu v elektronické podobě;
- (44) „elektronickým potvrzováním atributů“ potvrzování v elektronické podobě, které umožňuje ověřování atributů;
- (45) „kvalifikovaným elektronickým potvrzením atributů“ elektronické potvrzení atributů, které je vydáno kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze V;
- (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 ve vnitrostátním právu uznán za autentický;
- (47) „elektronickou archivací“ služba zajišťující přijímání, uchovávání, výmaz a přenos 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 dvou nebo více nezávislých prvků 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;
- (52) „pověřovacím údajem“ doklad o schopnostech, zkušenostech, právu nebo povolení osoby;
- (53) „elektronickou účetní knihou“ elektronický záznam údajů odolný proti neoprávněným zásahům, který zajišťuje pravost a integritu údajů, jež obsahuje, přesnost jejich data a času a jejich chronologické řazení;
- (54) „osobními údaji“ veškeré informace ve smyslu čl. 4 bodu 1 nařízení (EU) 2016/679;
- (55) „jedinečnou identifikací“ postup, při němž jsou osobní identifikační údaje nebo prostředky osobní identifikace porovnávány nebo propojeny se stávajícím účtem patřícím téže osobě.“

4) Článek 5 se nahrazuje tímto:

„Článek 5

Pseudonymy v elektronických transakcích

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

- 5) V kapitole II se název nahrazuje tímto:
„ODDÍL I
ELEKTRONICKÁ IDENTIFIKACE“.
- 6) Článek 6 se zrušuje.
- 7) Vkládají se nové články (6a, 6b, 6c a 6d), které znějí:

„Článek 6a

Evropské peněženky digitální identity

1. S cílem zajistit, aby všechny fyzické a právnické osoby v Unii měly bezpečný, důvěryhodný a hladký přístup k přeshraničním veřejným a soukromým službám, vydá každý členský stát do dvanácti měsíců od vstupu tohoto nařízení v platnost evropské peněženky digitální identity.
2. Evropské peněženky digitální identity jsou vydávány:
 - a) členským státem;
 - b) z pověření členského státu;
 - c) nezávisle, ale jsou uznávány členským státem.
3. Evropské peněženky digitální identity umožní uživateli:
 - a) bezpečně požadovat a získávat, ukládat, vybírat, kombinovat a sdílet způsobem, který je pro uživatele transparentní a sledovatelný, nezbytné zákonné osobní identifikační údaje a elektronické potvrzení atributů za účelem on-line a offline autentizace s cílem využívat veřejné a soukromé služby on-line;
 - b) podepisovat kvalifikovanými elektronickými podpisy.
4. Peněženky digitální identity zejména:
 - a) poskytují společné rozhraní:
 - 1) kvalifikovaným a nekvalifikovaným poskytovatelům služeb vytvářejících důvěru, kteří vydávají kvalifikovaná a nekvalifikovaná elektronická potvrzení atributů nebo jiné kvalifikované a nekvalifikované certifikáty za účelem vydávání těchto potvrzení a certifikátů evropské peněženky digitální identity;
 - 2) spoléhajícím se stranám, aby mohly požadovat a ověřovat osobní identifikační údaje a elektronická potvrzení atributů;
 - 3) pro předkládání osobních identifikačních údajů, elektronického potvrzení atributů nebo jiných údajů, jako jsou pověřovací údaje, spoléhajícím se stranám v místním režimu, který pro peněženku nevyžaduje přístup k internetu;
 - 4) umožňují uživateli interakci s evropskou peněženkou digitální identity a zobrazení „značky důvěry EU pro peněženku evropské digitální identity“;

- b) zajišťují, aby poskytovatelé služeb vytvářejících důvěru a kvalifikovaných potvrzení atributů nemohli obdržet žádné informace 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;
 - d) poskytují mechanismus, který zajistí, aby spoléhající se strana byla schopna uživatele ověřit a obdržet elektronická potvrzení atributů;
 - e) zajistí, aby osobní identifikační údaje uvedené v čl. 12 odst. 4 písm. d) jedinečně a trvale identifikovaly fyzickou nebo právnickou osobu, která je s nimi spojena.
5. Členské státy pro evropské peněženky digitální identity poskytnou mechanismy ověření:
- a) které zajistí, že je možné ověřit jejich pravost a platnost;
 - b) které spoléhajícím se stranám umožní ověřit platnost potvrzení atributů;
 - c) které spoléhajícím se stranám a kvalifikovaným poskytovatelům služeb vytvářejících důvěru umožní ověřit pravost a platnost přiřazených osobních identifikačních údajů.
6. Evropské peněženky digitální identity jsou vydávány v rámci oznámeného systému elektronické identifikace s „vysokou“ úrovní záruky. Používání evropských peněženek digitální identity je pro fyzické osoby bezplatné.
7. Evropskou peněženku digitální identity má uživatel plně pod kontrolou. Vydavatel evropské peněženky digitální identity neshromažďuje informace o používání peněženky, které nejsou nezbytné pro poskytování služeb peněženky, ani nekombinuje osobní identifikační údaje a jakékoli jiné uložené osobní údaje nebo údaje týkající se používání evropské peněženky digitální identity s osobními údaji z jiných služeb nabízených tímto vydavatelem nebo ze služeb třetích stran, které nejsou nezbytné pro poskytování služeb peněženky, ledaže o to uživatel výslovně požádal. Osobní údaje týkající se poskytování evropské peněženky digitální identity jsou uchovávány fyzicky a logicky odděleně od jakýchkoli jiných uchovávaných údajů. 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.
8. Článek 11 se použije obdobně pro evropskou peněženku digitální identity.
9. Ustanovení čl. 24 odst. 2 písm. b), e), g) a h) se použije obdobně na členské státy vydávající 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 2019/882.
11. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity technické a provozní specifikace a referenční normy pro požadavky uvedené v odstavcích 3, 4 a 5. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 48 odst. 2.

Článek 6b

Spoléhající se strany u evropských peněženek digitální identity

1. Pokud mají spoléhající se strany v úmyslu spoléhat se na evropské peněženky digitální identity vydané v souladu s tímto nařízením, sdělí to členskému státu, v němž je spoléhající se strana usazena, aby byl zajištěn soulad s požadavky stanovenými v právních předpisech Unie nebo vnitrostátních právních předpisech pro poskytování konkrétních služeb. Při sdělování svého záměru spoléhat se na evropské peněženky digitální identity informují rovněž o zamýšleném způsobu jejich použití.
2. Členské státy zavedou pro autentizaci spoléhajících se stran společný mechanismus.
3. Spoléhající se strany jsou odpovědné za provádění postupu autentizace osobních identifikačních údajů a elektronického potvrzování atributů pocházejících z evropských peněženek digitální identity.
4. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 10, technické a provozní specifikace pro požadavky uvedené v odstavcích 1 a 2.

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 čl. 6a odst. 3, 4 a 5, pokud se na tyto požadavky vztahuje certifikát kybernetické bezpečnosti nebo prohlášení o shodě či jejich části.
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.
3. Soulad evropských peněženek digitální identity s požadavky stanovenými v čl. 6a odst. 3, 4 a 5 je certifikován akreditovanými subjekty veřejného nebo soukromého sektoru určenými členskými státy.
4. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů seznam norem pro certifikaci evropských peněženek digitální identity uvedenou v odstavci 3.
5. Členské státy sdělí Komisi názvy a adresy veřejných nebo soukromých subjektů uvedených v odstavci 3. Komise tyto informace zpřístupní členským státům.
6. Komise je zmocněna k přijímání aktů v přenesené pravomoci v souladu s článkem 47, pokud jde o stanovení zvláštních kritérií, která mají splňovat určené subjekty uvedené v odstavci 3.

