

V Bruseli 3. júna 2021
(OR. en)

9471/21

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

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

NÁVRH

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	3. júna 2021
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	COM(2021) 281 final
Predmet:	Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o stanovenie rámca pre európsku digitálnu identitu

Delegáciám v prílohe zasielame dokument COM(2021) 281 final.

Príloha: COM(2021) 281 final



V Bruseli 3. 6. 2021
COM(2021) 281 final

2021/0136 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,

**ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o stanovenie rámca pre
európsku digitálnu identitu**

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

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Táto dôvodová správa je sprievodným dokumentom k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa mení a dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (nariadenie eIDAS)¹. Cieľom tohto právneho nástroja je na účely cezhraničného použitia zabezpečiť:

- prístup k vysoko bezpečným a dôveryhodným riešeniam v oblasti elektronickej totožnosti,
- aby sa verejné a súkromné služby mohli spoliehať na dôveryhodné a bezpečné riešenia v oblasti digitálnej identity,
- aby fyzické a právnické osoby boli oprávnené používať riešenia v oblasti digitálnej identity,
- aby tieto riešenia boli prepojené s rôznymi atribútmi a umožňovali cieľnú výmenu údajov o totožnosti obmedzenú na potreby konkrétnej požadovanej služby,
- akceptáciu kvalifikovaných dôveryhodných služieb v EÚ a rovnaké podmienky na ich poskytovanie.

Na trhu vzniká nové prostredie, v ktorom sa pozornosť presunula od poskytovania a používania pevných digitálnych identít k poskytovaniu špecifických atribútov súvisiacich s týmito identitami a spoliehaniu sa na ne. Existuje zvýšený dopyt po riešeniach v oblasti elektronickej totožnosti, ktorými možno zaistiť tieto schopnosti prinášajúce vyššiu efektívnosť a vysokú úroveň dôvery v celej EÚ, a to v súkromnom aj vo verejnom sektore, vychádzajúc z potreby identifikovať a overovať používateľov s vysokou úrovňou zabezpečenia.

Z hodnotenia nariadenia eIDAS² vyplynulo, že súčasné nariadenie nedostatočne rieši tieto nové požiadavky trhu, najmä z dôvodu svojich prirodzených obmedzení pre verejný sektor, obmedzených možností a zložitosti pripojenia sa súkromných online poskytovateľov k systému, nedostatočnej dostupnosti oznámených riešení v oblasti elektronickej identifikácie vo všetkých členských štátoch a nedostatočnej flexibilitate podporovať rôzne prípady použitia. Okrem toho riešenia v oblasti totožnosti, ktoré nepatria do rozsahu pôsobnosti nariadenia eIDAS, napríklad riešenia ponúkané poskytovateľmi sociálnych médií a finančnými inštitúciami, vyvolávajú obavy, pokiaľ ide o ochranu súkromia a údajov. Tieto riešenia nie sú schopné účinne reagovať na nové požiadavky trhu a nemajú dostatočné cezhraničné pokrytie na riešenie konkrétnych potrieb sektorov, v ktorých je identifikácia citlivá a vyžaduje vysoký stupeň istoty.

Len 14 členských štátov oznámilo aspoň jednu schému elektronickej identifikácie od nadobudnutia účinnosti časti nariadenia týkajúcej sa elektronickej identifikácie v septembri 2018. V dôsledku toho len 59 % osôb s pobytom v EÚ má cezhraničný prístup k dôveryhodným a bezpečným schémam elektronickej identifikácie. Len sedem schém je plne

¹ Ú. v. EÚ L 257/73 z 28.8.2014.

² [pridať odkaz po prijatí].

mobilných a reaguje na súčasné očakávania používateľov. Keďže nie všetky technické uzly na zabezpečenie pripojenia k rámcu interoperability eIDAS sú plne funkčné, cezhraničný prístup je obmedzený a len veľmi malý počet online verejných služieb, ktoré sú prístupné doma, je prístupný cezhranične prostredníctvom siete eIDAS.

Poskytnutím rámca európskej digitálnej identity na základe revízie súčasného rámca by do roku 2030 malo mať aspoň 80 % občanov možnosť používať riešenie v oblasti digitálnej identity na prístup ku kľúčovým verejným službám. Okrem toho vďaka bezpečnosti a kontrole, ktoré ponúka rámec európskej digitálnej identity, by občania a osoby s pobytom mali mať plnú dôveru v to, že európsky rámec digitálnej identity ponúkne každému prostriedky na kontrolu nad tým, kto má prístup k ich digitálnemu dvojčat'u a presne ku ktorým údajom. To si bude vyžadovať vysokú úroveň bezpečnosti vzhľadom na všetky aspekty poskytovania digitálnej identity vrátane vydávania európskej peňaženky digitálnej identity a infraštruktúry na získavanie, uchovávanie a poskytovanie údajov o digitálnej identite.

Súčasný rámec eIDAS sa okrem toho nevzťahuje na poskytovanie elektronických atribútov, napríklad osvedčení o zdravotnom stave alebo odbornej kvalifikácii, čo sťažuje zaistenie celoeurópskeho právneho uznávania takýchto potvrdení v elektronickej forme. Navyše nariadenie eIDAS neumožňuje používateľom obmedziť výmenu údajov o totožnosti, čo je absolútne nevyhnutné na poskytovanie služby.

Hoci z hodnotenia nariadenia eIDAS vyplýva, že rámec pre poskytovanie dôveryhodných služieb je pomerne úspešný, pretože poskytuje vysokú mieru dôvery a zabezpečuje zavádzanie a používanie väčšiny dôveryhodných služieb, na dosiahnutie úplnej harmonizácie a akceptácie je potrebné urobiť viac. V prípade kvalifikovaných certifikátov autentifikácie webových sídiel musia mať občania možnosť spoliehať sa na ne a využívať bezpečné a dôveryhodné informácie o tom, kto je za webovým sídlom, čím sa zníži počet podvodov.

Okrem toho v snahe reagovať na dynamiku trhov a technologický vývoj sa týmto návrhom rozširuje súčasný dôveryhodný zoznam služieb eIDAS o tri nové kvalifikované dôveryhodné služby, konkrétne poskytovanie služieb elektronickej archivácie, elektronickej registre a spravovanie zariadení na vyhotovenie elektronického podpisu a elektronickej pečate na diaľku.

Návrh ďalej ponúka harmonizovaný prístup k bezpečnosti, a to tak občanom spoliehajúcim sa na európsku digitálnu identitu, ktorá ich zastupuje online, ako aj poskytovateľom online služieb, ktorí sa budú môcť v plnej miere spoliehať na riešenia v oblasti digitálnej identity a akceptovať ich nezávisle od toho, kde boli vydané. Z tohto návrhu vyplýva posun pre vydavateľov riešení v oblasti európskej digitálnej identity, pretože poskytuje spoločnú technickú infraštruktúru, referenčný rámec a spoločné normy, ktoré sa majú vypracovať v spolupráci s členskými štátmi. Harmonizovaný prístup je nevyhnutný, aby sa zabránilo tomu, že vývoj nových riešení v oblasti digitálnej identity v členských štátoch spôsobí ďalšiu fragmentáciu vyvolanú používaním odlišných vnútroštátnych riešení. Harmonizovaný prístup zároveň posilní jednotný trh, pretože pri prístupe k verejným aj súkromným službám by občanom, iným osobám s pobytom a podnikom umožňoval identifikovať sa online bezpečným, pohodlným a jednotným spôsobom v celej EÚ. Používatelia by sa mohli spoliehať na vylepšený ekosystém pre elektronickú totožnosť a dôveryhodné služby uznávané a akceptované všade v Únii.

Aby sa predišlo fragmentácii a prekážkam z dôvodu odlišných noriem, Komisia prijme odporúčanie v rovnakom čase ako tento návrh. V odporúčaní bude stanovený proces na podporu spoločného prístupu, ktorý členským štátom a ďalším príslušným zainteresovaným stranám z verejného aj súkromného sektora umožní v úzkej spolupráci s Komisiou pracovať na vývoji súboru nástrojov na predchádzanie odlišným prístupom a zamedzenie ohrozeniu budúceho vykonávania rámca európskej digitálnej identity.

- **Súlad s existujúcimi ustanoveniami v tejto oblasti politiky**

Tento návrh vychádza zo súčasného nariadenia eIDAS, úlohy členských štátov ako poskytovateľov právnych totožností a rámca pre poskytovanie dôveryhodných elektronických služieb v Európskej únii. Návrh dopĺňa iné nástroje politiky na úrovni EÚ a je v súlade s nimi s cieľom premietnuť výhody vnútorného trhu do digitálneho sveta, najmä rozšírením možností cezhraničného prístupu k službám pre občanov. V tejto súvislosti sa návrhom vykonáva politický mandát udelený Európskou radou³ a predsedníčkou Európskej komisie⁴, a to vytvoriť celoúnijský rámec pre verejnú elektronickú identifikáciu, ktorým sa zaisťuje, že všetci občania alebo osoby s pobytom môžu mať prístup k bezpečnej európskej elektronickej totožnosti, ktorú možno použiť kdekoľvek v EÚ na identifikáciu a autentifikáciu pri prístupe k službám vo verejnom aj v súkromnom sektore, čo občanom umožní kontrolovať, ktoré údaje sú poskytované a ako sú používané.

- **Súlad s ostatnými politikami Únie**

Návrh je v súlade s prioritami digitálnej transformácie stanovenými v stratégii Formovanie digitálnej budúcnosti Európy⁵ a podporí dosiahnutie cieľov uvedených v oznámení o digitálnom desaťročí⁶. Každé spracúvanie osobných údajov podľa tohto nariadenia by sa malo vykonávať v plnom súlade so všeobecným nariadením o ochrane údajov (ďalej len „všeobecné nariadenie o ochrane údajov“)⁷. Týmto nariadením sa okrem toho zavádzajú osobitné záruky ochrany údajov.

V snahe zabezpečiť vysokú úroveň bezpečnosti je návrh zároveň v súlade s politikami Únie v oblasti kybernetickej bezpečnosti⁸. Cieľom návrhu je znížiť fragmentáciu uplatnením všeobecných požiadaviek kybernetickej bezpečnosti na poskytovateľov dôveryhodných služieb, na ktorých sa vzťahuje nariadenie eIDAS.

Návrh je ďalej v súlade s inými sektorovými politikami, ktoré vychádzajú z používania elektronických totožností, elektronických osvedčení atribútov a iných dôveryhodných služieb. Zahŕňa to nariadenie o jednotnej digitálnej bráne⁹, požiadavky, ktoré sa majú splniť vo finančnom sektore v súvislosti s bojom proti praniu špinavých peňazí a financovaniu

³ <https://www.consilium.europa.eu/media/45930/021020-euco-final-conclusions-sk.pdf>.

⁴ Správa o stave Únie zo 16. septembra 2020, pozri https://ec.europa.eu/commission/presscorner/detail/sk/SPEECH_20_1655.

⁵ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Formovanie digitálnej budúcnosti Európy.

⁶ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Digitálny kompas do roku 2030: digitálne desaťročie na európsky spôsob.

⁷ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (Ú. v. EÚ L 119, 4.5.2016, s. 1).

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

⁹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1724 z 2. októbra 2018 o zriadení jednotnej digitálnej brány na poskytovanie prístupu k informáciám, postupom a asistenčným službám a službám riešenia problémov a o zmene nariadenia (EÚ) č. 1024/2012 (Ú. v. EÚ L 295, 21.11.2018, s. 1).

terorizmu, iniciatívy zamerané na výmenu potvrdení týkajúcich sa sociálneho zabezpečenia, digitálne vodičské preukazy alebo budúce digitálne cestovné doklady a iné iniciatívy zamerané na znižovanie administratívnej záťaže pre občanov a podniky, ktoré v plnej miere vychádzajú z možností ponúkaných digitálnou transformáciou postupov vo verejnom aj v súkromnom sektore. Peňaženka okrem toho umožní kvalifikované elektronické podpisy, ktoré môžu uľahčiť politickú účasť¹⁰.

2. PRÁVNÝ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právny základ

Cieľom tejto iniciatívy je podporiť transformáciu Únie smerom k digitálnemu jednotnému trhu. S rastúcou digitalizáciou cezhraničných verejných a súkromných služieb, ktoré sa spoliehajú na používanie riešení v oblasti digitálnej identity, vzniká riziko, že v rámci súčasného právneho rámca budú občania čeliť prekážkam a nebudú môcť v plnej miere a jednoducho využívať online služby v celej EÚ a chrániť si svoje súkromie. Takisto existuje riziko, že nedostatky súčasného právneho rámca pre dôveryhodné služby by zvýšili fragmentáciu a znížili dôveru, ak by boli ponechané výlučne na členské štáty. Preto sa článok 114 ZFEÚ určil ako príslušný právny základ tejto iniciatívy.

• Subsidiarita (v prípade inej ako výlučnej právomoci)

Občania a podniky by mali mať možnosť využívať dostupnosť vysoko bezpečných a dôveryhodných riešení v oblasti digitálnej identity, ktoré možno používať v celej EÚ, ako aj prenosnosť elektronických osvedčení atribútov súvisiacich s totožnosťou. Najnovší technologický vývoj, požiadavky trhu a používateľov si vyžadujú dostupnosť používateľsky ústretovejších cezhraničných riešení umožňujúcich prístup k online službám v rámci celej EÚ, čo nariadením eIDAS v jeho súčasnej podobe nemožno zabezpečiť.

Používatelia sú takisto čoraz viac zvyknutí na globálne dostupné riešenia, napríklad keď akceptujú používanie riešení jednotného systému prihlasovania poskytovaných väčšími platformami sociálnych médií na prístup k online službám. Samotné členské štáty nemôžu riešiť problémy, ktoré v dôsledku toho vznikajú, pokiaľ ide o trhovú silu veľkých poskytovateľov, čo si vyžaduje interoperabilitu a dôveryhodné elektronické identifikácie na úrovni EÚ. Okrem toho elektronické osvedčenia atribútov vydané a akceptované v jednom členskom štáte, napríklad elektronický zdravotný certifikát, často nie sú právne uznávané alebo akceptované v iných členských štátoch. Tým vzniká riziko, že členské štáty budú pokračovať vo vývoji fragmentovaných vnútroštátnych riešení, ktoré nemôžu fungovať cezhranične.

Vnútroštátne postupy takisto vedú k riziku zvýšenej fragmentácie, pokiaľ ide o poskytovanie dôveryhodných služieb, hoci je vo veľkej miere upravené a funguje v súlade so súčasným právnym rámcom.

Zásah na úrovni EÚ je napokon najvhodnejším prostriedkom, ako poskytnúť občanom a podnikom prostriedky na cezhraničnú identifikáciu a výmenu osobných atribútov a potvrdení totožnosti s použitím vysoko bezpečných a dôveryhodných riešení v oblasti digitálnej identity v súlade s pravidlami EÚ v oblasti ochrany údajov. Táto situácia si vyžaduje dôveryhodnú a bezpečnú elektronickú identifikáciu a regulačný rámec, ktorým sa prepojí s atribútmi a potvrdeniami na úrovni EÚ. Iba zásahom na úrovni EÚ možno stanoviť harmonizované podmienky zabezpečujúce používateľskú kontrolu, prístup k cezhraničným online digitálnym službám a rámec interoperability, ktorý online službám uľahčí spoliehanie sa na používanie bezpečných riešení v oblasti digitálnej identity bez ohľadu na to, kde v EÚ bola vydaná alebo kde

¹⁰ Akčný plán pre európsku demokraciu, COM(2020) 790 final.

má občan bydlisko. Ako sa vo veľkej miere uvádza v preskúmaní nariadenia eIDAS, je nepravdepodobné, že vnútroštátny zásah by bol rovnako efektívny a účinný.