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.
 2. Na základě obdržených informací Komise zřizuje, zveřejňuje a udržuje seznam certifikovaných evropských peněženek digitální identity.
 3. Do šesti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 10, formáty a postupy použitelné pro účely odstavce 1.“
- 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 dvanácti měsíců od vstupu tohoto nařízení v platnost alespoň jeden systém elektronické identifikace včetně alespoň jednoho identifikačního prostředku.“.
- 10) V článku 9 se odstavce 2 a 3 nahrazují tímto:
- „2. Komise zveřejní v *Úředním věstníku Evropské unie* seznam systémů elektronické identifikace, které byly oznámeny podle odstavce 1 tohoto článku, a základní informace o těchto systémech.
 3. Komise zveřejní v *Úředním věstníku Evropské unie* změny seznamu uvedeného v odstavci 2 do jednoho měsíce od obdržení daného oznámení.“
- 11) Vkládá se nový článek 10a, který zní:
- „*Článek 10a*

Narušení bezpečnosti evropských peněženek digitální identity

1. Pokud jsou evropské peněženky digitální identity vydané podle článku 6a a mechanismy ověření uvedené v čl. 6a odst. 5 písm. a), b) a c) porušeny nebo částečně ohroženy způsobem, který ovlivňuje jejich spolehlivost 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 ostatní členské státy a Komisi.
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 ostatní členské státy a Komisi.
3. Není-li porušení nebo ohrožení uvedené v odstavci 1 napraveno do tří měsíců od pozastavení nebo zrušení, dotčený členský stát dotýcnou evropskou digitální peněženkou stáhne a informuje o stažení ostatní členské státy a Komisi. Je-li to odůvodněno závažností porušení, je evropská peněženka digitální identity stažena neprodleně.

4. Komise bez zbytečného odkladu zveřejní v *Úředním věstníku Evropské unie* odpovídající změny v seznamu uvedeném v článku 6d.
5. Do šesti měsíců od vstupu tohoto nařízení v platnost Komise prostřednictvím prováděcího aktu o zavedení evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 10, dále upřesní opatření uvedená v odstavcích 1 a 3.“

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

„Článek 11a

Jedinečná identifikace

1. Používají-li se k autentizaci oznámené prostředky pro elektronickou identifikaci a evropské peněženky digitální identity, zajistí členské státy jedinečnou identifikaci.
2. Členské státy pro účely tohoto nařízení zahrnou do minimálního souboru osobních identifikačních údajů uvedeného v čl. 12 odst. 4 písm. d) jedinečný a trvalý identifikátor v souladu s právem Unie, aby uživatele na jeho žádost identifikovaly v případech, kdy je identifikace uživatele vyžadována právními předpisy.
3. Do šesti měsíců od vstupu tohoto nařízení v platnost Komise prostřednictvím prováděcího aktu o zavedení peněženky evropské digitální identity, jak je uvedeno v čl. 6a odst. 10, dále upřesní opatření uvedená v odstavci 1 a 2.“

13) Článek 12 se mění takto:

- a) v odstavci 3 se zrušují písmena c) a d);
- b) v odstavci 4 se písmeno d) nahrazuje tímto:
„d) odkazu na minimální soubor osobních identifikačních údajů nezbytných k jedinečné a trvalé identifikaci fyzické nebo právnické osoby;“
- c) v odstavci 6 se písmeno a) nahrazuje tímto:
„a) výměnu informací, zkušeností a osvědčených postupů v oblasti systémů elektronické identifikace, a zejména v oblasti technických požadavků týkajících se interoperability, jedinečné identifikace a úrovní záruky;“

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

„Článek 12a

Certifikace systémů elektronické identifikace

1. Soulad oznámených systémů elektronické identifikace s požadavky stanovenými v článcích 6a, 8 a 10 může být certifikován subjekty veřejného nebo soukromého sektoru určenými členskými státy.
2. Vzájemné hodnocení systémů elektronické identifikace uvedené v čl. 12 odst. 6 písm. c) se nevztahuje na systémy elektronické identifikace nebo na část těchto systémů certifikovaných v souladu s odstavcem 1. 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 soulad těchto systémů s požadavky

stanovenými v čl. 8 odst. 2, pokud jde o úroveň záruky systémů elektronické identifikace.

3. Členské státy sdělí Komisi názvy a adresy veřejných nebo soukromých subjektů uvedených v odstavci 1. Komise tyto informace zpřístupní 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 12b a 12c, 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.
2. Pokud vnitrostátní právní předpisy nebo právní předpisy Unie vyžadují od soukromých spoléhajících se stran poskytujících služby silnou autentizaci uživatele k on-line identifikaci nebo pokud smluvní závazek vyžaduje silnou autentizaci uživatele, a to i v oblasti dopravy, energetiky, bankovníctví a finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, vzdělávání nebo telekomunikací, akceptují soukromé spoléhající se strany rovněž evropské peněženky digitální identity vydané v souladu s článkem 6a.
3. V případech, kdy velmi rozsáhlé on-line platformy ve smyslu článku 25 odst. 1 nařízení [odkaz na nařízení o aktu o digitálních službách] vyžadují, aby se uživatelé pro přístup k on-line službám autentizovali, přijmou rovněž evropské peněženky digitální identity vydané v souladu s článkem 6a výhradně na dobrovolnou žádost uživatele a s ohledem na minimální atributy nezbytné pro konkrétní on-line službu, pro kterou se autentizace požaduje, například doklad o věku.
4. Komise 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.

5. Komise do osmnácti měsíců od zavedení evropských peněženek digitální identity posoudí, zda by na základě důkazů prokazujících dostupnost a použitelnost evropské peněženky digitální identity měli být k přijímání evropské peněženky digitální identity výhradně na dobrovolnou žádost uživatele povinni další soukromí poskytovatelé on-line služeb. Kritéria hodnocení mohou zahrnovat rozsah uživatelské základny, přeshraniční přítomnost poskytovatelů služeb, technologický rozvoj a vývoj způsobů využívání. Komise je zmocněna k přijímání aktů v přenesené pravomoci na základě tohoto posouzení, pokud jde o přezkum požadavků na uznání evropské peněženky digitální identity podle bodů 1 až 4 tohoto článku.
6. Pro účely tohoto článku evropské peněženky digitální identity nepodléhají požadavkům uvedeným v článcích 7 a 9.

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 uznán v tomto členském státě 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 úroveň 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 právní 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 čl. 48 odst. 2 přijmout prováděcí akty, kterými stanoví podmínky, 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 prováděcí akt 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

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

20) Článek 17 se mění takto:

a) odstavec 4 se mění takto:

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

„c) informovat příslušné vnitrostátní orgány dotčených členských států určené podle směrnice (EU) XXXX/XXXX [o bezpečnosti sítí a informací 2] o veškerých závažných případech narušení bezpečnosti nebo ztráty integrity, o nichž se dozvědí při plnění svých úkolů. Pokud se závažné narušení bezpečnosti nebo ztráta integrity týká jiných členských států, orgán dohledu informuje jednotné kontaktní místo dotčeného členského státu určené podle směrnice (EU) XXXX/XXXX (o bezpečnosti sítí a informací 2);“

2) písmeno f) se nahrazuje tímto:

„f) spolupracovat 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 byla porušena pravidla týkající se ochrany osobních údajů, a o porušeních bezpečnosti, která představují porušení ochrany osobních údajů;“

b) odstavec 6 se nahrazuje tímto:

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

c) odstavec 8 se nahrazuje tímto:

- „8. Do dvanácti měsíců od vstupu tohoto nařízení v platnost Komise prostřednictvím prováděcích aktů dále upřesní úkoly dozorových úřadů uvedených v odstavci 4 a určí formáty a postupy pro podávání zpráv podle odstavce 6. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

21) Článek 18 se mění takto:

- a) název článku 18 se nahrazuje tímto:

„Vzájemná pomoc a spolupráce“;

- b) odstavec 1 se nahrazuje tímto:

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

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

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

5. Do dvanácti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů nezbytná procesní opatření pro usnadnění spolupráce mezi orgány dohledu uvedenými v odstavci 1.“

22) Článek 20 se mění takto:

- a) odstavec 1 se nahrazuje tímto:

„1. Kvalifikování poskytovatelé služeb vytvářejících důvěru se na vlastní náklady alespoň jednou za 24 měsíců podrobí auditu ze strany subjektu posuzování shody. Audit potvrdí, že kvalifikování 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]. Kvalifikování 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:

„Jestliže podle všeho došlo k porušení pravidel týkajících se ochrany osobních údajů, sdělí orgán dohledu výsledky svých auditů dozorovým úřadům podle nařízení (EU) 2016/679.“;

c) odstavce 3 a 4 se nahrazují tímto:

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

Pokud tento poskytovatel nezjedná nápravu, a to ve lhůtě případně stanovené orgánem dohledu, může orgán dohledu zejména s přihlédnutím k rozsahu, délce trvání a důsledkům daného neplnění odejmout danému poskytovateli nebo jím poskytované dotčené službě status kvalifikovaného poskytovatele nebo kvalifikované služby a případně jej požádat, 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 dvanácti měsíců od vstupu tohoto 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 prodloužení a dobu, v níž bude ověřování dokončeno.“;

b) odstavec 4 se nahrazuje tímto:

„4. Do dvanácti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů 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.“

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 „značnou“ nebo „vysokou“ úroveň záruky;
- b) pomocí kvalifikovaného elektronického potvrzení atributů nebo certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaných v souladu s písmeny a), c) nebo d);
- c) použitím jiných metod identifikace, které zajišťují identifikaci 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 1a, který zní:
- „1a. Do dvanácti měsíců od vstupu tohoto nařízení v platnost stanoví Komise prostřednictvím prováděcích aktů minimální technické specifikace, normy a postupy týkající se ověřování identity a atributů v souladu s odst. 1 písm. c). Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“;
- c) odstavec 2 se mění takto:
- 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. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro požadavky uvedené v odstavci 2. 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, pokud jde o dodatečná opatření uvedená v odst. 2 písm. f).“
- 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 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 29a, který zní:
- „Článek 29a*
- Požadavky na kvalifikovanou službu správy prostředků pro vytváření elektronických podpisů na dálku**
1. Správu prostředků pro vytváření kvalifikovaných elektronických podpisů na dálku jako kvalifikované služby může provádět pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který:
- a) vytváří nebo spravuje data pro vytváření elektronických podpisů jménem podepisující osoby;
- b) bez ohledu na přílohu II bod 1 písm. d) kopíruje data pro vytváření elektronických podpisů pouze pro účely zálohování a jsou-li splněny tyto požadavky:
- bezpečnost zkopírovaných souborů dat je na stejné úrovni jako u původních souborů dat;
- počet zkopírovaných souborů dat nepřesáhne minimum potřebné pro zajištění kontinuity služby;

- c) splňuje všechny požadavky uvedené v certifikační zprávě konkrétního kvalifikovaného prostředku pro vytváření podpisů na dálku vydaného podle článku 30.
2. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů technické specifikace a referenční čísla norem pro účely odstavce 1.“
- 29) V článku 30 se vkládá nový odstavec 3a, který zní:
- „3a. 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 dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů formáty a postupy použitelné pro účely odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“
- 31) Článek 32 se mění takto:
- a) v odstavci 1 se doplňuje nový pododstavec, který zní:
- „Pokud ověřování platnosti kvalifikovaných elektronických podpisů vyhovuje normám uvedeným v odstavci 3, předpokládá se shoda s požadavky stanovenými v prvním pododstavci.“;
- b) odstavec 3 se nahrazuje tímto:
- „3. Do dvanácti měsíců od vstupu tohoto nařízení v platnost 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 dvanácti měsíců od vstupu tohoto 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 pečeti uvedenými v článku 36 a v odstavci 5 tohoto článku.“;
- b) odstavec 4 se nahrazuje tímto:
- „4. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro zaručené elektronické pečeti. 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 pečeti 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 dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů referenční čísla norem pro kvalifikované certifikáty pro elektronické pečeti. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“
- 35) Vkládá se nový článek 39a, který zní:
- „Článek 39a*
- Požadavky na kvalifikovanou službu správy prostředků pro vytváření elektronických pečeti na dálku**
- Na kvalifikovanou službu správy prostředků pro vytváření elektronických pečeti 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 dvanácti měsíců od vstupu tohoto 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 dvanácti měsíců od vstupu tohoto 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 musí splňovat požadavky stanovené v příloze IV. Kvalifikované certifikáty pro autentizaci internetových stránek se považují za vyhovující 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. Pro tyto účely internetové prohlížeče zajistí, aby údaje o totožnosti poskytnuté pomocí kterékoli z metod byly zobrazeny uživatelsky přívětivým způsobem. Internetové prohlížeče zajistí podporu a interoperabilitu s kvalifikovanými certifikáty pro autentizaci internetových stránek uvedenými v odstavci 1, s výjimkou podniků, které jsou považovány za mikropodniky a malé podniky v souladu s doporučením Komise 2003/361/ES, v prvních pěti letech fungování jako poskytovatelé služeb prohlížení internetových stránek.
3. Do dvanácti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcích aktů specifikace a referenční čísla norem pro kvalifikované certifikáty pro autentizaci internetových stránek uvedené v odstavci 1. 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.
2. Kvalifikované elektronické potvrzení atributů má stejný právní účinek jako zákonně vydaná potvrzení v tištěné podobě.
3. Kvalifikované elektronické potvrzení atributů vydané v jednom členském státě se uznává jako kvalifikované elektronické potvrzení atributů v jakémkoli jiném členském státě.

Článek 45b

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. Kvalifikovaná elektronická potvrzení atributů nepodléhají 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.
4. Do šesti měsíců od vstupu tohoto nařízení v platnost určí Komise prostřednictvím prováděcího aktu o provádění evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 10, 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 ověřit autenticitu atributu přímo porovnáním s příslušným autentickým zdrojem na vnitrostátní úrovni nebo prostřednictvím určených zprostředkovatelů uznaných na vnitrostátní úrovni v souladu s vnitrostátními právními předpisy nebo právními předpisy Unie.
2. Do šesti měsíců od vstupu tohoto nařízení v platnost a s přihlédnutím k příslušným mezinárodním normám stanoví Komise prostřednictvím prováděcího aktu o provádění evropské peněženky digitální identity, jak je uvedeno v čl. 6a odst. 10, minimální technické specifikace, normy a postupy s odkazem na katalog atributů a systémy potvrzování atributů a ověřovací postupy pro kvalifikované elektronické potvrzení atributů.

Článek 45e

Vydávání elektronických potvrzení atributů evropským peněženkám digitální identity

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

Článek 45f

Dodatečná pravidla poskytování služeb elektronického potvrzování atributů

1. Poskytovatelé kvalifikovaných a nekvalifikovaných služeb elektronického potvrzování atributů nesmějí kombinovat osobní údaje týkající se poskytování těchto služeb s osobními údaji z jiných služeb, které nabízejí.
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 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 důvěryhodnost elektronického dokumentu i po uplynutí doby technické platnosti.

Do dvanácti 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.

ODDÍL 11

ELEKTRONICKÉ ÚČETNÍ KNIHY

Článek 45h

Právní účinky elektronických účetních knih

1. Elektronické účetní knize nesmějí být upírány právní účinky a nesmí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické pečeti.
2. U kvalifikované elektronické účetní knihy platí domněnka jedinečnosti a pravosti údajů, které obsahuje, správnosti jejich data a času a jejich chronologického řazení v rámci účetní knihy.

Článek 45i

Požadavky na kvalifikované elektronické účetní knihy

1. Kvalifikované elektronické účetní knihy musí splňovat tyto požadavky:
 - a) jsou vytvářeny jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru;
 - b) zajišťují jedinečnost, autenticitu a správné pořadí údajů zaznamenaných v účetní knize;

- c) zajišťují správné chronologické řazení údajů v účetní knize a správnost data a času vložení údajů;
 - d) zaznamenávají údaje takovým způsobem, že je možné zjistit jakoukoliv následnou změnu údajů.
2. Pokud elektronická účetní kniha 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 provádění a registrace souboru údajů do kvalifikované elektronické účetní knihy a pro vytváření kvalifikované elektronické účetní knihy. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

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

„Článek 48a

Požadavky týkající se podávání zpráv

1. Členské státy zajistí shromažďování statistických údajů týkajících se fungování evropských peněženek digitální identity 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;
 - c) incidenty a výpadky infrastruktury na vnitrostátní úrovni, které brání používání aplikací pro peněženku digitální identity.
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 vstupu tohoto 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 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) Doplnuje se nová příloha V uvedená v příloze V tohoto nařízení.
- 48) Doplnuje 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 Bruselu dne

*Za Evropský parlament
předseda*

*Za Radu
předseda/předsedkyně*

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Nařízení Evropského parlamentu a Rady o rámci pro evropskou digitální identitu, kterým se mění nařízení eIDAS

1.2. Příslušné oblasti politik

Oblast politiky: Vnitřní trh
Evropa připravená na digitální věk

1.3. Návrh/podnět se týká:

- ☐ nové akce
- ☐ nové akce následující po pilotním projektu / přípravné akci²⁸
- ☒ prodloužení stávající akce
- ☐ sloučení jedné či více akcí v jinou/novou akci nebo přesměrování jedné či více akcí na jinou/novou akci

1.4. Cíle

1.4.1. Obecné cíle

Obecným cílem tohoto podnětu je zajistit řádné fungování vnitřního trhu, zejména ve vztahu k poskytování a používání přeshraničních a meziodvětvových veřejných a soukromých služeb založených na dostupnosti a používání vysoce zabezpečených a důvěryhodných řešení elektronické identity. Tento cíl se promítá do strategického cíle stanoveného ve sdělení „Formování digitální budoucnosti Evropy“.