- **Proporcionalita**

Táto iniciatíva je primeraná k požadovaným cieľom a poskytuje vhodný nástroj na stanovenie potrebnej štruktúry interoperability na vytvorenie ekosystému európskej digitálnej identity vychádzajúceho z právnych totožností vydaných členskými štátmi a poskytovania kvalifikovaných a nekvalifikovaných atribútov digitálnej identity. Je jasným prínosom k dosiahnutiu cieľa zlepšiť digitálny jednotný trh prostredníctvom harmonizovanejšieho právneho rámca. Harmonizovanými európskymi peňaženkami digitálnej identity, ktoré budú vydávať členské štáty na základe spoločných technických noriem, sa takisto zabezpečuje spoločný prístup EÚ v prospech používateľov a strán spoliehajúcich sa na dostupnosť bezpečných cezhraničných riešení v oblasti elektronickej totožnosti. Táto iniciatíva sa zaoberá obmedzeniami súčasnej infraštruktúry interoperability elektronickej identifikácie založenej na vzájomnom uznávaní rôznych vnútroštátnych schém elektronickej identifikácie. Vzhľadom na stanovené ciele sa táto iniciatíva považuje za dostatočne primeranú a náklady za pravdepodobne zodpovedajúce potenciálnym prínosom. Navrhované nariadenie povedie k vzniku finančných a administratívnych nákladov, ktoré budú znášať členské štáty ako vydavatelia európskych peňažienok digitálnej identity, poskytovatelia dôveryhodných služieb a poskytovatelia online služieb. Tieto náklady však pravdepodobne vykompenzujú významné potenciálne prínosy pre občanov a používateľov plynúce priamo zo zvýšenia cezhraničného uznávania a akceptácie elektronickej totožnosti a služieb v oblasti atribútov.

Ak sa má dosiahnuť cieľ, ktorým je použiteľnosť a dostupnosť, nedá sa vyhnúť nákladom vyplývajúcim z tvorby a zosúladenia nových noriem pre poskytovateľov dôveryhodných služieb. Cieľom iniciatívy je využiť investície, ktoré už členské štáty vynaložili v rámci svojich vnútroštátnych schém identifikácie, a stavať na týchto investíciách. Navyše účelom dodatočných nákladov je podporiť harmonizáciu, pričom vzhľadom na očakávanie, že z dlhodobého hľadiska znížia administratívnu záťaž a náklady na dodržiavanie predpisov, sú tieto náklady opodstatnené. Náklady spojené s akceptáciou atribútov autentifikácie digitálnej identity v regulovaných sektoroch takisto možno považovať za nevyhnutné a primerané, pokiaľ sa nimi zabezpečí podpora celkového cieľa a prostriedky, pomocou ktorých regulované sektory budú môcť plniť právne povinnosti identifikovať používateľa zákonným spôsobom.

- **Výber nástroja**

Výber nariadenia ako právneho nástroja je odôvodnený potrebou zaistiť jednotné podmienky na vnútornom trhu na uplatňovanie európskej digitálnej identity prostredníctvom harmonizovaného rámca, ktorého cieľom je vytvoriť bezproblémovú interoperabilitu a poskytovať európskym občanom a spoločnostiam verejné a súkromné služby v celej Únii s vysoko bezpečnými a dôveryhodnými elektronickými identifikáciami.

3. VÝSLEDKY HODNOTENÍ *EX POST*, KONZULTÁCIÍ SO ZAJINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

- **Hodnotenia *ex post*/kontroly vhodnosti existujúcich právnych predpisov**

Hodnotenie fungovania nariadenia eIDAS bolo vykonané v rámci procesu preskúmania požadovaného v článku 49 nariadenia eIDAS. Pokiaľ ide o elektronickú totožnosť, hlavným zistením hodnotenia je, že nariadenie nedosiahlo svoj potenciál. Bol oznámený len obmedzený počet elektronických identifikácií, čo predstavuje obmedzené pokrytie obyvateľstva EÚ oznámenými schémami elektronickej identifikácie približne na 59 %.

Okrem toho je obmedzená aj akceptácia oznámených elektronických identifikácií na úrovni členských štátov aj poskytovateľov služieb. Ďalej sa zdá, že len niekoľko služieb dostupných prostredníctvom vnútroštátnej elektronickej identifikácie je pripojených do vnútroštátnej infraštruktúry eIDAS. Z hodnotiacej štúdie takisto vyplýva, že súčasný rozsah pôsobnosti a zameranie nariadenia eIDAS na schémy elektronickej identifikácie oznámené členskými štátmi EÚ a na umožnenie prístupu k online verejným službám sa zdajú byť príliš obmedzené a nedostatočné. Prevažná väčšina potrieb v oblasti elektronickej totožnosti a autentifikácie na diaľku je spojená so súkromným sektorom, najmä bankovými subjektmi, telekomunikačnými operátormi a operátormi platforiem, ktorí sú zo zákona povinní overovať totožnosť svojich zákazníkov. Pridaná hodnota nariadenia eIDAS, pokiaľ ide o elektronickú totožnosť, je obmedzená z dôvodu jeho nedostatočného rozsahu pôsobnosti, uplatňovania a používania.

Problémy identifikované v tomto návrhu súvisia s nedostatkami súčasného rámca eIDAS a zásadnými zmenami prostredia, ktoré sa týkajú trhov, spoločenského a technologického rozvoja a vyvolávajú nové potreby používateľov a trhu.

- **Konzultácie so zainteresovanými stranami**

Verejná konzultácia bola spustená 24. júla 2020 a ukončená 2. októbra 2020. Celkovo bolo Komisii doručených 318 príspevkov. Komisii bolo doručených aj 106 odpovedí na cieľný prieskum zainteresovaných strán. Zozbierali sa aj stanoviská členských štátov poskytnuté na rôznych bilaterálnych a multilaterálnych stretnutiach a v rámci prieskumov organizovaných od začiatku roka 2020. Ide najmä o prieskum medzi zástupcami členských štátov siete spolupráce eIDAS vykonaný v júli a auguste 2020 a rôzne špecializované semináre. Komisia viedla aj hĺbkové rozhovory so zástupcami sektorov a na bilaterálnych stretnutiach sa stretla so zainteresovanými stranami z podnikateľského prostredia z viacerých sektorov (napr. elektronický obchod, zdravotníctvo, finančné služby, telekomunikační operátori, výrobcovia zariadení atď.).

Veľká väčšina respondentov v rámci otvorenej verejnej konzultácie privítala vytvorenie jednotnej a všeobecne uznávanej digitálnej identity vychádzajúcej z právnych totožností vydaných členskými štátmi. Členské štáty do veľkej miery podporujú potrebu posilniť súčasné nariadenie eIDAS poskytnutím možnosti občanom mať prístup k verejným aj súkromným službám a uvedomujú si potrebu vytvoriť dôveryhodnú službu, ktorá umožní vydávanie a cezhraničné použitie elektronických osvedčení atribútov. Členské štáty celkovo zdôraznili potrebu vybudovať rámec európskej digitálnej identity na základe skúseností a silných stránok riešení na vnútroštátnej úrovni s cieľom nájsť synergie a mať prospech z vynaložených investícií. Mnohé zainteresované strany poukázali na to, ako pandémia ochorenia COVID-19 preukázala význam, ktorý má bezpečná identifikácia na diaľku pre všetkých, pokiaľ ide o prístup k verejným a súkromným službám. V súvislosti s dôveryhodnými službami väčšina aktérov súhlasí, že súčasný rámec je úspechom, ale sú potrebné niektoré dodatočné opatrenia na ďalšiu harmonizáciu určitých postupov súvisiacich s identifikáciou na diaľku a vnútroštátnym dohľadom. Zainteresované strany s prevažne vnútroštátnou zákazníckou základňou vyjadrili väčšie pochybnosti o pridanej hodnote rámca európskej digitálnej identity.

Verejný a súkromný sektor čoraz viac vníma peňaženky digitálnej identity ako najvhodnejší nástroj, ktorý používateľom dáva možnosť vybrať si, kedy a ktorým poskytovateľom súkromných služieb poskytnú rôzne atribúty v závislosti od prípadu použitia a zabezpečenia potrebného na príslušnú transakciu. Digitálne identity založené na digitálnych peňaženkách bezpečne uložených v mobilných zariadeniach boli označené ako hlavný prínos nadčasového riešenia. Súkromný trh (napr. Apple, Google, Thales) a vlády sa už týmto smerom uberajú.

- **Získavanie a využívanie expertízy**

Návrh vychádza z informácií získaných v rámci konzultácie so zainteresovanými stranami na účely správy o posúdení vplyvu a hodnotiacej správy nariadenia eIDAS vzhľadom na povinnosti preskúmania uvedené v článku 49 nariadenia eIDAS. So zástupcami členských štátov a expertmi sa zorganizovalo mnoho stretnutí.

- **Posúdenie vplyvu**

V súvislosti s týmto návrhom sa vykonalo posúdenie vplyvu. Výbor pre kontrolu regulácie vydal 19. marca 2021 zamietavé stanovisko s niekoľkými pripomienkami. Po opätovnom predložení upravenej verzie výbor 5. mája 2021 vydal kladné stanovisko.

Komisia skúma rôzne možnosti politiky na dosiahnutie všeobecného cieľa súčasnej iniciatívy, ktorým je zabezpečiť riadne fungovanie vnútorného trhu, najmä vo vzťahu k poskytovaniu a používaniu vysoko bezpečných a dôveryhodných riešení v oblasti elektronickej totožnosti.

Posúdenie vplyvu skúma základný scenár, možnosti politiky a ich vplyvy na tri posudzované možnosti politiky. Každá možnosť predstavuje výber na politické uváženie na základe úrovne ambícií. Prvá možnosť predstavuje nízku úroveň ambícií a súbor opatrení zameraných najmä na posilnenie účinnosti a efektívnosti súčasného nariadenia eIDAS. Prvá možnosť, ktorá predpokladá zavedenie povinného oznamovania vnútroštátnych schém elektronickej identifikácie a zjednodušenie súčasných nástrojov dostupných na dosiahnutie vzájomného uznávania, vychádza zo splnenia potrieb občanov spoliehaním sa na dostupnosť rôznych vnútroštátnych schém elektronickej identifikácie, ktorých cieľom je stať sa interoperabilnými.

Druhá možnosť predstavuje strednú úroveň ambícií a jej cieľom je najmä rozšíriť možnosti bezpečnej výmeny údajov súvisiacich s totožnosťou doplnením štátnych schém elektronickej identifikácie a podporením súčasného posunu smerom k službám identifikácie založenej na atribútoch. Cieľom tejto možnosti by bolo splnenie požiadaviek používateľov a vytvorenie novej kvalifikovanej dôveryhodnej služby na poskytovanie elektronických osvedčení atribútov, ktoré by boli prepojené na dôveryhodné zdroje a vykonateľné cezhranične. Tým by sa rozšíril rozsah pôsobnosti súčasného nariadenia eIDAS a podporilo by sa čo najviac prípadov použitia vychádzajúcich z potreby overiť s vysokou úrovňou zabezpečenia atribúty totožnosti spojené s osobou.

Tretia, uprednostňovaná možnosť, predstavuje najvyššiu úroveň ambícií a jej cieľom je regulovať poskytovanie vysoko bezpečnej osobnej peňaženky digitálnej identity vydannej členskými štátmi. Usúdilo sa, že v rámci uprednostňovanej možnosti možno plniť ciele tejto iniciatívy najúčinnšie. Aby sa ciele politiky naplnili v plnom rozsahu, uprednostňovaná možnosť vychádza z väčšiny opatrení posúdených v rámci prvej (spoliehanie sa na právne totožnosti osvedčené členskými štátmi a dostupnosť vzájomne uznávaných prostriedkov elektronickej identifikácie) a druhej možnosti (elektronické osvedčenia atribútov právne uznávané cezhranične).

Pokiaľ ide o všeobecný rámec pre dôveryhodné služby, táto úroveň ambícií si vyžaduje súbor opatrení, v rámci ktorých nie je potrebný postupný prístup na splnenie cieľov politiky.

Nová kvalifikovaná dôveryhodná služba na spravovanie zariadení na vyhotovenie elektronického podpisu a elektronickej pečate na diaľku by z hľadiska bezpečnosti, jednotnosti, právnej istoty a výberu pre spotrebiteľov priniesla významné výhody súvisiace s certifikáciou zariadení na vyhotovenie elektronického podpisu, ako aj v súvislosti s požiadavkami, ktoré majú splniť kvalifikovaní poskytovatelia dôveryhodných služieb

spravujúci takéto zariadenia. Novými ustanoveniami by sa posilnil celkový rámec regulácie a dohľadu pre poskytovanie dôveryhodných služieb.

Vplyvy možností politiky na rôzne kategórie zainteresovaných strán sú podrobne vysvetlené v prílohe 3 k posúdeniu vplyvu na podporu tejto iniciatívy. Posúdenie je kvantitatívne aj kvalitatívne. Zo štúdie posúdenia vplyvu vyplýva, že minimálne vyčísliteľné náklady možno odhadnúť na viac ako 3,2 mld. EUR, pretože niektoré nákladové položky nemožno vyčíslieť. Celkové vyčísliteľné výnosy boli odhadnuté na 3,9 – 9,6 mld. EUR. Pokiaľ ide o širšie ekonomické vplyvy, očakáva sa, že uprednostňovaná možnosť bude mať pozitívny vplyv na inovácie, medzinárodný obchod a konkurencieschopnosť, prispeje k ekonomickému rastu a povedie k dodatočným investíciám do riešení v oblasti digitálnej identity. Očakáva sa napríklad, že dodatočné investície vo výške 500 mil. EUR vyvolané legislatívnou zmenou v rámci možnosti 3 vytvoria po desiatich rokoch prínosy vo výške 1 268 mil. EUR (pri miere prijatia na úrovni 67 %).

Okrem toho sa očakáva, že uprednostňovaná možnosť bude mať pozitívny vplyv na zamestnanosť, pričom vytvorí 5 000 až 27 000 ďalších pracovných miest počas piatich rokov po jej realizácii. To možno vysvetliť dodatočnými investíciami a zníženými nákladmi pre podniky, ktoré sa spoliehajú na používanie riešení v oblasti elektronickej identifikácie.

Najväčší pozitívny vplyv na životné prostredie sa očakáva pri tretej možnosti, ktorá by mala v maximálnom rozsahu zlepšiť zavádzanie a použiteľnosť elektronickej identifikácie s pozitívnymi vplyvmi na znižovanie emisií súvisiacich s poskytovaním verejných služieb.

Elektronické registre poskytujú používateľom dôkaz a nemenný audítorský záznam pre stanovenie postupnosti transakcií a dátových záznamov, čím zabezpečujú integritu údajov. Hoci táto dôveryhodná služba nebola súčasťou posúdenia vplyvu, vychádza z existujúcich dôveryhodných služieb, pretože je kombináciou označovania údajov časovými pečiatkami a určovania ich postupnosti s istotou o pôvodcovi údajov, čo je podobné elektronickému podpisaniu. Táto dôveryhodná služba je potrebná na zabránenie fragmentácii vnútorného trhu, pretože vymedzuje jednotný celoeurópsky rámec umožňujúci cezhraničné uznávanie dôveryhodných služieb podporujúcich fungovanie kvalifikovaných elektronických registrov. Integrita údajov je naopak veľmi dôležitá pre združovanie dát z decentralizovaných zdrojov, nezávislé riešenia v oblasti totožnosti, určovanie vlastníctva digitálnych aktív, zaznamenávanie obchodných postupov na účely kontroly dodržiavania súladu s kritériami udržateľnosti a pre rôzne prípady použitia na kapitálových trhoch.

- **Regulačná vhodnosť a zjednodušenie**

V tomto návrhu sa stanovujú opatrenia, ktoré sa budú vzťahovať na subjekty verejného sektora, občanov a poskytovateľov online služieb. Znížia sa ním administratívne náklady a náklady orgánov verejnej správy na dodržiavanie predpisov, prevádzkové náklady a výdavky poskytovateľov online služieb v súvislosti s bezpečnosťou. Zníženie administratívnej záťaže bude prínosom pre občanov, ktorí sa budú plne spoliehať na digitálne prostriedky identifikácie a nástroj bezpečnej výmeny atribútov digitálnej identity s rovnakou právnou silou v zahraničí. Prínosom pre poskytovateľov elektronickej totožnosti budú aj úspory nákladov na dodržiavanie predpisov.