1.4.2. Specifické cíle

Specifický cíl č. 1

Zajistit přístup k důvěryhodným a zabezpečeným řešením digitální identity, která lze použít přeshraničně a která splňují očekávání uživatelů a poptávku na trhu.

Specifický cíl č. 2

Zajistit, aby se veřejné a soukromé služby mohly spoléhat na důvěryhodná a zabezpečená řešení digitální identity bez ohledu na hranice států.

Specifický cíl č. 3

Zajistit občanům plnou kontrolu nad jejich osobními údaji a zajistit jejich bezpečnost při používání řešení digitální identity.

Specifický cíl č. 4

Zajistit rovné podmínky pro poskytování kvalifikovaných služeb vytvářejících důvěru v EU a jejich přijetí.

²⁸ Uvedené v čl. 58 odst. 2 písm. a) nebo b) finančního nařízení.

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Celkově se očekává, že nejpřínosnější bude tato iniciativa pro koncové uživatele / občany, poskytovatele on-line služeb, poskytovatele aplikací pro peněženky a veřejné a soukromé poskytovatele služeb v oblasti digitální identity. Od iniciativy se očekává, že zajistí přístup k důvěryhodným a zabezpečeným řešením v oblasti digitální identity, která lze použít přeshraničně a která splňují očekávání uživatelů a odpovídají poptávce na trhu; že zajistí, aby se veřejné a soukromé služby mohly spoléhat na přeshraniční důvěryhodná a zabezpečená řešení v oblasti digitální identity; že občanům zajistí plnou kontrolu nad jejich osobními údaji a zajistí jejich bezpečnost při používání řešení v oblasti digitální identity; a že zajistí rovné podmínky pro poskytování kvalifikovaných služeb vytvářejících důvěru v EU a jejich přijetí.

Kromě možnosti přístupu k veřejným i soukromým službám by občané a společnosti měli přímý prospěch z pohodlí a uživatelské přívětivosti autentizačního rozhraní peněženky a byli by schopni provádět transakce vyžadující všechny úrovně záruky (např. od přihlášení na sociálních médiích po aplikace elektronického zdravotnictví).

Posílený přístup založený na „ochraně soukromí již od návrhu“ by mohl přinést další výhody, protože peněženka by v procesu uplatňování atributů nevyžadovala zprostředkovatele, což by občanům umožnilo komunikovat přímo s poskytovateli služeb a pověřenými. Zvýšená bezpečnost údajů peněženky by zabránila krádeži identity, čímž by se zabránilo finančním ztrátám evropských občanů a podniků.

Co se týče hospodářského růstu, očekává se, že zavedení systému založeného na normách sníží nejistotu účastníků trhu a bude mít rovněž pozitivní dopad na inovace.

A co je důležité, očekává se, že poskytne inkluzivnější přístup k veřejným a soukromým službám spojeným s veřejnými statky, jako jsou vzdělávání a zdravotnictví, u nichž některé sociální skupiny v současnosti narážejí na určité překážky. Například někteří občané se zdravotním postižením, často ti se sníženou pohyblivostí, nebo žijící ve venkovských oblastech mohou mít horší přístup ke službám, které obvykle vyžadují fyzickou přítomnost, pokud nejsou poskytovány v místě.

1.4.4. Ukazatele výkonnosti

Upřesněte ukazatele pro sledování pokroku a dosažených výsledků.

Aspekt monitorování a hodnocení a příslušné cíle	Ukazatel	Odpovědnost za shromažďování	Zdroje
Uplatňování			

Poskytnout přístup k prostředkům pro elektronickou identifikaci všem občanům EU	Počet evropských občanů a podniků, kterým byly vydány oznámené elektronické průkazy totožnosti/ evropské peněženky digitální identity, a počet vydaných pověřovacích údajů k identitě (potvrzení atributů).	Evropská komise a příslušné vnitrostátní orgány	Roční průzkum / údaje o monitorování a hodnocení shromážděné příslušnými vnitrostátními orgány
Poskytnout přístup k prostředkům pro elektronickou identifikaci všem občanům EU	Počet evropských občanů a podniků, kteří aktivně používají oznámené elektronické průkazy totožnosti/ evropské peněženky digitální identity a pověřovací údaje k identitě (potvrzení atributů)	Evropská komise a příslušné vnitrostátní orgány	Roční průzkum / údaje o monitorování a hodnocení shromážděné příslušnými vnitrostátními orgány
Zvýšit míru přeshraničního uznávání a přijímání systémů elektronické identifikace s cílem dosáhnout všeobecného přijetí	Počet poskytovatelů on-line služeb, kteří přijímají oznámené elektronické průkazy totožnosti/ evropské peněženky digitální identity a pověřovací údaje k identitě (potvrzení atributů)	Evropská komise	Každoroční průzkum
Zvýšit míru přeshraničního uznávání a přijímání systémů elektronické identifikace s cílem dosáhnout všeobecného přijetí	Počet on-line transakcí uskutečněných prostřednictvím oznámených elektronických průkazů totožnosti/ evropských peněženek digitální identity a pověřovacích údajů k identitě (potvrzení atributů) (celkem a přeshraničně)	Evropská komise	Každoroční průzkum
Podpořit přijetí soukromým sektorem a rozvoj nových služeb v oblasti digitální identity	Počet nových soukromě vydaných služeb v oblasti potvrzování atributů splňujících normy pro integraci do evropské peněženky digitální identity	Evropská komise a příslušné vnitrostátní orgány	Každoroční průzkum
Souvislosti			
Podpořit přijetí soukromým sektorem a rozvoj nových služeb v oblasti digitální identity	Velikost trhu s digitální identitou	Evropská komise	Každoroční průzkum

Podpořit přijetí soukromým sektorem a rozvoj nových služeb v oblasti digitální identity	Výdaje na veřejné zakázky spojené s digitální identitou	Evropská komise a příslušné vnitrostátní orgány	Každoroční průzkum
Zvýšit míru přeshraničního uznávání a přijímání systémů elektronické identifikace s cílem dosáhnout všeobecného přijetí	% podniků, které prodávají zboží nebo poskytují služby v elektronickém obchodě	Evropská komise	Eurostat
Zvýšit míru přeshraničního uznávání a přijímání systémů elektronické identifikace s cílem dosáhnout všeobecného přijetí	Podíl on-line transakcí vyžadujících silnou identifikaci zákazníka (celkem)	Evropská komise	Každoroční průzkum
Poskytnout přístup k prostředkům pro elektronickou identifikaci všem občanům EU	% jednotlivců provozujících elektronický obchod % jednotlivců, kteří mají přístup k veřejným službám on-line	Evropská komise	Eurostat

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech. Členské státy budou povinny vydat evropskou peněženku digitální identity do 24–48 měsíců (orientačně) od přijetí nařízení. Komisi bude svěřena pravomoc přijímat prováděcí akty, kterými stanoví technické specifikace a referenční normy pro technickou architekturu evropského rámce digitální identity do 12–24 měsíců (orientačně) od přijetí nařízení.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

Důvody pro akci na evropské úrovni (*ex ante*)

Vzhledem k rostoucí poptávce občanů, podniků a poskytovatelů on-line služeb po uživatelsky přívětivých, bezpečných a soukromí chránících řešeních v oblasti digitální identity, která lze použít přeshraničně, mohou další opatření na úrovni EU přinést větší hodnotu než opatření jednotlivých členských států, jak ukazuje hodnocení nařízení eIDAS.

Očekávaná vytvořená přidaná hodnota Unie (*ex-post*)

Harmonizovanější přístup na úrovni EU založený na zásadním přechodu od spoléhání se pouze na řešení digitální identity k poskytování elektronických potvrzení atributů by zajistil, že by občané a podniky měli přístup k veřejným a soukromým službám kdekoli v EU a využívali ověřené doklady totožnosti a atributy. Poskytovatelé on-line služeb by mohli přijímat řešení digitální identity nezávisle na tom, kde byla vydána, a využívat společný evropský přístup k důvěře, bezpečnosti a interoperabilitě. Uživatelé i poskytovatelé služeb mohou rovněž využívat stejné právní hodnoty, která je elektronickým potvrzením atributů přiznána v celé EU, což je obzvláště důležité, pokud je nutný koordinovaný postup, například pokud jde o digitální zdravotní osvědčení. Služby vytvářející důvěru a poskytující elektronická potvrzení atributů by rovněž těžily z dostupnosti evropského trhu pro své služby. Například návratnost nákladů na zajištění vysoce důvěryhodného a bezpečného prostředí pro poskytování kvalifikované služby vytvářející důvěru je díky úsporám z rozsahu snadněji dosažitelná na úrovni EU. Pouze rámec EU může zajistit plnou přeshraniční přenositelnost právní identity a elektronického potvrzování atributů s ní spojených, což umožní důvěřovat prohlášením o identitě učiněným jinými členskými státy.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Nařízení eIDAS (nařízení 910/2014) je jediným přeshraničním rámcem pro důvěryhodnou elektronickou identifikaci fyzických a právnických osob a pro služby vytvářející důvěru. Ačkoli nařízení eIDAS hraje na vnitřním trhu nespornou úlohu, od jeho přijetí se mnoho změnilo. Nařízení eIDAS, přijaté v roce 2014, je založeno na vnitrostátních systémech elektronické identifikace podle různých norem a zaměřuje se na relativně malý segment potřeb občanů a podniků v oblasti elektronické identifikace: zajištění přeshraničního přístupu k veřejným službám. Cílové služby se týkají především 3 % obyvatelstva EU s bydlištěm v jiném členském státě, než ve kterém se narodili.

Od té doby se digitalizace všech funkcí společnosti výrazně zvýšila. Pandemie COVID-19 měla v neposlední řadě na rychlost digitalizace velmi silný vliv. V důsledku toho se poskytování veřejných i soukromých služeb stále více přesouvá do digitální oblasti. Občané a podniky očekávají, že dosáhnou vysoké bezpečnosti a pohodlí u jakékoli činnosti on-line, jako je podávání daňových přiznání, zápis na zahraniční univerzitu, dálkové otevření bankovního účtu nebo žádost o půjčku, pronájem automobilu, zahájení podnikání v jiném členském státě, ověřování plateb přes internet, podávání nabídek v on-line výběrovém řízení a další.

V důsledku toho se radikálně zvýšila poptávka po prostředcích k identifikaci a autentizaci on-line, jakož i digitální výměně informací týkajících se naší totožnosti, atributů nebo kvalifikace (totožnost, adresy, věk, ale také odborná kvalifikace, řidičské průkazy a jiná povolení a platební systémy), a to bezpečně a s vysokou úrovní ochrany údajů.

To vyvolalo změnu paradigmatu směrem k pokročilým a pohodlným řešením, která jsou schopna integrovat různá ověřitelná data a certifikáty uživatele. Uživatelé očekávají prostředí s vlastním nastavením, v němž lze mít a sdílet různé pověřovací údaje a atributy, jako jsou například vnitrostátní elektronický průkaz totožnosti, profesní osvědčení, průkazy MHD nebo v některých případech dokonce digitální vstupenky na koncert. Jedná se o tzv. samostatné peněženky založené na aplikacích, které jsou

spravované prostřednictvím mobilního zařízení uživatele a které umožňují bezpečný a snadný přístup k různým službám, veřejným i soukromým, pod jeho plnou kontrolou.

1.5.4. *Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji*

Iniciativa podporuje evropské úsilí o obnovu tím, že občanům a podnikům poskytuje nezbytné nástroje, např. pohodlnou elektronickou identifikaci a služby vytvářející důvěru, které jim pomohou provádět každodenní činnosti on-line důvěryhodným a bezpečným způsobem. Je proto plně v souladu s cíli víceletého finančního rámce.

Provozní výdaje mají být financovány v rámci specifického cíle č. 5 programu Digitální Evropa. Smlouvy o zakázkách podporující rozvoj norem a technických specifikací a také náklady na údržbu stavebních kamenů elektronické identifikace a služeb vytvářejících důvěru se odhadují až na 3–4 miliony EUR ročně. O přesném přidělení těchto rozpočtových prostředků je třeba rozhodnout v okamžiku formulování budoucích pracovních programů. Granty podporující propojení veřejných a soukromých služeb s ekosystémem elektronické identifikace by výrazně podpořily dosažení cílů návrhu. Náklady poskytovatele služeb na integraci nezbytného rozhraní API peněženky pro elektronickou identifikaci se odhadují na přibližně 25 000 EUR coby jednorázové náklady na poskytovatele. Po projednání rozdělení rozpočtu na příští pracovní program by rozpočet na granty až do výše 0,5 milionu EUR na členský stát, bude-li k dispozici, přispěl k propojení kritického množství služeb.

Zasedání skupin odborníků související s vypracováním prováděcích aktů budou účtována správní části programu Digitální Evropa v celkové výši až 0,5 milionu EUR.

Synergie s ostatními nástroji

Tato iniciativa poskytne rámec pro poskytování elektronické identity a služeb elektronické identity v EU, na něž se mohou konkrétní odvětví spolehnout při plnění odvětvových právních požadavků, například v souvislosti s digitálními cestovními doklady, digitálními řidičskými průkazy atd. Podobně je návrh v souladu s cíli nařízení 2019/1157, které posiluje bezpečnost průkazů totožnosti a dokladů o pobytu. Podle tohoto nařízení jsou členské státy povinny zavést nové průkazy totožnosti s aktualizovanými bezpečnostními prvky do srpna 2021. Jakmile budou vypracovány, mohly by členské státy modernizovat nové průkazy totožnosti tak, aby mohly být oznamovány jako systémy elektronické identifikace definované v nařízení IDAS.

Iniciativa rovněž přispěje k transformaci celní oblasti na bezpapírové elektronické prostředí v kontextu iniciativy pro rozvoj prostředí jednotného portálu EU pro oblast celnictví. Je třeba rovněž poznamenat, že budoucí návrh přispěje k evropským politikám mobility tím, že usnadní právní požadavky provozovatelů v námořním odvětví na podávání zpráv stanovené v souvislosti s evropským prostředím jednotného námořního portálu, které se začne uplatňovat od 15. srpna 2025. Totéž platí pro spojení s nařízením o elektronických informacích o nákladní dopravě, které orgánům členských států ukládá povinnost přijímat elektronické informace o nákladní dopravě. Aplikace evropské peněženky digitální identity bude rovněž schopna zpracovat pověřovací údaje týkající se řidičů, vozidel a operací požadovaných právním rámcem EU v oblasti silniční dopravy (např. digitální řidičské průkazy / směrnice 2006/126/ES). Specifikace budou v souvislosti s tímto

rámcem dále rozpracovány. Budoucí iniciativa by rovněž mohla přispět k utváření budoucích iniciativ v oblasti koordinace sociálního zabezpečení, jako je případný vývoj evropského průkazu sociálního zabezpečení, který by mohl stavět na základech důvěry (trust anchors) nabízených oznamovanými identitami v rámci nařízení eIDAS.

Tato iniciativa podporuje provádění nařízení GDPR (2016/679) tím, že uživatelům dává kontrolu nad tím, jak jsou jeho osobní údaje používány. Poskytuje vysokou úroveň doplňkovosti s novým aktem o kybernetické bezpečnosti a jeho společnými systémy certifikace kybernetické bezpečnosti. Potřeba jedinečné identity internetu věcí podle nařízení eIDAS rovněž zajišťuje soulad s aktem o kybernetické bezpečnosti a potřebu zahrnout vedle osob a společností širší okruh aktérů, jako jsou stroje, objekty, dodavatelé a zařízení internetu věcí.

Nařízení o jednotné digitální bráně má rovněž důležité body a je v souladu s touto iniciativou. Cílem nařízení o jednotné digitální bráně je plně modernizovat veřejné správní služby a usnadnit on-line přístup k informacím, správním postupům a asistenčním službám, které občané a podniky potřebují, když žijí nebo působí v jiné zemi EU. Tato iniciativa představuje základ pro splnění cíle, kterým je naplnit v rámci jednotné digitální brány zásadu „jen jednou“.

Kromě toho existuje soudržnost s evropskou strategií pro data a navrhovaným nařízením o evropské správě údajů, které poskytuje rámec na podporu aplikací založených na datech v případech, kdy je vyžadován přenos osobních údajů, což uživatelům umožňuje mít kontrolu a údaje plně anonymizovat.

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

Iniciativa bude vycházet ze stavebních bloků elektronické identifikace a služeb vytvářejících důvěru, které byly vyvinuty v rámci programu Nástroje pro propojení Evropy a které jsou integrovány do programu Digitální Evropa.

Členské státy mohou dále požádat o financování zřízení nebo zlepšení nezbytné infrastruktury z Nástroje pro oživení a odolnost.