- **Základné práva**

Keďže osobné údaje patria do rozsahu pôsobnosti niektorých prvkov nariadenia, opatrenia sú navrhnuté tak, aby v plnej miere spĺňali právne predpisy na ochranu údajov. Návrhom sa

napríklad zlepšujú možnosti výmeny údajov a zverejňovania informácií podľa vlastného uváženia. Európska peňaženka digitálnej identity umožní používateľovi kontrolovať množstvo údajov poskytovaných spoľiehajúcim sa stranám a byť informovaný o atribútoch potrebných na poskytovanie konkrétnej služby. Poskytovatelia služieb informujú členské štáty o svojom zámere spoliehať sa na európsku peňaženku digitálnej identity, čo by členským štátom umožnilo kontrolovať, že poskytovatelia služieb žiadajú o súbory citlivých údajov týkajúcich sa napríklad zdravia len v súlade s vnútroštátnym právom.

4. VPLYV NA ROZPOČET

Na optimálne dosiahnutie cieľov tejto iniciatívy je potrebné financovať niekoľko opatrení na úrovni Komisie, kde sa predpokladá pridelenie 60 ekvivalentov plného pracovného času v rokoch 2022 až 2027, ako aj na úrovni členských štátov prostredníctvom ich aktívnej účasti na expertných skupinách a vo výboroch súvisiacich s prácou v rámci iniciatívy a zložených zo zástupcov členských štátov. Celkové finančné zdroje potrebné na vykonávanie návrhu v rokoch 2022 až 2027 budú do výšky 30,825 mil. EUR vrátane administratívnych nákladov vo výške 8,825 mil. EUR a prevádzkových výdajov až do výšky 22 mil. EUR pokrytých programom Digitálna Európa (ak sa dosiahne dohoda). Prostredníctvom financovania sa podporia náklady spojené s údržbou, vývojom, hosťateľskými službami, prevádzkovaním a podporou základných prvkov elektronickej identifikácie a dôveryhodných služieb. Môžu sa podporiť aj granty na pripojenie služieb k ekosystému európskej peňaženky digitálnej identity, vývoj noriem a technických špecifikácií. A nakoniec sa financovaním podporí aj vykonávanie ročných prieskumov a štúdií o účinnosti a efektívnosti nariadenia pri dosahovaní jeho cieľov. „Finančný výkaz“ pripojený k tejto iniciatíve obsahuje podrobný prehľad príslušných nákladov.

5. ĎALŠIE PRVKY

- **Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ**

Vplyvy sa budú monitorovať a hodnotiť v súlade s usmerneniami pre lepšiu právnu reguláciu vzťahujúcimi sa na vykonávanie a uplatňovanie navrhovaného nariadenia. Spôsob monitorovania je dôležitou súčasťou návrhu, najmä vzhľadom na nedostatky súčasného rámca podávania správ, ako to vyplýva z hodnotiacej štúdie. Navyše k požiadavkám na podávanie správ, ktoré boli zahrnuté do navrhovaného nariadenia s cieľom zaistiť lepšie údaje a základňu pre analýzu, sa v rámci monitorovania bude monitorovať: 1. rozsah, v akom sa potrebné zmeny vykonali v súlade s prijatými opatreniami; 2. či sa vykonali potrebné zmeny príslušných vnútroštátnych systémov; 3. či sa dodržali potrebné zmeny povinností regulovaných subjektov v oblasti dodržiavania predpisov. Európska komisia (1, 2 a 3) a príslušné vnútroštátne orgány (2 a 3) budú zodpovedné za získavanie údajov na základe vopred vymedzených ukazovateľov.

Pokiaľ ide o uplatňovanie navrhovaného nástroja, Európska komisia a príslušné vnútroštátne orgány prostredníctvom ročných prieskumov posúdia: 1. prístup k prostriedkom elektronickej identifikácie pre všetkých občanov EÚ; 2. väčšie cezhraničné uznávanie a akceptáciu schém elektronickej identifikácie; 3. opatrenia na podporenie prijatia súkromným sektorom a rozvoj nových služieb digitálnej identity.

Kontextové informácie zhromaždí Európska komisia prostredníctvom ročných prieskumov o: 1. veľkosti trhu s digitálnou identitou; 2. výdavkoch na verejné obstarávanie spojené s digitálnou identitou; 3. podiele podnikov poskytujúcich svoje služby online; 4. podiele

online transakcií vyžadujúcich silnú identifikáciu zákazníka; 5. podiele občanov EÚ používajúcich online súkromné a verejné služby.

- **Podrobné vysvetlenie osobitných ustanovení návrhu**

V návrhu nariadenia sa v článku 6a požaduje, aby členské štáty vydali európsku peňaženku digitálnej identity v rámci oznámenej schémy elektronickej identifikácie v súlade so spoločnými technickými normami po vykonaní povinného posúdenia súladu a dobrovoľnej certifikácie v rámci európskeho rámca certifikácie kybernetickej bezpečnosti, ako sa stanovuje v akte o kybernetickej bezpečnosti. Obsahuje ustanovenia, ktorých cieľom je zabezpečiť, aby fyzické a právnické osoby mali možnosť bezpečne si vyžiadať, získať, uchovávať, kombinovať a používať osobné identifikačné údaje a elektronické osvedčenia atribútov na autentifikáciu online aj offline, a umožniť prístup k tovaru a online verejným a súkromným službám pod kontrolou používateľa. Touto certifikáciou nie je dotknuté všeobecné nariadenie o ochrane údajov v tom zmysle, že operácie spracúvania osobných údajov súvisiace s európskou peňaženkou digitálnej identity môžu byť certifikované len v súlade s článkami 42 a 43 všeobecného nariadenia o ochrane údajov.

V návrhu sa v článku 6b stanovujú osobitné ustanovenia o požiadavkách vzťahujúcich sa na spoliehajúce sa strany na zabránenie podvodom a zaistenie autentifikácie osobných údajov o totožnosti a elektronických osvedčení atribútov pochádzajúcich z európskej peňaženky digitálnej identity.

V záujme sprístupnenia väčšieho množstva prostriedkov elektronickej identifikácie na cezhraničné použitie a zvýšenia efektívnosti procesu vzájomného uznávania oznámených schém elektronickej identifikácie sa v článku 7 zavádza povinnosť členských štátov oznámiť aspoň jednu schému elektronickej identifikácie. Okrem toho sa do článku 11a dopĺňajú ustanovenia na uľahčenie jedinečnej identifikácie v snahe zabezpečiť jednoznačnú a trvalú identifikáciu fyzických osôb. Týka sa to prípadov, keď sa identifikácia vyžaduje v právnych predpisoch, napríklad v oblasti zdravia, vo finančnej oblasti na plnenie povinností týkajúcich sa boja proti praniu špinavých peňazí a financovaniu terorizmu alebo na účely súdnych konaní. Na tento účel sa bude od členských štátov vyžadovať, aby do minimálneho súboru osobných identifikačných údajov zahrnuli jedinečný a trvalý identifikátor. Efektívnosť vzájomného uznávania zvyšuje možnosť členských štátov spoliehať sa na certifikáciu v záujme zabezpečenia súladu s nariadením a tým nahradiť proces partnerského preskúmania.

V oddiele 3 sa zavádzajú nové ustanovenia o cezhraničnom spoliehaní sa na európsku peňaženku digitálnej identity na zabezpečenie toho, aby sa používatelia mohli spoliehať na používanie európskej peňaženky digitálnej identity pri prístupe k online službám poskytovaným subjektmi verejného sektora a súkromnými poskytovateľmi služieb vyžadujúcimi používanie silnej autentifikácie používateľa.

V kapitole III o dôveryhodných službách sa mení článok 14 o medzinárodných aspektoch v záujme umožniť Komisii prijímanie vykonávacích rozhodnutí osvedčujúcich rovnocennosť požiadaviek uplatňovaných na poskytovateľov dôveryhodných služieb usadených v tretích krajinách a rovnocennosť služieb, ktoré poskytujú, okrem používania dohôd o vzájomnom uznávaní v súlade s článkom 218 ZFEÚ.

V súvislosti so všeobecným ustanovením uplatniteľným na dôveryhodné služby sa na účely zosúladenia s pravidlami uplatniteľnými na sieťovú a informačnú bezpečnosť v EÚ menia články 17, 18, 20, 21 a 24. Pokiaľ ide o metódy, ktoré majú kvalifikovaní poskytovatelia dôveryhodných služieb používať na overenie totožnosti fyzickej alebo právnickej osoby, ktorej sú kvalifikované certifikáty vydané, s cieľom zabezpečiť uplatňovanie rovnakých

pravidiel v celej EÚ boli harmonizované a objasnené ustanovenia o používaní prostriedkov identifikácie na diaľku.

V kapitole III sa uvádza nový článok 29a na účely vymedzenia požiadaviek na kvalifikovanú službu spravovania zariadení na vyhotovenie elektronického podpisu na diaľku. Táto nová kvalifikovaná dôveryhodná služba by priamo súvisela s opatreniami, ktoré sa uvádzajú a posudzujú v posúdení vplyvu, a vychádzala z týchto opatrení, najmä z opatrení týkajúcich sa „harmonizácie certifikačného procesu pre elektronické podpisovanie na diaľku“ a ďalších opatrení zameraných na to, aby členské štáty harmonizovali postupy v oblasti dohľadu.

Na zabezpečenie toho, aby používatelia mohli identifikovať subjekt, ktorý stojí za webovým sídlom, článok 45 sa mení tak, aby sa od poskytovateľov webových prehliadačov vyžadovalo, aby uľahčili používanie kvalifikovaných certifikátov na autentifikáciu webových sídiel.

Kapitola III obsahuje tri nové oddiely.

Novým oddielom 9 sa vkladajú ustanovenia o právnych účinkoch elektronických osvedčení atribútov, ich používaní v určených sektoroch a požiadavky na kvalifikované osvedčenia atribútov. S cieľom zabezpečiť vysokú mieru dôvery sa do článku 45d vkladá ustanovenie o overovaní atribútov na základe autentických zdrojov. Do článku 45e sa vkladá požiadavka, ktorou sa má zabezpečiť, aby používatelia európskej peňaženky digitálnej identity mohli využívať dostupné elektronické osvedčenia atribútov a boli im takéto osvedčenia vydané k európskej peňaženke digitálnej identity. V článku 45f sa zase uvádzajú ďalšie pravidlá poskytovania služieb elektronického osvedčovania atribútov vrátane pravidiel ochrany osobných údajov.

V novom oddiele 10 sa umožňuje poskytovanie kvalifikovaných služieb elektronickej archivácie na úrovni EÚ. Článok 45g o kvalifikovaných službách elektronickej archivácie dopĺňa články 34 a 40 o kvalifikovaných službách uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí.

V novom oddiele 11 sa stanovuje rámec pre dôveryhodné služby v súvislosti s vytváraním a údržbou elektronických registrov a kvalifikovaných elektronických registrov. Elektronický register je kombináciou označovania údajov časovými pečiatkami a určovania ich postupnosti s istotou o pôvodcovi údajov podobne ako pri elektronickom podpísaní s dodatočnou výhodou, že umožňuje decentralizované riadenie, ktoré je vhodné pri spolupráci viacerých strán. Je to dôležité pre rôzne prípady použitia, ktoré môžu vychádzať z elektronických registrov.

Elektronické registre pomáhajú spoločnostiam šetriť náklady zvýšením efektívnosti a bezpečnosti spolupráce viacerých strán a uľahčujú regulačný dohľad. Pri chýbajúcej európskej regulácii vzniká riziko, že vnútroštátni zákonodarcovia stanovia rozdielne vnútroštátne normy. Aby sa zabránilo fragmentácii vnútorného trhu, je potrebné vymedziť jednotný celoeurópsky rámec, ktorý umožní cezhraničné uznávanie dôveryhodných služieb podporujúcich fungovanie elektronických registrov. Táto celoeurópska norma pre uzlových operátorov sa bude uplatňovať bez ohľadu na iné sekundárne právne predpisy EÚ. Ak sa elektronické registre používajú na podporenie vydávania dlhopisov a/alebo obchodovania s dlhopismi, resp. na účely kryptoaktív, prípady použitia by mali byť zlučiteľné so všetkými uplatniteľnými finančnými pravidlami, napríklad so smernicou o trhoch s finančnými nástrojmi¹¹, smernicou o platobných službách¹² a s budúcim nariadením o trhoch

¹¹ Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ, text s významom pre EHP, (Ú. v. EÚ L 173, 12.6.2014, s. 349 – 496).

s kryptoaktívami¹³. Ak sú prípady použitia spojené s osobnými údajmi, poskytovatelia služieb budú musieť dodržiavať ustanovenia všeobecného nariadenia o ochrane údajov.

V roku 2017 bolo 75 % všetkých prípadov použitia elektronických registrov v sektore bankovníctva a financií. Prípady použitia elektronických registrov sú dnes čoraz rozmanitejšie, pričom 17 % prípadov použitia je v oblasti komunikácie a médií, 15 % v oblasti výroby a prírodných zdrojov, 10 % v štátnom sektore, 8 % v poisťovníctve, 5 % v maloobchode, 6 % v doprave a 5 % v oblasti verejnoprospešných služieb¹⁴.

A nakoniec v kapitole VI sa uvádza nový článok 48b v snahe zabezpečiť, aby sa na účely monitorovania účinnosti zmeneného nariadenia získavala štatistika používania európskej peňaženky digitálnej identity.

¹² Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES, (Ú. v. EÚ L 337, 23.12.2015, s. 35 – 127).

¹³ Návrh nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937, COM(2020) 593 final.

¹⁴ Gartner, *Blockchain Evolution* (Vývoj blockchainu), 2020.

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o stanovenie rámca pre európsku digitálnu identitu

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru¹⁵,

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

- (1) V oznámení Komisie z 19. februára 2020 s názvom Formovanie digitálnej budúcnosti Európy¹⁶ sa ohlasuje revízia nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 s cieľom zlepšiť jeho účinnosť, rozšíriť jeho prínosy na súkromný sektor a podporiť dôveryhodné digitálne identity pre všetkých Európanov.
- (2) Európska rada vo svojich záveroch z 1. – 2. októbra 2020¹⁷ vyzvala Komisiu, aby navrhla vytvorenie úijného rámca na bezpečnú verejnú elektronickú identifikáciu vrátane interoperabilných digitálnych podpisov s cieľom poskytnúť ľuďom kontrolu nad ich online totožnosťou a údajmi, ako aj umožniť prístup k verejným, súkromným a cezhraničným digitálnym službám.
- (3) V oznámení Komisie s názvom Digitálny kompas do roku 2030: digitálne desaťročie na európsky spôsob¹⁸ z 9. marca 2021 sa stanovuje cieľ v podobe úijného rámca, ktorý do roku 2030 povedie k plošnému zavádzaniu dôveryhodnej identity kontrolovanej používateľom, vďaka ktorej bude mať každý používateľ kontrolu nad svojimi online interakciami a pohybmi v online priestore.
- (4) Harmonizovanejší prístup k digitálnej identifikácii by mal znížiť riziká a náklady súčasnej fragmentácie spôsobenej využívaním rozdielnych vnútroštátnych riešení a posilni jednotný trh tým, že umožní občanom, ďalším obyvateľom vymedzeným podľa vnútroštátnych právnych predpisov a podnikom, aby sa pohodlne a jednotným spôsobom identifikovali online v celej Únii. Každý by mal mať bezpečný prístup k verejným a súkromným službám využívajúcim zlepšený ekosystém dôveryhodných služieb a overené dôkazy totožnosti a osvedčenia atribútov, ako je napríklad univerzitný diplom právne uznaný a akceptovaný kdekoľvek v Únii. Cieľom rámca

¹⁵ Ú. v. EÚ C ..., ..., s.

¹⁶ COM/2020/67 final.

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

¹⁸ COM/2021/118 final/2.

pre európsku digitálnu identitu je dosiahnuť posun od spoliehania sa len na vnútroštátne riešenia digitálnej identity k poskytovaniu elektronických osvedčení atribútov platných na európskej úrovni. Poskytovatelia elektronických osvedčení atribútov by mali využívať výhody, ktoré prináša jasný a jednotný súbor pravidiel, a orgány verejnej správy by mali mať možnosť využívať elektronické dokumenty v danom formáte.