1.6. Doba trvání a finanční dopad návrhu/podnětu

☐ Časově omezená doba trvání

☐ s platností od [DD.MM.]RRRR do [DD.MM.]RRRR,

☐ finanční dopad od RRRR do RRRR u prostředků na závazky a od RRRR do RRRR u prostředků na platby.

☒ Časově neomezená doba trvání

Provádění s obdobím rozběhu od RRRR do RRRR,

poté plné fungování.

1.7. Předpokládaný způsob řízení²⁹

☒ Přímé řízení Komisí

☒ prostřednictvím jejích útvarů, včetně jejích zaměstnanců v delegacích Unie,

☐ prostřednictvím výkonných agentur.

☐ Sdílené řízení s členskými státy

☐ **Nepřímé řízení**, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

☐ třetí země nebo subjekty určené těmito zeměmi,

☐ mezinárodní organizace a jejich agentury (upřesněte),

☐ EIB a Evropský investiční fond,

☐ subjekty uvedené v člancích 70 a 71 finančního nařízení,

☐ veřejnoprávní subjekty,

☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém poskytují dostatečné finanční záruky,

☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství soukromého a veřejného sektoru a poskytující dostatečné finanční záruky,

☐ osoby pověřené prováděním specifických akcí v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.

Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.

Poznámky

<p>[...]</p> <p>[...]</p>

²⁹

Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Nařízení bude poprvé přezkoumáno dva roky po svém plném uplatňování a poté každé čtyři roky. Komise musí o svých zjištěních podat zprávu Evropskému parlamentu a Radě.

V souvislosti s uplatňováním opatření navíc členské státy shromažďují statistické údaje týkající se používání a fungování evropské peněženky digitální identity a kvalifikovaných služeb vytvářejících důvěru. Statistické údaje se shromažďují ve zprávě, která se každoročně předkládá Komisi.

2.2. Systémy řízení a kontroly

2.2.1. *Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie*

Nařízení stanoví harmonizovanější pravidla pro poskytování služeb elektronické identifikace a služeb vytvářejících důvěru na vnitřním trhu a současně zajišťuje dodržování důvěry a kontrolu uživatelů nad vlastními údaji. Tato nová pravidla vyžadují vypracování technických specifikací a norem a dohled a koordinaci činností vnitrostátních orgánů. Související stavební prvky pro elektronickou identifikaci, elektronický podpis atd. budou navíc spravovány a poskytovány v rámci programu Digitální Evropa. Rovněž je třeba vzít v úvahu zdroje potřebné pro komunikaci a jednání o dohodě o vzájemném uznávání služeb vytvářejících důvěru se třetími zeměmi.

K plnění těchto úkolů je nutné poskytnout útvarům Komise náležité zdroje. Odhaduje se, že prosazování nového nařízení bude vyžadovat 11 plných pracovních úvazků; 4–5 plných pracovních úvazků zaměřených na právní činnost, 4–5 plných pracovních úvazků zaměřených na technickou práci a dva plné pracovní úvazky na koordinaci a mezinárodní informační a administrativní podporu.

2.2.2. *Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění*

Jedním z hlavních problémů vedoucích k nedostatkům současného legislativního rámce je nedostatečná harmonizace vnitrostátních systémů. V zájmu překonání tohoto problému v současné iniciativě bude potřeba spoléhat se na referenční normy a technické specifikace, které budou definovány v prováděcích aktech.

Při vypracovávání těchto prováděcích aktů bude Komisi nápomocna skupina odborníků. Komise bude navíc již nyní spolupracovat s členskými státy na dohodě o technické povaze budoucího systému, aby se během vyjednávání návrhu zabránilo další roztržitésti.

2.2.3. *Odhad a odůvodnění nákladové efektivity kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)*

Co se týče výdajů na schůze skupiny odborníků, vzhledem k nízké hodnotě na transakci (např. proplacení cestovních nákladů delegáta na schůzi, pokud je schůze fyzická) se standardní postupy vnitřní kontroly jeví jako dostatečné.

Rovněž pro pilotní projekty, které mají být prováděny v rámci programu Digitální Evropa, by měly postačovat standardní postupy GŘ CNECT.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření, např. opatření uvedená ve strategii pro boj proti podvodům.

Stávající opatření k předcházení podvodům vztahující se na Komisi budou zahrnovat dodatečné prostředky potřebné pro toto nařízení.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	Číslo		zemí ESVO ³¹	kandidátských zemí ³²	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
2	02 04 05 01 vyslání	RP/	ANO	NE	/NE	NE
2	02 01 30 01 podpůrné výdaje na program Digitální Evropa	NRP				
7	20 02 06 správní výdaje	NRP	NE			

Nové rozpočtové položky, jejichž vytvoření se požaduje

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	Číslo		zemí ESVO	kandidátských zemí	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
	[XX.YY.YY.YY]		ANO/NE	ANO/NE	ANO/NE	ANO/NE

³⁰ RP = rozlišené prostředky / NRP = nerozlišené prostředky.

³¹ ESVO: Evropské sdružení volného obchodu.

³² Kandidátské země a případně potenciální kandidáti ze západního Balkánu.

3.2. Odhadovaný finanční dopad návrhu na prostředky

3.2.1. Odhadovaný souhrnný dopad na operační prostředky

- ☐ Návrh/podnět nevyžaduje využití operačních prostředků.
- ☒ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	Číslo	2
------------------------------------------	--------------	----------

GŘ: CNECT			Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027		CELKEM
○ Operační prostředky			O přidělení rozpočtu bude rozhodnuto při vypracovávání pracovních programů. Uvedená čísla představují minimum potřebné pro údržbu a modernizaci ³³ .							
Rozpočtová položka ³⁴ 02 04 05	Závazky	(1a)	2,000	4,000	4,000	4,000	4,000	4,000		22,000
	Platby	(2a)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	22,000
Rozpočtová položka	Závazky	(1b)								
	Platby	(2b)								
Prostředky správní povahy financované z rámce na zvláštní programy ³⁵										
Rozpočtová položka 02 01 03 01		(3)	0,048	0,144	0,144	0,072	0,072	0,072		0,552
Prostředky na GŘ CNECT CELKEM	Závazky	=1a+1b +3	2,048	4,144	4,144	4,072	4,072	4,072		22,552
	Platby	=2a+2b +3	1,048	3,144	4,144	4,072	4,072	4,072	2,000	22,552

³³ Pokud skutečné náklady překročí uvedené částky, budou náklady financovány z položky 02 04 05 01.

³⁴ Podle oficiální rozpočtové nomenklatury.

³⁵ Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

○ Operační prostředky CELKEM	Závazky	(4)	2,000	4,000	4,000	4,000	4,000	4,000		22,000
	Platby	(5)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	22,000
○ Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)	0,048	0,144	0,144	0,072	0,072	0,072		0,552
CELKEM prostředky z OKRUHU 2 viceletého finančního rámce	Závazky	=4+6	2,048	4,144	4,144	4,072	4,072	4,072		22,552
	Platby	=5+6	0,048	4,144	4,144	4,072	4,072	4,072	2,000	22,552

Okruh víceletého finančního rámce	7	Správní výdaje
------------------------------------------	----------	----------------

Tento oddíl se vyplní pomocí „rozpočtových údajů správní povahy“, jež se nejprve uvedou v [příloze legislativního finančního výkazu](#) (příloha V interních pravidel), která se pro účely konzultace mezi útvary vloží do aplikace DECIDE.