- (5) Na podporu konkurencieschopnosti európskych podnikov by poskytovatelia online služieb mali mať možnosť využívať riešenia digitálnej identity uznávané v celej Únii bez ohľadu na členský štát, v ktorom boli vydané, a mať tak prospech z harmonizovaného európskeho prístupu k dôvere, bezpečnosti a interoperabilite. Používatelia aj poskytovatelia služieb by mali byť schopní využívať výhody, ktoré prináša rovnaká právna sila elektronického osvedčovania atribútov v celej Únii.
- (6) Na spracúvanie osobných údajov pri vykonávaní tohto nariadenia sa vzťahuje nariadenie (EÚ) 2016/679¹⁹. V tomto nariadení by sa preto mali stanoviť osobitné záruky, aby sa poskytovateľom prostriedkov elektronickej identifikácie a elektronického osvedčovania atribútov zabránilo spájať osobné údaje z iných služieb s osobnými údajmi týkajúcimi sa služieb, ktoré patria do rozsahu pôsobnosti tohto nariadenia.
- (7) Je potrebné stanoviť harmonizované podmienky na vytvorenie rámca pre európske peňaženky digitálnej identity, ktoré by mali vydávať členské štáty a ktoré by mali všetkým občanom Únie a ďalším obyvateľom Únie vymedzeným podľa vnútroštátnych právnych predpisov umožňovať bezpečnú výmenu údajov týkajúcich sa ich totožnosti používateľsky ústretovým a pohodlným spôsobom pod výlučnou kontrolou používateľa. Technológie, ktoré sa použijú na dosiahnutie týchto cieľov, by sa mali vyvinúť tak, aby sa dosiahla najvyššia úroveň bezpečnosti, jednoduchosti používania a širokej použiteľnosti. Členské štáty by mali zabezpečiť rovnaký prístup k digitálnej identifikácii pre všetkých svojich štátnych príslušníkov a obyvateľov.
- (8) S cieľom zabezpečiť dodržiavanie práva Únie alebo vnútroštátneho práva, ktoré je v súlade s právom Únie, by poskytovatelia služieb mali členským štátom oznámiť svoj zámer využívať európske peňaženky digitálnej identity. To členským štátom umožní chrániť používateľov pred podvodmi a zabrániť nezákonnému používaniu údajov o totožnosti a elektronických osvedčení atribútov, ako aj zabezpečiť, aby spracúvanie citlivých údajov, ako sú údaje o zdravotnom stave, mohli overovať spoľiehajúce sa strany v súlade s právom Únie alebo vnútroštátnym právom.
- (9) Všetky európske peňaženky digitálnej identity by mali používateľom umožniť cezhraničnú elektronickú identifikáciu a autentifikáciu online aj offline na získanie prístupu k širokej škále verejných a súkromných služieb. Bez toho, aby boli dotknuté výhradné práva členských štátov, pokiaľ ide o identifikáciu ich štátnych príslušníkov a obyvateľov, peňaženky môžu slúžiť aj inštitucionálnym potrebám orgánov verejnej správy, medzinárodných organizácií a inštitúcií, orgánov, úradov a agentúr Únie. Používanie offline by bolo dôležité v mnohých odvetviach, a to aj v sektore zdravotníctva, kde sa služby často poskytujú prostredníctvom osobnej interakcie, a v prípade ereceptov by mala existovať možnosť využívať kódy QR alebo podobné technológie na overenie pravosti. S cieľom splniť bezpečnostné požiadavky podľa

¹⁹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

tohto nariadenia by európske peňaženky digitálnej identity, opierajúc sa o „vysokú“ úroveň zabezpečenia, mali využívať potenciál, ktorý ponúkajú riešenia odolné proti neoprávnenej manipulácii, ako sú napríklad bezpečné prvky. Európske peňaženky digitálnej identity by mali používateľom takisto umožniť vytvárať a používať kvalifikované elektronické podpisy a pečate akceptované v celej EÚ. Aby osoby a podniky v celej EÚ dosiahli výhody vyplývajúce zo zjednodušenia a zníženia nákladov, a to aj umožnením právomocí zastupovať a prostredníctvom elektronických mandátov, členské štáty by mali vydávať európske peňaženky digitálnej identity založené na spoločných normách s cieľom zabezpečiť plynulú interoperabilitu a vysokú úroveň bezpečnosti. Len príslušné orgány členských štátov môžu poskytnúť vysoký stupeň dôvery pri zisťovaní totožnosti osoby a poskytnúť tak záruku, že osoba, ktorá tvrdí, že má určitú totožnosť alebo si na určitú totožnosť uplatňuje nárok, je v skutočnosti osobou, ktorou tvrdí, že je. Je preto nevyhnutné, aby sa európske peňaženky digitálnej identity opierali o právnu identitu občanov, ďalších obyvateľov alebo právnických osôb. Dôvera v európske peňaženky digitálnej identity by sa posilnila tým, že vydávajúce strany by boli v súlade s nariadením (EÚ) 2016/679 povinné zaviesť primerané technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti zodpovedajúcej rizikám, ktoré vznikajú v súvislosti s právami a slobodami fyzických osôb.

- (10) S cieľom dosiahnuť vysokú úroveň bezpečnosti a dôveryhodnosti sa v tomto nariadení stanovujú požiadavky na európske peňaženky digitálnej identity. Súlad európskych peňaženiek digitálnej identity s týmito požiadavkami by mali certifikovať akreditované orgány verejného alebo súkromného sektora určené členskými štátmi. Využívaním systému certifikácie založeného na dostupnosti noriem spoločne dohodnutých s členskými štátmi by sa mala zabezpečiť vysoká úroveň dôvery a interoperability. Certifikácia by sa mala opierať najmä o príslušné európske systémy certifikácie kybernetickej bezpečnosti zriadené podľa nariadenia (EÚ) 2019/881²⁰. Certifikácia týkajúca sa spracovania osobných údajov podľa nariadenia (ES) 2016/679, by takouto certifikáciou nemala byť dotknutá.
- (11) Európske peňaženky digitálnej identity by mali zabezpečiť najvyššiu úroveň bezpečnosti osobných údajov používaných na autentifikáciu bez ohľadu na to, či sa takéto údaje uchovávajú lokálne alebo na cloude, pričom sa zohľadnia rôzne úrovne rizika. Používanie biometrických údajov na autentifikáciu je jednou z metód identifikácie, ktorá poskytuje vysokú úroveň spoľahlivosti, najmä ak sa používa v kombinácii s inými zložkami autentifikácie. Keďže biometrické údaje predstavujú jedinečnú charakteristiku osoby, používanie biometrických údajov si vyžaduje organizačné a bezpečnostné opatrenia, ktoré sú primerané riziku, ktoré takéto spracúvanie môže znamenať pre práva a slobody fyzických osôb, a ktoré musia byť v súlade s nariadením 2016/679.
- (12) S cieľom zabezpečiť, aby bol rámec európskej digitálnej identity otvorený inováciám, technologickému vývoju a aby bol nadčasový, členské štáty by sa mali nabádať k tomu, aby spoločne vytvárali sandboxy na testovanie inovačných riešení v kontrolovanom a bezpečnom prostredí, a to najmä so zámerom zlepšiť funkčnosť, ochranu osobných údajov, bezpečnosť a interoperabilitu riešení a získať vstupy pre

²⁰ Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

budúce aktualizácie technických referencií a právnych požiadaviek. Toto prostredie by malo podporovať začlenenie európskych malých a stredných podnikov, startupov a individuálnych inovátorov a výskumných pracovníkov.

- (13) Nariadením (EÚ) 2019/1157²¹ sa posilňuje zabezpečenie preukazov totožnosti zlepšenými bezpečnostnými prvkami do augusta 2021. Členské štáty by mali zvážiť uskutočniteľnosť oznamovania preukazov totožnosti v rámci schém elektronickej identifikácie s cieľom rozšíriť cezhraničnú dostupnosť prostriedkov elektronickej identifikácie.
- (14) Proces oznamovania schém elektronickej identifikácie by sa mal zjednodušiť a urýchliť s cieľom podporiť prístup k pohodlným, dôveryhodným, bezpečným a inovačným riešeniam autentifikácie a identifikácie a v prípade potreby nabádať súkromných poskytovateľov totožnosti, aby orgánom členských štátov ponúkali schémy elektronickej identifikácie na oznámenie ako vnútroštátne schémy elektronických preukazov totožnosti podľa nariadenia č. 910/2014.
- (15) Zjednodušením súčasných postupov oznamovania a partnerského preskúmania sa zabráni rôznorodým prístupom k posudzovaniu rôznych oznámených schém elektronickej identifikácie a uľahčí sa budovanie dôvery medzi členskými štátmi. Nové zjednodušené mechanizmy by mali podporovať spoluprácu členských štátov v oblasti bezpečnosti a interoperability ich oznámených schém elektronickej identifikácie.
- (16) Na zabezpečenie súladu s požiadavkami tohto nariadenia a príslušných vykonávacích aktov by členské štáty by mali využívať nové, flexibilné nástroje. Toto nariadenie by malo členským štátom umožniť využívať správy a posúdenia vykonané akreditovanými orgánmi posudzovania zhody alebo dobrovoľné systémy certifikácie bezpečnosti IKT, ako sú systémy certifikácie, ktoré sa majú zriadiť na úrovni Únie podľa nariadenia (EÚ) 2019/881, aby podporili svoje tvrdenia o zosúladiení systémov alebo ich častí s požiadavkami nariadenia na interoperabilitu a bezpečnosť oznámených schém elektronickej identifikácie.
- (17) Na priradenie používateľov z iného členského štátu k príslušnej právnej identite používajú poskytovatelia služieb údaje o totožnosti poskytnuté súborom osobných identifikačných údajov dostupných zo schém elektronickej identifikácie podľa nariadenia (EÚ) č. 910/2014. Napriek použitiu súboru údajov eIDAS si však zabezpečenie presného priradenia v mnohých prípadoch vyžaduje dodatočné informácie o používateľovi a osobitné jedinečné postupy identifikácie na vnútroštátnej úrovni. S cieľom ďalej podporovať použiteľnosť prostriedkov elektronickej identifikácie by sa v tomto nariadení malo od členských štátov vyžadovať prijatie osobitných opatrení, aby sa v procese elektronickej identifikácie zabezpečilo správne priradenie totožnosti. Na ten istý účel by sa týmto nariadením mal rozšíriť aj povinný minimálny súbor údajov a malo by sa vyžadovať používanie jedinečného a trvalého elektronického identifikátora v súlade s právom Únie v prípadoch, keď je potrebné jednoznačným a trvalým spôsobom právne identifikovať používateľa na jeho žiadosť.

²¹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1157 z 20. júna 2019 o posilnení zabezpečenia preukazov totožnosti občanov Únie a dokladov o pobyte vydávaných občanom Únie a ich rodinným príslušníkom vykonávajúcim svoje právo na voľný pohyb (Ú. v. EÚ L 188, 12.7.2019, s. 67).

- (18) V súlade so smernicou (EÚ) 2019/882²² by osoby so zdravotným postihnutím mali mať možnosť používať európske peňaženky digitálnej identity, dôveryhodné služby a produkty pre koncových používateľov používané pri poskytovaní týchto služieb na rovnakom základe ako ostatní používatelia.
- (19) Toto nariadenie by sa nemalo vzťahovať na aspekty súvisiace s uzatváraním a platnosťou zmlúv alebo iných právnych záväzkov, pri ktorých sú požiadavky na formu stanovené vo vnútroštátnom práve alebo práve Únie. Nemalo by mať ani vplyv na vnútroštátne požiadavky na formu v súvislosti s verejnými registrami, a to konkrétne s obchodným registrom a katastrom nehnuteľností.
- (20) Poskytovanie a využívanie dôveryhodných služieb nadobúda čoraz väčší význam v prípade medzinárodného obchodu a spolupráce. Medzinárodní partneri EÚ vytvárajú rámce dôvery inšpirované nariadením (EÚ) č. 910/2014. S cieľom uľahčiť uznávanie takýchto služieb a ich poskytovateľov sa preto vo vykonávacích právnych predpisoch ako doplnok k možnosti vzájomného uznávania dôveryhodných služieb a ich poskytovateľov usadených v Únii a v tretích krajinách v súlade s článkom 218 zmluvy môžu stanoviť podmienky, za ktorých by sa rámce dôvery tretích krajín mohli považovať za rovnocenné rámci dôvery pre kvalifikované dôveryhodné služby a ich poskytovateľov v tomto nariadení.
- (21) Toto nariadenie by malo vychádzať z aktov Únie, ktorými sa zabezpečujú konkurencieschopné a spravodlivé trhy v digitálnom sektore. Vychádza najmä z nariadenia XXX/XXXX [akt o digitálnych trhoch], ktorým sa zavádzajú pravidlá pre poskytovateľov základných služieb platformy určených ako strážcovia prístupu a okrem iného im zakazuje vyžadovať od komerčných používateľov, aby v kontexte služieb, ktoré ponúkajú komerční používatelia využívajúci základné služby platformy daného strážcu prístupu, používali či ponúkali identifikačnú službu strážcu prístupu alebo s ňou zabezpečili interoperabilitu. V článku 6 ods. 1 písm. f) nariadenia XXX/XXXX [akt o digitálnych trhoch] sa vyžaduje, aby strážcovia prístupu umožnili komerčným používateľom a poskytovateľom doplnkových služieb prístup k tým istým prvkom operačného systému, hardvéru alebo softvéru, ktoré sú dostupné alebo používané pri poskytovaní akýchkoľvek doplnkových služieb zo strany strážcu prístupu, a interoperabilitu s nimi. Podľa článku 2 ods. 15 [aktu o digitálnych trhoch] identifikačné služby predstavujú druh doplnkových služieb. Komerční používatelia a poskytovatelia doplnkových služieb by preto mali mať možnosť získať prístup k takým hardvérovým alebo softvérovým prvkom, ako sú bezpečnostné prvky v smartfónoch, a prostredníctvom európskych peňaženiek digitálnej identity alebo oznámených prostriedkov elektronickej identifikácie členských štátov zabezpečiť s nimi interoperabilitu.
- (22) S cieľom zefektívniť povinnosti v oblasti kybernetickej bezpečnosti uložené poskytovateľom dôveryhodných služieb, ako aj umožniť týmto poskytovateľom a ich príslušným orgánom využívať právny rámec stanovený smernicou XXXX/XXXX (smernica NIS2) sa od dôveryhodných služieb vyžaduje, aby prijali primerané technické a organizačné opatrenia podľa smernice XXXX/XXXX (smernica NIS2), ako sú opatrenia na riešenie systémových zlyhaní, ľudskej chyby, zlomyseľného konania alebo prírodných javov, s cieľom riadiť riziká, ktoré predstavujú pre bezpečnosť sietí a informačných systémov, ktoré tieto poskytovatelia používajú pri

²² Smernica Európskeho parlamentu a Rady (EÚ) 2019/882 zo 17. apríla 2019 o požiadavkách na prístupnosť výrobkov a služieb (Ú. v. EÚ L 151, 7.6.2019, s. 70).

poskytovaní svojich služieb, ako aj oznamovali závažné incidenty a kybernetické hrozby v súlade so smernicou XXXX/XXXX (smernica NIS2). Pokiaľ ide o oznamovanie incidentov, poskytovatelia dôveryhodných služieb by mali oznamovať všetky incidenty, ktoré majú závažný vplyv na poskytovanie ich služieb, vrátane incidentov spôsobených krádežou alebo stratou zariadení, škody spôsobené na sieťových kábloch alebo incidenty, ku ktorým došlo v súvislosti s identifikáciou osôb. Požiadavky na riadenie kybernetických rizík a oznamovacie povinnosti podľa smernice XXXXXX [NIS2] by sa mali považovať za doplnkové k požiadavkám uloženým poskytovateľom dôveryhodných služieb podľa tohto nariadenia. Príslušné orgány určené podľa smernice XXXX/XXXX (smernica NIS2) by v prípade potreby mali naďalej uplatňovať zavedené vnútroštátne postupy alebo usmernenia týkajúce sa vykonávania požiadaviek na bezpečnosť a oznamovanie a dohľad nad dodržiavaním takýchto požiadaviek podľa nariadenia (EÚ) č. 910/2014. Žiadne požiadavky podľa tohto nariadenia nemajú vplyv na povinnosť oznamovať porušenia ochrany osobných údajov podľa nariadenia (EÚ) 2016/679.