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	CELKEM
GŘ: CNECT								
○ Lidské zdroje		0,776	1,470	1,470	1,470	1,470	1,318	7,974
○ Ostatní správní výdaje		0,006	0,087	0,087	0,087	0,016	0,016	0,299
CELKEM GŘ CNECT	Prostředky	0,782	1,557	1,557	1,557	1,486	1,334	8,273

Prostředky z OKRUHU 7 víceletého finančního rámce CELKEM	(Závazky celkem = platby celkem)	0,782	1,557	1,557	1,557	1,486	1,334	8,273
-------------------------------------------------------------------------	-------------------------------------	-------	-------	-------	-------	-------	-------	--------------

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027		CELKEM
Prostředky z OKRUHŮ 1 až 7 víceletého finančního rámce CELKEM	Závazky	2,830	5,701	5,701	5,629	5,558	5,408		30,825
	Platby	1,830	4,701	5,701	5,629	5,558	5,406	2,000	30,825

3.2.2. Odhadovaný výstup financovaný z operačních prostředků

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uved'te cíle a výstupy			Rok 2022		Rok 2023		Rok 2024		Rok 2025		Rok 2026		Rok 2027		CELKEM	
	↓	Druh 36	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet
SPECIFICKÝ CÍL č. 1 ³⁷ ...			Zajistit přístup k důvěryhodným a zabezpečeným řešením digitální identity, která lze použít přeshraničně a která splňují očekávání uživatelů a poptávku na trhu.													
Každoroční			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Mezisoučet za specifický cíl č. 1			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
SPECIFICKÝ CÍL č. 2 ...			Zajistit, aby se veřejné a soukromé služby mohly přeshraničně spoléhat na důvěryhodná a zabezpečená řešení digitální identity.													
Průzkumy/studie			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Mezisoučet za specifický cíl č. 2			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
SPECIFICKÝ CÍL č. 3 ...			Zajistit občanům plnou kontrolu nad jejich osobními údaji a zajistit jejich bezpečnost při používání řešení digitální identity.													
Průzkumy/studie			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Mezisoučet za specifický cíl č. 3			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
SPECIFICKÝ CÍL č. 4 ...			Zajistit rovné podmínky pro poskytování kvalifikovaných služeb vytvářejících důvěru v EU a jejich přijetí.													
Průzkumy/studie			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Mezisoučet za specifický cíl č. 4			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
CELKEM			4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	24	1,200

³⁶ Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).
³⁷ Popsaný v bodě 1.4.2. „Specifické cíle...“.

3.2.3. Odhadovaný souhrnný dopad na správní prostředky

- ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.
- ☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	CELKEM
--	-------------	-------------	-------------	-------------	-------------	-------------	--------

OKRUH 7 víceletého finančního rámce							
Lidské zdroje	0,776	1,470	1,470	1,470	1,470	1,318	7,974
Ostatní správní výdaje	0,006	0,087	0,087	0,087	0,0162	0,0162	0,299
Mezisoučet za OKRUH 7 víceletého finančního rámce	0,782	1,557	1,557	1,557	1,486	1,334	8,273

Mimo OKRUH 7³⁸ víceletého finančního rámce							
Lidské zdroje							
Ostatní výdaje správní povahy							
Vložit administrativní náklady v rámci programu Digitální Evropa	0,048	0,144	0,144	0,072	0,072	0,072	0 552
Mezisoučet mimo OKRUH 7 víceletého finančního rámce	0,048	0,144	0,144	0,072	0,072	0,072	0 552

CELKEM	0,830	1,701	1,701	1,629	1,558	1,406	8,825
---------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy budou pokryty z prostředků GRŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny v rámci GRŘ a případně doplněny z dodatečného přidělu, který lze řídicímu GRŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

³⁸ Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

3.2.4. Odhadované potřeby v oblasti lidských zdrojů

- ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.
- ☒ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v přepočtu na plné pracovní úvazky

	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027
20 01 02 01 (v ústředí a v zastoupeních Komise)	4	8	8	8	8	7
20 01 02 03 (při delegacích)						
01 01 01 01 (v nepřímém výzkumu)						
01 01 01 11 (v přímém výzkumu)						
Jiné rozpočtové položky (upřesněte)						
20 02 01 (SZ, VNO, ZAP z celkového rámce)	2	3	3	3	3	3
20 02 03 (SZ, MZ, VNO, ZAP a MOD při delegacích)						
XX 01 xx yy zz ³⁹	– v ústředí					
	– při delegacích					
01 01 01 02 (SZ, VNO, ZAP v nepřímém výzkumu)						
01 01 01 12 (SZ, VNO, ZAP v přímém výzkumu)						
Jiné rozpočtové položky (upřesněte)						
CELKEM	6	11	11	11	11	10

XX je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeořazeny v rámci GŘ, a případně doplněny z dodatečného přidělu, který lze řídicímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci	Úředníci budou zejména provádět právní činnost, koordinační činnosti a jednání se třetími zeměmi a subjekty v souvislosti se vzájemným uznáváním služeb vytvářejících důvěru.
Externí zaměstnanci	S technickým a funkčním uspořádáním systému by měli pomoci národní odborníci. SZ by se měli rovněž podílet na technických úkolech, včetně správy stavebních bloků.

³⁹ Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

3.2.5. Slučitelnost se stávajícím víceletým finančním rámcem

Návrh/podnět:

- ☒ může být v plném rozsahu financován přerozdělením prostředků v rámci příslušného okruhu víceletého finančního rámce (VFR).

Upřesněte, jaká úprava se požaduje, příslušné rozpočtové položky a odpovídající částky. V případě zásadní úpravy přiložte excelovou tabulku.

- ☐ vyžaduje použití nepřiděleného rozpětí v rámci příslušného okruhu VFR a/nebo použití zvláštních nástrojů definovaných v nařízení o VFR.

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky, odpovídající částky a navrhované nástroje, které mají být použity.

- ☐ vyžaduje revizi VFR.

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky a odpovídající částky.

3.2.6. Příspěvky třetích stran

Návrh/podnět:

- ☒ nepočítá se spolufinancováním od třetích stran.
- ☐ počítá se spolufinancováním od třetích stran podle následujícího odhadu:

prostředky v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok N ⁴⁰	Rok N+1	Rok N+2	Rok N+3	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			Celkem
Upřesněte spolufinancující subjekt								
Spolufinancované prostředky CELKEM								

⁴⁰ Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

3.3. Odhadovaný dopad na příjmy

☒ Návrh/podnět nemá žádný finanční dopad na příjmy.

☐ Návrh/podnět má tento finanční dopad:

☐ na vlastní zdroje

☐ na jiné příjmy

uved'te, zda je příjem účelově vázán na výdajové položky ☐

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová položka:	rozpočtová	Prostředky dostupné v běžném rozpočtovém roce	Dopad návrhu/podnětu ⁴¹					
			Rok N	Rok N+1	Rok N+2	Rok N+3	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)	
Článek								

U účelově vázaných příjmů upřesněte dotčené výdajové rozpočtové položky.

[...]

Jiné poznámky (např. způsob/vzorec výpočtu dopadu na příjmy nebo jiné údaje).

[...]

⁴¹ Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.

PŘÍLOHA
LEGISLATIVNÍHO FINANČNÍHO VÝKAZU

Název návrhu/podnětu:

Návrh nařízení o rámci pro evropskou digitální identitu, kterým se mění nařízení eIDAS

- 1. POTŘEBNÉ LIDSKÉ ZDROJE A NÁKLADY NA TYTO ZDROJE**
- 2. VÝŠE OSTATNÍCH VÝDAJŮ SPRÁVNÍ POVAHY**
- 3. CELKOVÉ SPRÁVNÍ NÁKLADY**
- 4. METODY VÝPOČTU POUŽITÉ K ODHADU NÁKLADŮ**
 - 4.1. Lidské zdroje**
 - 4.2. Ostatní správní výdaje**

Tato příloha musí být připojena k legislativnímu finančnímu výkazu při zahájení konzultací mezi jednotlivými útvary.

Tabulky s údaji slouží jako zdroj pro tabulky obsažené v legislativním finančním výkazu. Jsou určeny pouze pro interní použití v Komisi.

1) Náklady na potřebné lidské zdroje

- ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.
- ☒ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

HEADING 7 of the multiannual financial framework	Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL		
	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	
• Establishment plan posts (officials and temporary staff)															
20 01 02 01 - Headquarters and Representation offices	AD	4	608	7	1.064	7	1.064	7	1.064	7	1.064	6	912	38	5.776
	AST	0	-	1	152	1	152	1	152	1	152	1	152	5	760
20 01 02 03 - Union Delegations	AD														
	AST														
External staff [1]															
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC	1	82	1	82	1	82	1	82	1	82	1	82	6	492
	END	1	86	2	172	2	172	2	172	2	172	2	172	11	946
	INT														
20 02 03 – External personnel - Union Delegations	AC														
	AL														
	END														
	INT														
	JPD														
Other HR related budget lines (specify)															
Subtotal HR – HEADING 7		6	776	11	1.470	11	1.470	11	1.470	11	1.470	10	1.318	60	7.974

4.3. Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeočleněny v rámci GŘ, a případně doplněny z dodatečného přidělu, který lze řídicímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

4.4.

4.5.