- (23) Náležitá pozornosť by sa mala venovať zabezpečeniu účinnej spolupráce medzi orgánmi NIS a eIDAS. V prípadoch, keď je orgán dohľadu podľa tohto nariadenia iný ako príslušné orgány určené podľa smernice XXXX/XXXX [NIS2], tieto orgány by mali úzko a včas spolupracovať formou výmeny príslušných informácií s cieľom zabezpečiť účinný dohľad a súlad poskytovateľov dôveryhodných služieb s požiadavkami stanovenými v tomto nariadení a smernici XXXX/XXXX [NIS2]. Orgány dohľadu podľa tohto nariadenia by mali byť oprávnené požiadať príslušný orgán podľa smernice XXXXX/XXXX [NIS2], aby im poskytol relevantné informácie potrebné na udelenie kvalifikovaného štatútu a na vykonanie opatrení v oblasti dohľadu s cieľom overiť, či poskytovatelia dôveryhodných služieb dodržiavajú príslušné požiadavky podľa NIS 2, alebo od nich vyžadovať, aby nesúlad napravili.
- (24) Je dôležité, aby sa ustanovil právny rámec na uľahčenie cezhraničného uznávania medzi existujúcimi vnútroštátnymi právnymi systémami týkajúcimi sa elektronických doručovacích služieb pre registrované zásielky. Tento rámec by tiež mohol otvoriť nové trhové príležitosti pre poskytovateľov dôveryhodných služieb z Únie, aby mohli ponúkať nové celoeurópske elektronické doručovacie služby pre registrované zásielky, a zaistiť, aby bola identifikácia príjemcov zabezpečená s vyššou úrovňou spoľahlivosti ako identifikácia odosielateľa.
- (25) Vo väčšine prípadov si občania a ďalší obyvatelia nemôžu cezhranične a digitálne vymieňať informácie týkajúce sa ich totožnosti, ako sú adresy, vek a odborná kvalifikácia, vodičské preukazy a iné povolenia a platobné údaje, bezpečným spôsobom a s vysokou úrovňou ochrany údajov.
- (26) Malo by byť možné vydávať a spracúvať dôveryhodné digitálne atribúty a prispievať k znižovaniu administratívnej záťaže tým, že sa občanom a ďalším obyvateľom umožní využívať ich v súkromných a verejných transakciách. Občania a ďalší obyvatelia by mali mať napríklad možnosť preukázať vlastníctvo platného vodičského preukazu vydaného orgánom v jednom členskom štáte, ktorý príslušné orgány v iných členských štátoch môžu overiť a spoľahnúť sa na ňu, ďalej možnosť využívať svoje potvrdenia týkajúce sa sociálneho zabezpečenia alebo budúce digitálne cestovné doklady v cezhraničnom kontexte.
- (27) Každý subjekt, ktorý zhromažďuje, vytvára a vydáva osvedčené atribúty, ako sú diplomy, preukazy, rodné listy, by mal mať možnosť stať sa poskytovateľom elektronického osvedčovania atribútov. Spoliehajúce sa strany by mali používať

elektronické osvedčenia atribútov ako ekvivalent k osvedčeniam v papierovej podobe. Preto by sa elektronickému osvedčeniu atribútov nemal odopierať právny účinok z dôvodu, že je v elektronickej forme alebo že nespĺňa požiadavky na kvalifikované elektronické osvedčenie atribútov. Na tento účel by sa mali stanoviť všeobecné požiadavky na zabezpečenie toho, aby kvalifikované elektronické osvedčenie atribútov malo rovnocenný právny účinok ako osvedčenia v papierovej podobe vydané v súlade so zákonom. Tieto požiadavky by sa však mali uplatňovať bez toho, aby boli dotknuté právne predpisy Únie alebo vnútroštátne právne predpisy, v ktorých sa vymedzujú dodatočné sektorové požiadavky, pokiaľ ide o formu so základnými právnymi účinkami, a v príslušných prípadoch najmä cezhraničné uznávanie kvalifikovaného elektronického osvedčenia atribútov.

- (28) Široká dostupnosť a použiteľnosť európskych peňaženiek digitálnej identity si vyžaduje, aby boli akceptované zo strany súkromných poskytovateľov služieb. Súkromné spoločnosti sa strany, ktoré poskytujú služby v oblasti dopravy, energetiky, bankovníctva a finančných služieb, sociálneho zabezpečenia, zdravia, pitnej vody, poštových služieb, digitálnej infraštruktúry, vzdelávania alebo telekomunikácií, by mali akceptovať používanie európskej peňaženky digitálnej identity na poskytovanie služieb, ak sa podľa vnútroštátneho práva alebo práva Únie alebo na základe zmluvnej povinnosti vyžaduje na online identifikáciu silná autentifikácia používateľa. V prípade, že veľmi veľké online platformy vymedzené v článku 25 ods. 1 nariadenia [referenčné nariadenie DSA] vyžadujú, aby sa používatelia pri prístupe k online službám autentifikovali, tieto platformy by mali byť na základe dobrovoľnej žiadosti používateľa povinné akceptovať používanie európskych peňaženiek digitálnej identity. Používatelia by nemali mať povinnosť používať peňaženku na prístup k súkromným službám, ale ak si to želajú, veľmi veľké online platformy by na tento účel mali akceptovať európsku peňaženku digitálnej identity, pričom by mali dodržiavať zásadu minimalizácie údajov. Vzhľadom na význam veľmi veľkých online platforiem z dôvodu ich dosahu, najmä pokiaľ ide o počet príjemcov služieb a hospodárskych transakcií, je to potrebné na zvýšenie ochrany používateľov pred podvodmi a zabezpečenie vysokej úrovne ochrany údajov. Mali by sa vypracovať samoregulačné kódexy správania na úrovni Únie (ďalej len „kódexy správania“) s cieľom prispieť k širokej dostupnosti a použiteľnosti prostriedkov elektronickej identifikácie vrátane európskych peňaženiek digitálnej identity v rozsahu pôsobnosti tohto nariadenia. Kódexy správania by mali uľahčiť širokú akceptáciu prostriedkov elektronickej identifikácie vrátane európskych peňaženiek digitálnej identity zo strany tých poskytovateľov služieb, ktorí sa nepovažujú za veľmi veľké platformy a ktorí pri autentifikácii používateľov využívajú služby elektronickej identifikácie tretích strán. Mali by sa vypracovať do 12 mesiacov od prijatia tohto nariadenia. Komisia by mala posúdiť účinnosť týchto ustanovení, pokiaľ ide o dostupnosť a použiteľnosť európskych peňaženiek digitálnej identity pre používateľa, po 18 mesiacoch od ich zavedenia, a zrevidovať ustanovenia s cieľom zabezpečiť ich akceptáciu prostredníctvom delegovaných aktov na základe tohto posúdenia.
- (29) Európska peňaženka digitálnej identity by mala technicky umožniť selektívne zverejňovanie atribútov spoliehajúcim sa stranám. Táto funkcia by sa mala stať základným prvkom štruktúry peňaženky, čím by sa posilnilo pohodlie a ochrana osobných údajov vrátane minimalizácie spracúvania osobných údajov.
- (30) Atribúty poskytnuté kvalifikovanými poskytovateľmi dôveryhodných služieb ako súčasť kvalifikovaného osvedčenia atribútov by mali byť overené na základe

autentických zdrojov buď priamo kvalifikovaným poskytovateľom dôveryhodných služieb, alebo prostredníctvom určených sprostredkovateľov uznaných na vnútroštátnej úrovni v súlade s vnútroštátnym právom alebo právom Únie na účely bezpečnej výmeny osvedčených atribútov medzi poskytovateľmi totožnosti alebo služieb osvedčovania atribútov a spoliehajúcimi sa stranami.

- (31) Bezpečná elektronická identifikácia a poskytovanie osvedčení atribútov by mali ponúknuť dodatočnú flexibilitu a riešenia sektoru finančných služieb, aby sa umožnila identifikácia klientov a výmena osobitných atribútov potrebných napríklad na splnenie požiadaviek náležitej starostlivosti vo vzťahu ku klientovi podľa nariadenia o boji proti praniu špinavých peňazí [odkaz sa doplní po prijatí návrhu], požiadaviek na vhodnosť vyplývajúcich z právnych predpisov o ochrane investorov, alebo aby podporilo plnenie prísnych požiadaviek na autentifikáciu zákazníka v prípade prihlásenia sa do účtu a iniciovania transakcií v oblasti platobných služieb.
- (32) Služby autentifikácie webových sídiel poskytujú používateľom istotu, že za daným webovým sídlom stojí skutočný a legitímny subjekt. Uvedené služby prispievajú k budovaniu dôvery a istoty v súvislosti s podnikaním online, keďže používatelia budú dôverovať autentifikovanému webovému sídlu. Používanie služieb autentifikácie webových sídiel je na webových sídlach dobrovoľné. Aby sa však autentifikácia webových sídiel stala prostriedkom na zvyšovanie dôvery, poskytovanie lepšej skúsenosti pre používateľa a podporu rastu na vnútornom trhu, týmto nariadením sa stanovujú minimálne povinnosti týkajúce sa bezpečnosti a zodpovednosti poskytovateľov autentifikácie webových sídiel a ich služieb. Na tento účel by webové prehliadače mali zabezpečiť podporu kvalifikovaných certifikátov autentifikácie webových sídiel podľa nariadenia (EÚ) č. 910/2014 a interoperabilitu s nimi. Mali by uznávať a zobrazovať kvalifikované certifikáty autentifikácie webových sídiel s cieľom poskytovať vysokú úroveň zabezpečenia a umožniť vlastníkom webových sídiel uvádzať svoju totožnosť ako vlastníkov webových sídiel a používateľom identifikovať vlastníkov webových sídiel s vysokým stupňom istoty. S cieľom ďalej podporovať používanie kvalifikovaných certifikátov autentifikácie webových sídiel by verejné orgány v členských štátoch mali zvážiť ich začlenenie do svojich webových sídiel.
- (33) Mnohé členské štáty zaviedli vnútroštátne požiadavky na služby poskytujúce bezpečnú a dôveryhodnú digitálnu archiváciu s cieľom umožniť dlhodobé uchovávanie elektronických dokumentov a súvisiace dôveryhodné služby. Na zabezpečenie právnej istoty a dôvery je nevyhnutné poskytnúť právny rámec na uľahčenie cezhraničného uznávania kvalifikovaných elektronických archivačných služieb. Tento rámec by pre poskytovateľov dôveryhodných služieb z Únie mohol tiež otvoriť nové trhové príležitosti.
- (34) Kvalifikované elektronické registre zaznamenávajú údaje spôsobom, ktorý zabezpečuje jedinečnosť, pravosť a správne poradie vkladania údajov a je odolný voči neoprávnenému zasahovaniu. Elektronický register, podobne ako elektronické podpisovanie, kombinuje účinok časovej pečiatky údajov s istotou, pokiaľ ide o pôvodcu údajov, a má dodatočný prínos v tom, že umožňuje decentralizovanejšie modely riadenia, ktoré sú vhodné na spoluprácu viacerých strán. Napríklad vytvára spoľahlivý auditorský záznam o pôvode komodít v cezhraničnom obchode, podporuje ochranu práv duševného vlastníctva, umožňuje flexibilné trhy s elektrickou energiou, poskytuje základ pre pokročilé riešenia v oblasti nezávislej totožnosti a podporuje efektívnejšie a transformatívne verejné služby. Aby sa zabránilo fragmentácii vnútorného trhu, je dôležité vymedziť celoeurópsky právny rámec, ktorý umožní

cezhraničné uznávanie dôveryhodných služieb na zaznamenávanie údajov v elektronických registroch.

- (35) Certifikácia kvalifikovaných poskytovateľov dôveryhodných služieb by mala poskytnúť právnu istotu pre prípady použitia, ktoré vychádzajú z elektronických registrov. Táto dôveryhodná služba pre elektronické registre a kvalifikované elektronické registre a certifikácia elektronických registrov ako kvalifikovaného poskytovateľa dôveryhodných služieb by mali byť dostupné bez ohľadu na potrebu prípadov použitia, v ktorých sa vyžaduje dodržanie práva Únie alebo vnútroštátneho práva v súlade s právom Únie. Prípady použitia, ktoré zahŕňajú spracúvanie osobných údajov, musia byť v súlade s nariadením (EÚ) 2016/679. Prípady používania kryptoaktív by mali byť zlučiteľné so všetkými platnými finančnými pravidlami, napríklad so smernicou o trhoch s finančnými nástrojmi²³, smernicou o platobných službách²⁴ a budúcim nariadením o trhoch s kryptoaktívami²⁵.
- (36) Aby sme sa vyhli fragmentácii a prekážkam spôsobeným rôznymi normami a technickými obmedzeniami a zabezpečili koordinovaný proces, ktorý by zabránil ohrozeniu vykonávania budúceho európskeho rámca digitálnej identity, je potrebný proces úzkej a štruktúrovanej spolupráce medzi Komisiou, členskými štátmi a súkromným sektorom. Na dosiahnutie tohto cieľa by členské štáty mali spolupracovať v rámci stanovenom v odporúčaní Komisie XXX/XXXX [Súbor nástrojov pre koordinovaný prístup k európskemu rámcu digitálnej identity]²⁶ s cieľom určiť súbor nástrojov pre európsky rámec digitálnej identity. Súbor nástrojov by mal zahŕňať komplexnú technickú architektúru a referenčný rámec, súbor spoločných noriem a technických referencií a súbor usmernení a opisov najlepších postupov vzťahujúcich sa minimálne na všetky aspekty funkcií a interoperability európskych peňaženiek digitálnej identity vrátane elektronických podpisov a kvalifikovanej dôveryhodnej služby na osvedčovanie atribútov, ako sa stanovuje v tomto nariadení. V tejto súvislosti by členské štáty mali dosiahnuť aj dohodu o spoločných prvkoch obchodného modelu a štruktúre poplatkov v rámci európskych peňaženiek digitálnej identity s cieľom uľahčiť ich využívanie v cezhraničnom kontexte, najmä zo strany malých a stredných podnikov. Obsah súboru nástrojov by sa mal vyvíjať paralelne s výsledkami diskusií a procesu prijímania európskeho rámca digitálnej identity a tieto výsledky by sa v ňom mali zohľadniť.
- (37) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1525²⁷ prebehla konzultácia s európskym dozorným úradníkom pre ochranu údajov.
- (38) Nariadenie (EÚ) 910/2014 by sa preto malo zodpovedajúcim spôsobom zmeniť,

²³ Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ, text s významom pre EHP (Ú. v. EÚ L 173, 12.6.2014, s. 349 – 496).

²⁴ Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (Ú. v. EÚ L 337, 23.12.2015, s. 35 – 127).

²⁵ Návrh nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937, COM(2020) 593 final.

²⁶ [Po prijatí vložte odkaz].

²⁷ Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

PRIJALI TOTO NARIADENIE:

Článok 1

Nariadenie (EÚ) 910/2014 sa mení takto:

1. Článok 1 sa nahrádza takto:

„Cieľom tohto nariadenia je zabezpečiť riadne fungovanie vnútorného trhu a poskytnúť primeranú úroveň bezpečnosti prostriedkov elektronickej identifikácie a dôveryhodných služieb. Na tieto účely sa týmto nariadením:

- a) stanovujú podmienky, za ktorých členské štáty poskytujú a uznávajú prostriedky elektronickej identifikácie fyzických a právnických osôb, ktoré patria do oznámenej schémy elektronickej identifikácie iného členského štátu;
- b) stanovujú pravidlá pre dôveryhodné služby, najmä elektronické transakcie;
- c) stanovuje právny rámec pre elektronické podpisy, elektronické pečate, elektronické časové pečiatky, elektronické dokumenty, elektronické doručovacie služby pre registrované zásielky, certifikačné služby na autentifikáciu webových sídiel, elektronické archivovanie a elektronické osvedčovanie atribútov, správu zariadení na vyhotovenie elektronického podpisu na diaľku a vyhotovenie elektronickej pečate na diaľku, a elektronické registre;
- d) stanovujú podmienky, za ktorých členské štáty vydávajú európske peňaženky digitálnej identity.“

2. Článok 2 sa mení takto:

a) Odsek 1 sa nahrádza takto:

„1. Toto nariadenie sa vzťahuje na schémy elektronickej identifikácie, ktoré boli oznámené členskými štátmi, európske peňaženky digitálnej identity vydané členskými štátmi a na poskytovateľov dôveryhodných služieb, ktorí sú usadení v Únii.“;

b) Odsek 3 sa nahrádza takto:

„3. Toto nariadenie nemá vplyv na vnútroštátne právo ani právo Únie súvisiace s uzatváraním a platnosťou zmlúv alebo iných právnych či procesných záväzkov týkajúcich sa sektorovo špecifických požiadaviek, pokiaľ ide o formu so základnými právnymi účinkami.“

3. Článok 3 sa mení takto:

a) Bod 2 sa nahrádza takto:

„2. „prostriedok elektronickej identifikácie“ je hmotná a/alebo nehmotná jednotka vrátane európskych peňažien digitálnej identity alebo preukazov totožnosti podľa nariadenia 2019/1157, ktorá obsahuje osobné identifikačné údaje a ktorá sa používa na autentifikáciu v rámci online alebo offline služby;“;

b) Bod 4 sa nahrádza takto:

„4. „schéma elektronickej identifikácie“ je systém na elektronickú identifikáciu, v rámci ktorého sa fyzickým osobám alebo právnickým

osobám alebo fyzickým osobám zastupujúcim právnické osoby vydávajú prostriedky elektronickej identifikácie“;

c) Bod 14 sa nahrádza takto:

„14. „certifikát pre elektronický podpis“ je elektronické osvedčenie alebo súbor osvedčení, ktoré alebo ktorý spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym“;

d) Bod 16 sa nahrádza takto:

„16. „dôveryhodná služba“ je elektronická služba, ktorá sa spravidla poskytuje za odmenu a spočíva:

- a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky, elektronického osvedčenia atribútov a certifikátov, ktoré s týmito službami súvisia;
- b) vo vyhotovovaní, overovaní a validácii certifikátov na autentifikáciu webových sídiel;
- c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia;
- d) v elektronickej archivácii elektronických dokumentov;
- e) v správe zariadení na vyhotovenie elektronického podpisu na diaľku a elektronickej pečate na diaľku;
- f) v zaznamenávaní elektronických údajov do elektronického registra.“;

e) Bod 21 sa nahrádza takto:

„21. „produkt“ je hardvér alebo softvér alebo príslušné zložky hardvéru a/alebo softvéru určené na používanie pri poskytovaní elektronickej identifikácie a dôveryhodných služieb“;

f) Vkladajú sa tieto body 23a a 23b:

„23a. „zariadenie na vyhotovenie kvalifikovaného podpisu na diaľku“ je zariadenie na vyhotovenie kvalifikovaného elektronického podpisu, v ktorom kvalifikovaný poskytovateľ dôveryhodných služieb v mene podpisovateľa vytvára, spravuje alebo duplikuje údaje na vyhotovenie elektronického podpisu;

23b. „zariadenie na vyhotovenie kvalifikovanej pečate na diaľku“ je zariadenie na vyhotovenie kvalifikovanej elektronickej pečate, v ktorom kvalifikovaný poskytovateľ dôveryhodných služieb v mene pôvodcu pečate vytvára, spravuje alebo duplikuje údaje na vyhotovenie elektronickej pečate“;

g) Bod 29 sa nahrádza takto:

„29. „certifikát pre elektronicú pečať“ je elektronické osvedčenie alebo súbor osvedčení, ktoré alebo ktorý spája údaje na validáciu elektronickej pečate s právnickou osobou a potvrdzuje jej názov“;

h) Bod 41 sa nahrádza takto:

„41. „validácia“ je proces overenia a potvrdenia, že elektronický podpis alebo elektronická pečať či osobné identifikačné údaje alebo elektronické osvedčenie atribútov sú platné;“;

i) Dopĺňajú sa tieto body 42 až 55:

„42. „európska peňaženka digitálnej identity“ je produkt a služba, ktoré používateľovi umožňujú uchovávať údaje o totožnosti, potvrdenia a atribúty spojené s jeho totožnosťou, na požiadanie ich poskytovať spoľiehajúcim sa stranám a používať ich na autentifikáciu online aj offline na účely služby v súlade s článkom 6a a vyhotovovať kvalifikované elektronické podpisy a pečate;

43. „atribút“ je prvok, charakteristika alebo vlastnosť fyzickej alebo právnickej osoby alebo subjektu, v elektronickej forme;

44. „elektronické osvedčenie atribútov“ je osvedčenie v elektronickej forme, ktoré umožňuje autentifikáciu atribútov;

45. „kvalifikované elektronické osvedčenie atribútov“ je elektronické osvedčenie atribútov, ktoré vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a ktoré spĺňa požiadavky stanovené v prílohe V;

46. „autentický zdroj“ je register alebo systém, za ktorý je zodpovedný subjekt verejného sektora alebo súkromný subjekt, ktorý obsahuje atribúty o fyzickej alebo právnickej osobe a považuje sa za primárny zdroj týchto informácií alebo je v rámci vnútroštátneho práva uznaný za autentický;

47. „elektronická archivácia“ je služba zabezpečujúca príjem, uchovávanie, vymazávanie a prenos elektronických údajov alebo dokumentov s cieľom zaručiť počas celého obdobia uchovávania ich integritu, správnosť ich pôvodu a ich právne prvky;

48. „kvalifikovaná elektronická archivačná služba“ je služba, ktorá spĺňa požiadavky stanovené v článku 45g;

49. „značka dôvery EÚ pre peňaženku digitálnej identity“ je jednoduché, rozpoznateľné a jasné označenie toho, že peňaženka digitálnej identity bola vydaná v súlade s týmto nariadením;

50. „silná autentifikácia používateľa“ je autentifikácia založená na použití dvoch alebo viacerých prvkov kategorizovaných ako znalosti, vlastníctvo a charakteristické znaky používateľa, ktoré sú od seba nezávislé takým spôsobom, že porušenie jedného prvku neohrozuje spoľahlivosť ostatných prvkov, a je navrhnutá tak, aby chránila dôvernosť autentifikačných údajov;

51. „používateľské konto“ je mechanizmus, ktorý používateľovi umožňuje prístup k verejným alebo súkromným službám za podmienok stanovených poskytovateľom služieb;

52. „potvrdenie“ je doklad o schopnostiach, skúsenostiach, právach alebo povolení osoby;

53. „elektronický register“ je elektronický záznam údajov zabezpečený proti neoprávnenej manipulácii, ktorý zaisťuje autenticitu a integritu údajov, ktoré obsahuje, správnosť ich dátumu a času a ich chronologického usporiadania;
54. „osobné údaje“ sú všetky informácie v zmysle vymedzenia v článku 4 bode 1 nariadenia (EÚ) 2016/679;
55. „jedinečná identifikácia“ je proces, pri ktorom sa osobné identifikačné údaje alebo osobné identifikačné prostriedky priradia k existujúcemu kontu patriacemu tej istej osobe alebo sa s ním prepoja.“

4. Článok 5 sa nahrádza takto:

„Článok 5

Pseudonymy v elektronickej transakcii

Bez toho, aby bol dotknutý právny účinok pseudonymov podľa vnútroštátneho práva, nie je ich používanie pri elektronických transakciách zakázané.“

5. V kapitole II sa nadpis nahrádza takto:

„ODDIEL I

ELEKTRONICKÁ IDENTIFIKÁCIA“.

6. Článok 6 sa vypúšťa.

7. Vkladajú sa tieto články 6a, 6b, 6c a 6d:

„Článok 6a

Európske peňaženky digitálnej identity

1. S cieľom zabezpečiť, aby všetky fyzické a právnické osoby v Únii mali bezpečný, dôveryhodný a bezproblémový prístup k cezhraničným verejným a súkromným službám, každý členský štát vydá do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia európsku peňaženku digitálnej identity.
2. Európske peňaženky digitálnej identity:
 - a) vydáva členský štát;
 - b) sa vydávajú na základe poverenia členského štátu;
 - c) sa vydávajú nezávisle, ale členský štát ich uznáva.
3. Európske peňaženky digitálnej identity používateľovi umožňujú:
 - a) bezpečne požadovať a získavať, uchovávať, vyberať, kombinovať a zdieľať potrebné zákonné osobné identifikačné údaje a elektronické osvedčenie atribútov na autentifikáciu online aj offline spôsobom, ktorý je pre používateľa transparentný a vysledovateľný, na účely využívania verejných a súkromných online služieb;
 - b) podpisovať pomocou kvalifikovaných elektronických podpisov.
4. Európske peňaženky digitálnej identity najmä:
 - a) zabezpečujú spoločné rozhranie:

1. kvalifikovaným a nekvalifikovaným poskytovateľom dôveryhodných služieb, ktorí vydávajú kvalifikované a nekvalifikované elektronické osvedčenia atribútov alebo iné kvalifikované a nekvalifikované certifikáty na účely vydávania takýchto potvrdení a certifikátov pre európsku peňaženku digitálnej identity;
 2. pre spoliehajúce sa strany, aby mohli požadovať a validovať osobné identifikačné údaje a elektronické osvedčenia atribútov;
 3. na predkladanie osobných identifikačných údajov, elektronických osvedčení atribútov alebo iných údajov, ako sú napríklad potvrdenia, v lokálnom režime, v ktorom si peňaženka nevyžaduje prístup k internetu, spoliehajúcim sa stranám;
 4. pre používateľa s cieľom umožniť interakciu s európskou peňaženkou digitálnej identity a zobraziť „značku dôvery EÚ pre peňaženku digitálnej identity“;
- b) zabezpečujú, aby poskytovatelia dôveryhodných služieb kvalifikovaných osvedčení atribútov nemohli dostávať žiadne informácie o používaní týchto atribútov;
 - c) spĺňajú požiadavky stanovené v článku 8, aby bola úroveň zabezpečenia „vysoká“, najmä pokiaľ ide o požiadavky na preukazovanie a overovanie totožnosti a na riadenie a autentifikáciu prostriedkov elektronickej identifikácie;
 - d) poskytujú mechanizmus na zabezpečenie toho, aby spoliehajúca sa strana bola schopná autentifikovať používateľa a prijímať elektronické osvedčenia atribútov;
 - e) zabezpečiť, aby osobné identifikačné údaje uvedené v článku 12 ods. 4 písm. d) jednoznačne a trvalo reprezentovali fyzickú alebo právnickú osobu, s ktorou sa spájajú.
5. Členské štáty poskytujú mechanizmy validácie pre európske peňaženky digitálnej identity s cieľom:
 - a) zabezpečiť, aby bolo možné overiť ich pravosť a platnosť;
 - b) umožniť spoliehajúcim sa stranám overiť platnosť osvedčení atribútov;
 - c) umožniť spoliehajúcim sa stranám a kvalifikovaným poskytovateľom dôveryhodných služieb overiť pravosť a platnosť priradených osobných identifikačných údajov.
 6. Európske peňaženky digitálnej identity sa vydávajú v rámci oznámenej schémy elektronickej identifikácie, ktorej úroveň zabezpečenia je „vysoká“. Používanie európskych peňaženiek digitálnej identity je pre fyzické osoby bezplatné.
 7. Používateľ musí mať európsku peňaženku digitálnej identity plne pod kontrolou. Vydavateľ európskej peňaženky digitálnej identity nesmie zhromažďovať informácie o používaní peňaženky, ktoré nie sú potrebné na poskytovanie služieb peňaženky, ani spájať osobné identifikačné údaje a akékoľvek iné osobné údaje uložené alebo týkajúce sa používania európskej peňaženky digitálnej identity s osobnými údajmi z akýchkoľvek iných služieb ponúkaných týmto vydavateľom alebo zo služieb tretích strán, ktoré nie sú

potrebné na poskytovanie služieb peňaženky, pokiaľ o to používateľ výslovne nepožiadaval. Osobné údaje týkajúce sa poskytovania európskych peňaženiek digitálnej identity sa uchovávajú fyzicky a logicky oddelene od všetkých ostatných uchovávaných údajov. Ak je európska peňaženka digitálnej identity poskytovaná súkromnými subjektmi v súlade s odsekom 2 písm. b) a c), ustanovenia článku 45f ods. 4 sa uplatňujú *mutatis mutandis*.

8. Článok 11 sa na európsku peňaženku digitálnej identity uplatňuje *mutatis mutandis*.
9. Článok 24 ods. 2 písm. b), e), g) a h) sa uplatňujú *mutatis mutandis* na členské štáty vydávajúce európske peňaženky digitálnej identity.
10. Európska peňaženka digitálnej identity sa sprístupní osobám so zdravotným postihnutím v súlade s požiadavkami na prístupnosť uvedenými v prílohe I k smernici 2019/882.
11. Do 6 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia stanoví technické a prevádzkové špecifikácie a referenčné normy pre požiadavky uvedené v odsekoch 3, 4 a 5 prostredníctvom vykonávacieho aktu o implementácii európskej peňaženky digitálnej identity. Tento vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 6b

Spoliehajúce sa strany v prípade európskych peňaženiek digitálnej identity

1. Ak majú spoliehajúce sa strany v úmysle využívať európske peňaženky digitálnej identity vydané v súlade s týmto nariadením, oznámia to členskému štátu, v ktorom je spoliehajúca sa strana usadená, aby sa zabezpečil súlad s požiadavkami stanovenými v práve Únie alebo vo vnútroštátnom práve na poskytovanie osobitných služieb. Pri oznamovaní svojho zámeru využívať európske peňaženky digitálnej identity informujú aj o zamýšľanom použití európskej peňaženky digitálnej identity.
2. Členské štáty zavedú spoločný mechanizmus autentifikácie spoliehajúcich sa strán.
3. Spoliehajúce sa strany sú zodpovedné za vykonanie postupu autentifikácie osobných identifikačných údajov a elektronické osvedčenie atribútov pochádzajúcich z európskych peňaženiek digitálnej identity.
4. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia stanoví technické a prevádzkové špecifikácie pre požiadavky uvedené v odsekoch 1 a 2 prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 10.

Článok 6c

Certifikácia európskych peňaženiek digitálnej identity

1. Európske peňaženky digitálnej identity, ktoré boli certifikované alebo pre ktoré bolo vydané vyhlásenie o zhode v rámci systému kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 a na ktoré boli uverejnené odkazy v Úradnom vestníku Európskej únie, sa považujú za vyhovujúce požiadavkám týkajúcim sa kybernetickej bezpečnosti stanoveným v článku 6a ods. 3, 4 a 5, pokiaľ certifikát kybernetickej bezpečnosti alebo vyhlásenie o zhode alebo ich časti tieto požiadavky spĺňajú.

2. Súlad s požiadavkami stanovenými v článku 6a ods. 3, 4 a 5 týkajúcimi sa operácií spracúvania osobných údajov, ktoré vykonáva vydavateľ európskych peňaženiek digitálnej identity, sa certifikuje podľa nariadenia (EÚ) 2016/679.
3. Súlad európskych peňaženiek digitálnej identity s požiadavkami stanovenými v článku 6a odsekoch 3, 4 a 5 certifikujú akreditované verejné alebo súkromné subjekty určené členskými štátmi.
4. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov vypracuje zoznam noriem na certifikáciu európskych peňaženiek digitálnej identity uvedenú v odseku 3.
5. Členské štáty oznámia Komisii názvy a adresy verejných alebo súkromných subjektov, ktoré sú uvedené v odseku 3. Komisia sprístupní tieto informácie členským štátom.
6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 47, pokiaľ ide o stanovenie osobitných kritérií, ktoré musia splniť určené subjekty uvedené v odseku 3.