Mimo OKRUH 7 víceletého finančního rámce		Rok 2022		Rok 2023		Rok 2024		Rok 2025		Rok 2026		Rok 2027		CELKEM	
		Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky
01 01 01 01 nepřímý výzkum ⁴² 01 01 01 11 přímý výzkum Jiné (upřesněte)	AD														
	AST														
Externí zaměstnanci financovaní z operačních prostředků (bývalé položky „BA“).	– v ústředí	SZ													
		VNO													
		ZAP													
	– při delegacích Unie	SZ													
		MZ													
		VNO													
		ZAP													
		MOD													
01 01 01 02 nepřímý výzkum 01 01 01 12 přímý výzkum Jiné (upřesněte) ⁴³	SZ														
	VNO														
	ZAP														
Jiné rozpočtové položky související s HR (upřesněte)															

⁴² Vyberte příslušnou rozpočtovou položku nebo v případě potřeby upřesněte jinou; v případě většího počtu rozpočtových položek by měli být zaměstnanci rozlišeni podle jednotlivých dotčených rozpočtových položek

⁴³ Vyberte příslušnou rozpočtovou položku nebo v případě potřeby upřesněte jinou; v případě většího počtu rozpočtových položek by měli být zaměstnanci rozlišeni podle jednotlivých dotčených rozpočtových položek

Mezisoučet HR – mimo OKRUH 7															
Celkem HR (všechny okruhy VFR)		6	0,776	11	1,470	11	1,470	11	1,470	11	1,470	10	1,318	60	7,974

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GR, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeoobsazeny v rámci GR, a případně doplněny z dodatečného přidělu, který lze řídicímu GR poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

4.6. Výše ostatních správních výdajů

4.7. ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy

4.8. ☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

OKRUH 7 víceletého finančního rámce	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Celkem
V ústředí nebo na území EU:							
20 02 06 01 – Náklady na služební cesty a reprezentaci	0,006	0,015	0,015	0,015	0,015	0,015	0,081
20 02 06 02 – Náklady na konference a zasedání							
20 02 06 03 – Výbory ⁴⁴		0,072	0,072	0,072	0,0012	0,012	0,218
20 02 06 04 – Studie a konzultace							
20 04 – Výdaje na informační technologie (podnikové) ⁴⁵							
Jiné rozpočtové položky nesouvisející s HR (podle potřeby upřesněte)							
Při delegacích Unie:							
20 02 07 01 – Náklady na služební cesty, konference a reprezentaci							
20 02 07 02 – Další vzdělávání zaměstnanců							
20 03 05 – Infrastruktura a logistika							
Jiné rozpočtové položky nesouvisející s HR (podle potřeby upřesněte)							
Mezisoučet jiné – OKRUH 7 víceletého finančního rámce	0,006	0,087	0,087	0,087	0,016	0,016	0,299

⁴⁴ Upřesněte druh výboru a skupinu, do níž náleží.

⁴⁵ Vyžaduje se stanovisko GR DIGIT – investičního týmu IT (viz Pokyny pro financování IT, C(2020) 6126 final ze dne 10. září 2020, s. 7)

v milionech EUR (zaokrouhleno na tři desetinná místa)

Mimo OKRUH 7 víceletého finančního rámce	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Celkem
Výdaje na technickou a administrativní pomoc (mimo externí zaměstnance) z operačních prostředků (bývalé položky „BA“):	0,048	0,144	0,144	0,072	0,072	0,072	0,552
– v ústředí							
– při delegacích Unie							
Ostatní výdaje na řízení v oblasti výzkumu							
Výdaje politiky v oblasti informačních technologií na operační programy ⁴⁶							
Výdaje podniků na informační technologie na operační programy ⁴⁷							
Jiné rozpočtové položky nesouvisející s HR (podle potřeby upřesněte)							
Mezisoučet jiné – mimo OKRUH 7 víceletého finančního rámce	0,048	0,144	0,144	0,072	0,072	0,072	0,552
Ostatní správní výdaje celkem (všechny okruhy VFR)	0,054	0,231	0,231	0,159	0,088	0,088	0,851

⁴⁶ Vyžaduje se stanovisko GŘ DIGIT – investičního týmu IT (viz Pokyny pro financování IT, C(2020) 6126 final ze dne 10. září 2020, s. 7)

⁴⁷ Tato položka zahrnuje místní správní systémy a příspěvky na spolufinancování podnikových IT systémů (viz Pokyny pro financování IT, C(2020) 6126 final ze dne 10. září 2020)

5. CELKOVÉ SPRÁVNÍ NÁKLADY (VŠECHNY OKRUHY VFR)

v milionech EUR (zaokrouhleno na tři desetinná místa)

Souhrn	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Celkem
Okruh 7 – Lidské zdroje	0,776	1,470	1,470	1,470	1,470	1,318	7,974
Okruh 7 – Ostatní správní výdaje	0,006	0,087	0,087	0,087	0,016	0,016	0,218
Mezisoučet okruhu 7							
Mimo okruh 7 – Lidské zdroje							
Mimo okruh 7 – Ostatní správní výdaje	0,048	0,144	0,144	0,072	0,072	0,072	0,552
Mezisoučet – ostatní okruhy							
1. CELKEM							
2. za OKRUH 7 a mimo OKRUH 7	0,830	1,701	1,701	1,629	1,558	1,406	8,825

- 1) Potřeby v oblasti správních prostředků budou pokryty z prostředků, které jsou již vyčleněny na řízení akce a/nebo byly přesunuty, a případně doplněny z dodatečného přidělu, který lze řídicímu GŘ poskytnout v rámci ročního přidělování a s ohledem na stávající rozpočtová omezení.

6. METODY VÝPOČTU POUŽITÉ K ODHADU NÁKLADŮ

a) Lidské zdroje

Tato část objasňuje metodu výpočtu použitou k odhadu potřebných lidských zdrojů (předpokládané pracovní vytížení, včetně konkrétních pracovních míst (pracovní profily Sysper 2), kategorie zaměstnanců a příslušné průměrné náklady)

1.	OKRUH 7 víceletého finančního rámce
2.	<u>POZN.: Průměrné náklady na každou kategorii zaměstnanců v ústředí jsou k dispozici na stránkách BudgWeb:</u>
3.	<u>https://my.intracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx</u>
4.	<input type="radio"/> Úředníci a dočasní zaměstnanci
5.	<u>7 úředníků AD (včetně 1 z CNECT/F.3 v letech 2023–2024) x 152 000 EUR / rok v letech 2023–2027 (polovina z toho v roce 2022 vzhledem k očekávanému přijetí v polovině roku 2022):</u>
6.	<u>1 úředník AST x 152 000 EUR / rok v letech 2023–2027 (polovina z toho v roce 2022 vzhledem k očekávanému přijetí v polovině roku 2022)</u>
7.	
8.	<input type="radio"/> Externí zaměstnanci
9.	<u>SZ: 1 x 82 000 EUR / rok v letech 2023–2027 (polovina z toho v roce 2022 vzhledem k očekávanému přijetí v polovině roku 2022) (použit indexační faktor):</u>
10.	<u>END 2 x 86 000 EUR / rok v letech 2023–2027 (polovina z toho v roce 2022 vzhledem k očekávanému přijetí v polovině roku 2022) (použit indexový faktor):</u>
11.	

12.	Mimo OKRUH 7 víceletého finančního rámce
13.	<input type="radio"/> Pouze pracovní místa financovaná z rozpočtu na výzkum
14.	
15.	<input type="radio"/> Externí zaměstnanci
16.	

7. OSTATNÍ SPRÁVNÍ VÝDAJE

Uveďte podrobnosti o metodě výpočtu použité pro jednotlivé rozpočtové položky, a zejména příslušné předpoklady (např. počet zasedání za rok, průměrné náklady atd.).

17.	OKRUH 7 víceletého finančního rámce
18.	<u>Dvouměsíční zasedání výborů x 12 000 EUR / zasedání 2022–2024 za účelem přijetí prováděcích aktů. Poté výroční zasedání výboru za účelem přijetí aktualizovaných prováděcích aktů.</u>
19.	<u>Služební cesty jsou především cesty do Lucemburku a Bruselu, jedná se ale také o účast na konferencích, setkáních s členskými státy a dalšími zúčastněnými stranami.</u>
20.	

21.	Mimo OKRUH 7 víceletého finančního rámce
22.	<u>Zasedání skupin odborníků budou účtována správní části programu Digitální Evropa.</u>
23.	<u>Očekává se, že se během přípravy prováděcího aktu (v polovině období 2022–2024) budou konat měsíční zasedání (náklady ve výši 12 000 EUR), a mimo toto období se plánují dvouměsíční zasedání, aby se zajistila koordinace v rámci celé EU týkající se technického provádění.</u>
24.	