Článok 6d

Uverejnenie zoznamu certifikovaných európskych peňaženiek digitálnej identity

1. Členské štáty bez zbytočného odkladu informujú Komisiu o európskych peňaženkách digitálnej identity, ktoré boli vydané podľa článku 6a a certifikované subjektmi uvedenými v článku 6c ods. 3. Takisto bez zbytočného odkladu informujú Komisiu v prípade, keď sa certifikácia zruší.
 2. Komisia na základe získaných informácií vypracuje, zverejní a vedie zoznam certifikovaných európskych peňaženiek digitálnej identity.
 3. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia vymedzí formáty a postupy uplatniteľné na účely odseku 1 prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 10.“
8. Pred článok 7 sa vkladá tento nadpis:
- „ODDIEL II
- SCHÉMY ELEKTRONICKEJ IDENTIFIKÁCIE“.**
9. Úvodná veta článku 7 sa nahrádza takto:
- „Podľa článku 9 ods. 1 členské štáty oznámia do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia aspoň jednu schému elektronickej identifikácie zahŕňajúcu aspoň jeden prostriedok identifikácie:“.
10. V článku 9 sa odseky 2 a 3 nahrádzajú takto:
- „2. Komisia v *Úradnom vestníku Európskej únie* uverejní zoznam schém elektronickej identifikácie oznámených podľa odseku 1 tohto článku a základné informácie o nich.
 3. Komisia uverejní zmeny zoznamu uvedeného v odseku 2 v *Úradnom vestníku Európskej únie* do jedného mesiaca od prijatia oznámenia.“
11. Vkladá sa tento článok 10a:
- „Článok 10a

Narušenie bezpečnosti európskych peňaženiek digitálnej identity

1. Ak sú európske peňaženky digitálnej identity vydané podľa článku 6a a mechanizmy validácie uvedené v článku 6a ods. 5 písm. a), b) a c) narušené alebo čiastočne skompromitované spôsobom, ktorý ovplyvňuje ich spoľahlivosť alebo spoľahlivosť iných európskych peňaženiek digitálnej identity, vydávajúci členský štát bezodkladne pozastaví vydávanie a zruší platnosť danej európskej peňaženky digitálnej identity a informuje o tom ostatné členské štáty a Komisiu.
 2. Po náprave narušenia alebo skompromitovania uvedeného v odseku 1 vydávajúci členský štát obnoví vydávanie a používanie európskej peňaženky digitálnej identity a bez zbytočného odkladu o tom informuje ostatné členské štáty a Komisiu.
 3. Ak sa narušenie alebo skompromitovanie uvedené v odseku 1 neodstráni do troch mesiacov od pozastavenia alebo zrušenia, príslušný členský štát stiahne predmetnú európsku peňaženku digitálnej identity a informuje o tomto stiahnutí ostatné členské štáty a Komisiu. Ak je to odôvodnené závažnosťou narušenia, príslušná európska peňaženka digitálnej identity sa stiahne bezodkladne.
 4. Komisia bez zbytočného odkladu uverejní zodpovedajúce zmeny zoznamu uvedeného v článku 6d v *Úradnom vestníku Európskej únie*.
 5. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia podrobnejšie vymedzí opatrenia uvedené v odsekoch 1 a 3 prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 10.“
12. Vkladá sa tento článok 11a:
- „Článok 11a*
- Jedinečná identifikácia**
1. Ak sa na autentifikáciu používajú oznámené prostriedky elektronickej identifikácie a európske peňaženky digitálnej identity, členské štáty musia zabezpečiť jedinečnú identifikáciu.
 2. Členské štáty na účely tohto nariadenia musia do minimálneho súboru osobných identifikačných údajov uvedených v článku 12 ods. 4 písm. d) zahrnúť jedinečný a trvalý identifikátor v súlade s právom Únie na identifikáciu používateľa na jeho žiadosť v tých prípadoch, keď sa identifikácia používateľa vyžaduje podľa právnych predpisov.
 3. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia podrobnejšie vymedzí opatrenia uvedené v odsekoch 1 a 2 prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 10.“
13. Článok 12 sa mení takto:
- a) V odseku 3 sa vypúšťajú písmená c) a d);
 - b) V odseku 4 sa písmeno d) nahrádza takto:

- „d) odkaz na minimálny súbor osobných identifikačných údajov potrebných na jedinečnú a trvalú reprezentáciu fyzickej alebo právnickej osoby;“;
- c) V odseku 6 sa písmeno a) nahrádza takto:
 - „a) vo výmene informácií, skúseností a osvedčených postupov, pokiaľ ide o schémy elektronickej identifikácie, a najmä technické požiadavky týkajúce sa interoperability, jedinečnej identifikácie a úrovni zabezpečenia;“.

14. Vkladá sa tento článok 12a:

„Článok 12a

Certifikácia schém elektronickej identifikácie

1. Zhodu oznámených schém elektronickej identifikácie s požiadavkami stanovenými v článku 6a, článku 8 a článku 10 môžu certifikovať verejné alebo súkromné subjekty určené členskými štátmi.
2. Partnerské preskúmanie schém elektronickej identifikácie uvedené v článku 12 ods. 6 písm. c) sa nevzťahuje na schémy elektronickej identifikácie alebo časť takýchto schém, ktoré sú certifikované v súlade s odsekom 1. Členské štáty môžu na preukázanie súladu takýchto schém s požiadavkami stanovenými v článku 8 ods. 2, pokiaľ ide o úrovne zabezpečenia schém elektronickej identifikácie, použiť certifikát alebo vyhlásenie Únie o zhode vydané v súlade s príslušným európskym systémom certifikácie kybernetickej bezpečnosti stanoveným podľa nariadenia (EÚ) 2019/881.
3. Členské štáty oznámia Komisii názvy a adresy verejných alebo súkromných subjektov, ktoré sú uvedené v odseku 1. Komisia sprístupní tieto informácie členským štátom.“

15. Za článok 12a sa vkladá tento nadpis:

„ODDIEL III

CEZHRANIČNÉ VYUŽÍVANIE PROSTRIEDKOV ELEKTRONICKEJ IDENTIFIKÁCIE“.

16. Vkladajú sa tieto články 12b a 12c:

„Článok 12b

Cezhraničné využívanie európskych peňaženiek digitálnej identity

1. Ak členské štáty podľa vnútroštátneho práva alebo administratívnej praxe na prístup k online službe, ktorú poskytuje subjekt verejného sektora, vyžadujú elektronickej identifikáciu s použitím prostriedkov elektronickej identifikácie a autentifikáciou, akceptujú aj európske peňaženky digitálnej identity vydané v súlade s týmto nariadením.
2. Ak sa podľa vnútroštátneho práva alebo práva Únie od súkromných spoliehajúcich sa strán, ktoré poskytujú služby, vyžaduje, aby na online identifikáciu používali silnú autentifikáciu používateľa, alebo ak sa silná autentifikácia používateľa vyžaduje na základe zmluvnej povinnosti, a to aj v oblastiach dopravy, energetiky, bankovníctva a finančných služieb, sociálneho zabezpečenia, zdravia, pitnej vody, poštových služieb, digitálnej infraštruktúry, vzdelávania alebo telekomunikácií, súkromné spoliehajúce sa strany takisto

akceptujú používanie európskych peňaženiek digitálnej identity vydaných v súlade s článkom 6a.

3. Ak veľmi veľké online platformy vymedzené v článku 25 ods. 1 nariadenia [referenčné nariadenie DSA] vyžadujú, aby sa používatelia autentifikovali na prístup k online službám, akceptujú aj používanie európskych peňaženiek digitálnej identity vydaných v súlade s článkom 6a výlučne na základe dobrovoľnej žiadosti používateľa a s minimálnymi atribútmi potrebnými pre konkrétnu online službu, pre ktorú sa autentifikácia požaduje, ako napríklad dôkaz o veku.
4. Komisia podporuje a uľahčuje vypracúvanie samoregulačných kódexov správania na úrovni Únie (ďalej len „kódexy správania“) s cieľom prispieť k širokej dostupnosti a použiteľnosti európskych peňaženiek digitálnej identity v rozsahu pôsobnosti tohto nariadenia. Týmto kódexmi správania sa zabezpečuje akceptácia prostriedkov elektronickej identifikácie vrátane európskych peňaženiek digitálnej identity v rozsahu pôsobnosti tohto nariadenia, a to najmä zo strany poskytovateľov služieb, ktorí na autentifikáciu používateľov využívajú služby elektronickej identifikácie tretích strán. Komisia uľahčí vypracovanie takýchto kódexov správania v úzkej spolupráci so všetkými príslušnými zainteresovanými stranami a podporí poskytovateľov služieb, aby dokončili vypracovanie kódexov správania do 12 mesiacov od prijatia tohto nariadenia a účinne ich vykonávali do 18 mesiacov od prijatia tohto nariadenia.
5. Komisia do 18 mesiacov po zavedení európskych peňaženiek digitálnej identity posúdi, či na základe dôkazov preukazujúcich dostupnosť a použiteľnosť európskej peňaženky digitálnej identity bude ďalším súkromným poskytovateľom online služieb uložená povinnosť akceptovať používanie európskej peňaženky digitálnej identity výlučne na základe dobrovoľnej žiadosti používateľa. Kritériá posudzovania môžu zahŕňať rozsah používateľskej základne, cezhraničnú prítomnosť poskytovateľov služieb, technologický vývoj, vývoj modelov používania. Komisia je splnomocnená na základe tohto posúdenia prijímať delegované akty týkajúce sa revízie požiadaviek na uznávanie európskej peňaženky digitálnej identity podľa bodov 1 až 4 tohto článku.
6. Na účely tohto článku sa na európske peňaženky digitálnej identity nevzťahujú požiadavky uvedené v článkoch 7 a 9.

Článok 12c

Vzájomné uznávanie iných prostriedkov elektronickej identifikácie

1. Keď sa podľa vnútroštátneho práva alebo administratívnej praxe na prístup k online službe, ktorú poskytuje subjekt verejného sektora v jednom členskom štáte, vyžaduje elektronická identifikácia pomocou prostriedku elektronickej identifikácie a autentifikácia, prostriedok elektronickej identifikácie vydaný v inom členskom štáte sa v prvom členskom štáte uznáva na účely cezhraničnej autentifikácie pre danú online službu, ak sú splnené tieto podmienky:
 - a) prostriedok elektronickej identifikácie bol vydaný v rámci schémy elektronickej identifikácie, ktorá je začlenená do zoznamu uvedenom v článku 9;

- b) úroveň zabezpečenia prostriedku elektronickej identifikácie zodpovedá úrovni zabezpečenia, ktorá je rovnaká alebo vyššia ako úroveň zabezpečenia, ktorú vyžaduje príslušný subjekt verejného sektora na prístup k danej online službe v príslušnom členskom štáte, a v žiadnom prípade nesmie byť nižšia ako úroveň zabezpečenia „pokročilá“;
- c) príslušný subjekt verejného sektora v dotknutom členskom štáte používa vo vzťahu k prístupu k danej online službe úroveň zabezpečenia „pokročilá“ alebo „vysoká“.

Takéto uznávanie sa začne najneskôr 6 mesiacov po tom, ako Komisia uverejní zoznam uvedený v písmene a) prvého pododseku.

- 2. Prostriedok elektronickej identifikácie, ktorý je vydaný v rozsahu pôsobnosti schémy elektronickej identifikácie začlenenej do zoznamu uvedeného v článku 9 a ktorý zodpovedá úrovni zabezpečenia „nízka“, môžu subjekty verejného sektora uznávať na účely cezhraničnej autentifikácie v prípade online služieb, ktoré tieto subjekty poskytujú.“

17. V článku 13 sa odsek 1 nahrádza takto:

- „1. Bez ohľadu na odsek 2 tohto článku sú poskytovatelia dôveryhodných služieb zodpovední za škodu spôsobenú úmyselne alebo z neobstaranosti akejkoľvek fyzickej alebo právnickej osobe v dôsledku nedodržania povinností podľa tohto nariadenia a povinností v oblasti riadenia kybernetickobezpečnostných rizík podľa článku 18 smernice XXXX/XXXX [NIS2].“

18. Článok 14 sa nahrádza takto:

„Článok 14

Medzinárodné aspekty

- 1. Komisia môže v súlade s článkom 48 ods. 2 prijať vykonávacie akty stanovujúce podmienky, za ktorých možno požiadavky tretej krajiny uplatniteľné na poskytovateľov dôveryhodných služieb usadených na jej území a na dôveryhodné služby, ktoré poskytujú, považovať za rovnocenné s požiadavkami uplatniteľnými na kvalifikovaných poskytovateľov dôveryhodných služieb usadených v Únii a na kvalifikované dôveryhodné služby, ktoré poskytujú.
- 2. Ak Komisia prijala vykonávací akt podľa odseku 1 alebo uzavrela medzinárodnú dohodu o vzájomnom uznávaní dôveryhodných služieb v súlade s článkom 218 zmluvy, dôveryhodné služby poskytované poskytovateľmi usadenými v príslušnej tretej krajine sa považujú za rovnocenné s kvalifikovanými dôveryhodnými službami poskytovanými kvalifikovanými poskytovateľmi dôveryhodných služieb usadenými v Únii.“

19. Článok 15 sa nahrádza takto:

„Článok 15

Prístupnosť pre osoby so zdravotným postihnutím

Poskytovanie dôveryhodných služieb a produktov pre koncových používateľov používaných pri poskytovaní týchto služieb sa sprístupní osobám so zdravotným postihnutím v súlade s požiadavkami na prístupnosť uvedenými v prílohe I k smernici 2019/882 o požiadavkách na prístupnosť výrobkov a služieb.“

20. Článok 17 sa mení takto:

a) Odsek 4 sa mení takto:

1. V odseku 4 sa písmeno c) nahrádza takto:

„c) informovať príslušné vnútroštátne orgány dotknutých členských štátov určené podľa smernice (EÚ) XXXX/XXXX [NIS2] o každom významnom narušení bezpečnosti alebo strate integrity, o ktorom sa dozvedia pri plnení svojich úloh. Ak sa závažné narušenie bezpečnosti alebo strata integrity týka iných členských štátov, orgán dohľadu informuje jednotné kontaktné miesto dotknutého členského štátu určené podľa smernice (EÚ) XXXX/XXXX (NIS2);“;

2. Písmeno f) nahrádza takto:

„f) spolupracovať s orgánmi dohľadu zriadenými podľa nariadenia (EÚ) 2016/679, najmä ich bez zbytočného odkladu informovať o výsledkoch auditov kvalifikovaných poskytovateľov dôveryhodných služieb, ak boli porušené pravidlá ochrany osobných údajov, a o narušeníach bezpečnosti, ktoré predstavujú narušenie ochrany osobných údajov;“;

b) Odsek 6 sa nahrádza takto:

„6. Každý rok do 31. marca predloží každý orgán dohľadu Komisii správu o svojich hlavných činnostiach počas predchádzajúceho kalendárneho roka.“;

c) Odsek 8 sa nahrádza takto:

„8. Komisia do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia prostredníctvom vykonávacích aktov podrobnejšie vymedzí úlohy orgánov dohľadu uvedených v odseku 4 a vymedzí formáty a postupy na podávanie správ uvedených v odseku 6. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

21. Článok 18 sa mení takto:

a) Názov článku 18 sa nahrádza takto:

„**Vzájomná pomoc a spolupráca**“;

b) Odsek 1 sa nahrádza takto:

„1. Orgány dohľadu spolupracujú s cieľom výmeny osvedčených postupov a informácií týkajúcich sa poskytovania dôveryhodných služieb.“;

c) Dopĺňajú sa tieto odseky 4 a 5:

„4. Orgány dohľadu a príslušné vnútroštátne orgány podľa smernice Európskeho parlamentu a Rady (EÚ) XXXX/XXXX [NIS2] spolupracujú a navzájom si pomáhajú pri zabezpečovaní toho, aby poskytovatelia dôveryhodných služieb spĺňali požiadavky stanovené v tomto nariadení a v smernici (EÚ) XXXX/XXXX [NIS2]. Orgán dohľadu požiada príslušný vnútroštátny orgán podľa smernice XXXX/XXXX [NIS2], aby vykonal opatrenia dohľadu na overenie dodržiavania požiadaviek podľa smernice XXXX/XXXX [NIS2] zo

strany poskytovateľov dôveryhodných služieb, aby od poskytovateľov dôveryhodných služieb vyžadoval nápravu akéhokoľvek nedodržania týchto požiadaviek, aby včas poskytol výsledky všetkých činností dohľadu spojených s poskytovateľmi dôveryhodných služieb a aby informoval orgány dohľadu o relevantných incidentoch oznámených v súlade so smernicou XXXX/XXXX [NIS2].

5. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov stanoví potrebné dojednania o postupe na uľahčenie spolupráce medzi orgánmi dohľadu uvedenými v odseku 1.“

22. Článok 20 sa mení takto:

- a) Odsek 1 sa nahrádza takto:

„1. Kvalifikovaní poskytovatelia dôveryhodných služieb aspoň každých 24 mesiacov podliehajú auditu na vlastné náklady, ktorý vykonáva orgán posudzovania zhody. Auditom sa potvrdí, že kvalifikovaní poskytovatelia dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky stanovené v tomto nariadení a v článku 18 smernice (EÚ) XXXX/XXXX [NIS2]. Kvalifikovaní poskytovatelia dôveryhodných služieb predložia orgánu dohľadu výslednú správu o posúdení zhody do troch pracovných dní od prijatia.“;

- b) V odseku 2 sa posledná veta nahrádza takto:

„Ak sa zdá, že boli porušené predpisy týkajúce sa ochrany osobných údajov, orgán dohľadu informuje o výsledkoch svojho auditu orgány dohľadu podľa nariadenia (EÚ) 2016/679.“;

- c) Odseky 3 a 4 sa nahrádzajú takto:

„3. Ak kvalifikovaný poskytovateľ dôveryhodných služieb nesplní niektorú z požiadaviek stanovených v tomto nariadení, orgán dohľadu ho požiada, aby v prípade potreby v stanovenej lehote poskytol nápravu.

Ak uvedený poskytovateľ neposkytne nápravu, v prípade potreby v lehote stanovenej orgánom dohľadu, orgán dohľadu môže, berúc do úvahy najmä rozsah, trvanie a dôsledky neposkytnutia nápravy, odňať príslušnému poskytovateľovi alebo službe, ktorú poskytuje, kvalifikovaný štatút a požiadať ho, aby v prípade potreby v stanovenej lehote splnil požiadavky smernice XXXX/XXXX [NIS2]. Orgán dohľadu informuje orgán uvedený v článku 22 ods. 3 na účely aktualizácie dôveryhodných zoznamov uvedených v článku 22 ods. 1.

Orgán dohľadu informuje kvalifikovaného poskytovateľa dôveryhodných služieb o odňatí jeho kvalifikovaného štatútu alebo kvalifikovaného štatútu dotknutej služby.

4. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné číslo pre tieto normy:

- a) akreditácia orgánov posudzovania zhody a správa o posúdení zhody uvedená v odseku 1;

- b) požiadavky na audit pre orgány posudzovania zhody na vykonávanie posudzovania zhody kvalifikovaných poskytovateľov dôveryhodných služieb uvedených v odseku 1, ktoré vykonávajú orgány posudzovania zhody;
- c) systémy posudzovania zhody na vykonávanie posudzovania zhody kvalifikovaných poskytovateľov dôveryhodných služieb orgánmi posudzovania zhody a na poskytnutie správy o posúdení zhody uvedenej v odseku 1.

Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

23. Článok 21 sa mení takto:

a) Odsek 2 sa nahrádza takto:

„2. Orgán dohľadu overí, či poskytovateľ dôveryhodných služieb a dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky stanovené v tomto nariadení, a to najmä požiadavky na kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú.

S cieľom overiť, či poskytovateľ dôveryhodných služieb dodržiava požiadavky stanovené v článku 18 smernice XXXX [NIS2], orgán dohľadu požiada príslušné orgány uvedené v smernici XXXX [NIS2], aby v tejto súvislosti vykonali opatrenia dohľadu a poskytli informácie o výsledku do troch dní od ich ukončenia.

Ak orgán dohľadu usúdi, že poskytovateľ dôveryhodných služieb a dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky uvedené v prvom pododseku, udelí tomuto poskytovateľovi dôveryhodných služieb a dôveryhodným službám, ktoré poskytuje, kvalifikovaný štatút a informuje orgán uvedený v článku 22 ods. 3 na účely aktualizácie dôveryhodných zoznamov uvedených v článku 22 ods. 1, a to najneskôr do troch mesiacov po oznámení v súlade s odsekom 1 tohto článku.

Ak sa overovanie neukončí do troch mesiacov od oznámenia, orgán dohľadu o tom informuje poskytovateľa dôveryhodných služieb a oznámi mu dôvody omeškania a lehotu, v ktorej sa overovanie má ukončiť.“;

b) Odsek 4 sa nahrádza takto:

„4. Komisia do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia prostredníctvom vykonávacích aktov vymedzí formáty a postupy oznamovania a overovania na účely odsekov 1 a 2 tohto článku. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

24. V článku 23 sa dopĺňa tento odsek 2a:

„2a. Odseky 1 a 2 sa uplatňujú aj na poskytovateľov dôveryhodných služieb usadených v tretích krajinách a na služby, ktoré poskytujú, za predpokladu, že boli uznané v Únii v súlade s článkom 14.“

25. Článok 24 sa mení takto:

a) Odsek 1 sa nahrádza takto:

„1. Pri vydávaní kvalifikovaného certifikátu alebo kvalifikovaného elektronického osvedčenia atribútov pre dôveryhodnú službu kvalifikovaný poskytovateľ dôveryhodných služieb overí totožnosť a prípadne všetky osobitné atribúty fyzickej alebo právnickej osoby, ktorej sa kvalifikovaný certifikát alebo kvalifikované elektronické osvedčenie atribútu vydáva.

Informácie uvedené v prvom pododseku overuje kvalifikovaný poskytovateľ dôveryhodných služieb buď priamo, alebo prostredníctvom spolaľahnutia sa na tretiu stranu, a to ktorýmkoľvek z týchto spôsobov:

- a) prostredníctvom oznámených prostriedkov elektronickej identifikácie, ktoré spĺňajú požiadavky stanovené v článku 8, pokiaľ ide o úroveň zabezpečenia „pokročilá“ alebo „vysoká“;
- b) prostredníctvom kvalifikovaných elektronických osvedčení atribútov alebo certifikátu pre kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať vydaných v súlade s písmenom a), c) alebo d);
- c) použitím iných metód identifikácie, ktoré zabezpečujú identifikáciu fyzickej osoby s vysokou úrovňou spoľahlivosti, ktorých zhodu potvrdí orgán posudzovania zhody;
- d) fyzickou prítomnosťou fyzickej osoby alebo splnomocneného zástupcu právnickej osoby vhodnými postupmi a v súlade s vnútroštátnymi právnymi predpismi, ak nie sú k dispozícii iné prostriedky.“;

b) Vkladá sa tento odsek 1a:

„1a. Komisia do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia stanoví prostredníctvom vykonávacích aktov minimálne technické špecifikácie, normy a postupy, pokiaľ ide o overovanie totožnosti a atribútov v súlade s odsekom 1 písm. c). Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

c) Odsek 2 sa mení takto:

1. Písmeno d) sa nahrádza takto:

„d) pred uzavretím zmluvného vzťahu jasným, komplexným a ľahko dostupným spôsobom vo verejne prístupnom priestore a jednotlivo informuje každú osobu, ktorá chce využívať kvalifikovanú dôveryhodnú službu, o presných podmienkach využívania tejto služby vrátane obmedzení jej využívania;“;

2. Vkladajú sa tieto písmená fa) a fb):

„fa) má vhodné politiky a prijíma zodpovedajúce opatrenia na riadenie právnych, obchodných, prevádzkových a iných priamych alebo nepriamych rizík pre poskytovanie kvalifikovanej dôveryhodnej služby. Bez ohľadu na ustanovenia

článku 18 smernice EÚ XXXX/XXX [NIS2] tieto opatrenia zahŕňajú minimálne:

i) opatrenia týkajúce sa postupov registrácie a zavádzania v rámci určitej služby v súvislosti so službami;

ii) opatrenia týkajúce sa procesných alebo administratívnych kontrol;

iii) opatrenia týkajúce sa riadenia a vykonávania služieb;

fb) oznamuje orgánu dohľadu a prípadne iným príslušným orgánom všetky narušenia alebo porušenia súvisiace s vykonávaním opatrení uvedených v písmene fa) bodoch i), ii) a iii), ktoré majú významný vplyv na poskytovanú dôveryhodnú službu alebo na osobné údaje v nej uchovávané;“;

3. Písmená g) a h) sa nahrádzajú takto:

„g) prijíma vhodné opatrenia proti falšovaniu, krádeži alebo zneužitiu údajov alebo proti neoprávnenému vymazaniu, zmene alebo zneprístupneniu údajov;

h) zaznamenáva a tak dlho, ako je to potrebné, po ukončení činností kvalifikovaného poskytovateľa dôveryhodných služieb uchováva prístupné všetky relevantné informácie týkajúce sa údajov, ktoré kvalifikovaný poskytovateľ dôveryhodných služieb vydal a prijal, na účely predloženia dôkazov v súdnom konaní a na účely zabezpečenia kontinuity služby. Takéto zaznamenávanie sa môže vykonávať elektronicky;“;

4. Písmeno j) sa vypúšťa;

d) Vkladá sa tento odsek 4a:

„4a. Odseky 3 a 4 sa zodpovedajúcim spôsobom uplatňujú na zrušenie elektronických osvedčení atribútov.“;

e) Odsek 5 sa nahrádza takto:

„5. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem pre požiadavky uvedené v odseku 2. Ak dôveryhodné systémy a produkty spĺňajú uvedené normy, predpokladá sa, že sú v súlade s požiadavkami stanovenými v tomto článku. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

f) Vkladá sa tento odsek 6:

„6. Komisia je splnomocnená prijímať delegované akty týkajúce sa dodatočných opatrení uvedených v odseku 2 písm. fa).“

26. V článku 28 sa odsek 6 nahrádza takto:

„6. Do 12 mesiacov po nadobudnutí účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem pre kvalifikované certifikáty pre elektronický podpis. Ak kvalifikovaný certifikát pre elektronický podpis spĺňa uvedené normy, predpokladá sa, že je v súlade s požiadavkami stanovenými v prílohe I. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

27. V článku 29 sa dopĺňa tento nový odsek 1a:
- „1a. Generovanie, správu a duplikácie údajov na vyhotovenie elektronického podpisu v mene podpisovateľa môže vykonávať len kvalifikovaný poskytovateľ dôveryhodných služieb poskytujúci kvalifikovanú dôveryhodnú službu na správu zariadenia na vyhotovenie kvalifikovaného elektronického podpisu na diaľku.“
28. Vkladá sa tento článok 29a:
- „Článok 29a
- Požiadavky na kvalifikovanú službu na správu zariadení na vyhotovenie elektronického podpisu na diaľku**
1. Správu zariadení na vyhotovenie elektronických podpisov na diaľku ako kvalifikovanú službu môže vykonávať len kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý:
- a) generuje alebo spravuje údaje na vyhotovenie elektronického podpisu v mene podpisovateľa;
 - b) bez ohľadu na bod 1 písm. d) prílohy II duplikuje údaje na vyhotovenie elektronického podpisu len na účely zálohovania za predpokladu, že sú splnené tieto požiadavky:
bezpečnosť duplikovaných súborov údajov musí byť na rovnakej úrovni ako v prípade pôvodných súborov údajov;
počet duplikovaných súborov údajov nesmie prekročiť minimálne množstvo nevyhnutné na zabezpečenie kontinuity služby;
 - c) spĺňa všetky požiadavky uvedené v certifikačnej správe konkrétneho zariadenia na vyhotovenie kvalifikovaného podpisu na diaľku vydanéj podľa článku 30.
2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov stanoví technické špecifikácie a referenčné čísla noriem na účely odseku 1.“
29. V článku 30 sa vkladá tento odsek 3a:
- „3a. Certifikácia uvedená v odseku 1 je platná 5 rokov pod podmienkou pravidelného dvojročného posúdenia zraniteľnosti. Ak sa zistia slabé miesta a neodstránia sa, certifikácia sa zruší.“
30. V článku 31 sa odsek 3 nahrádza takto:
- „3. Komisia do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia prostredníctvom vykonávacích aktov vymedzí formáty a postupy uplatniteľné na účely odseku 1. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“
31. Článok 32 sa mení takto:
- a) V odseku 1 sa dopĺňa tento pododsek:
„Ak validácia kvalifikovaných elektronických podpisov spĺňa normy uvedené v odseku 3, predpokladá sa, že je v súlade s požiadavkami stanovenými v prvom pododseku.“;

b) Odsek 3 sa nahrádza takto:

„3. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem na validáciu kvalifikovaných elektronických podpisov. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

32. Článok 34 sa nahrádza takto:

„Článok 34

Kvalifikovaná služba uchovávania kvalifikovaných elektronických podpisov

1. Kvalifikovanú službu uchovávania kvalifikovaných elektronických podpisov môže poskytovať iba kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý používa postupy a technológie, ktoré umožňujú predĺžiť dôveryhodnosť kvalifikovaného elektronického podpisu aj na obdobie po uplynutí technologickej platnosti.
2. Ak opatrenia týkajúce sa kvalifikovanej služby uchovávania kvalifikovaných elektronických podpisov spĺňajú normy uvedené v odseku 3, predpokladá sa, že sú v súlade s požiadavkami uvedenými v odseku 1.
3. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem pre kvalifikovanú službu uchovávania kvalifikovaných elektronických podpisov. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

33. Článok 37 sa mení takto:

a) Vkladá sa tento odsek 2a:

„2a. Ak zdokonalená elektronická pečať spĺňa normy uvedené v odseku 4, predpokladá sa, že je v súlade s požiadavkami na zdokonalené elektronické pečate uvedenými v článku 36 a odseku 5 tohto článku.“;

b) Odsek 4 sa nahrádza takto:

„4. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem pre zdokonalené elektronické pečate. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

34. Článok 38 sa mení takto:

a) Odsek 1 sa nahrádza takto:

„1. Kvalifikované certifikáty pre elektronické pečate musia spĺňať požiadavky stanovené v prílohe III. Ak kvalifikovaný certifikát pre elektronickú pečať spĺňa normy uvedené v odseku 6, predpokladá sa, že je v súlade s požiadavkami stanovenými v prílohe III.“;

b) Odsek 6 sa nahrádza takto:

„6. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem pre kvalifikované certifikáty pre elektronické pečate. Uvedené vykonávacie

akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

35. Vkladá sa tento článok 39a:

„Článok 39a

Požiadavky na kvalifikovanú službu na správu zariadení na vyhotovenie elektronických pečatí na diaľku

Článok 29a sa uplatňuje *mutatis mutandis* na kvalifikovanú službu na správu zariadení na vyhotovenie elektronických pečatí na diaľku.“

36. Článok 42 sa mení takto:

- a) Vkladá sa tento nový odsek 1a:

„1a. Ak spojenie dátumu a času s údajmi a presný zdroj času spĺňajú normy uvedené v odseku 2, predpokladá sa, že sú v súlade s požiadavkami stanovenými v odseku 1.“;

- b) Odsek 2 sa nahrádza takto:

„2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem na spojenie dátumu a času s údajmi a pre presné zdroje času. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

37. Článok 44 sa mení takto:

- a) Vkladá sa tento odsek 1a:

„1a. Ak proces odosielania a doručovania údajov spĺňa normy uvedené v odseku 2, predpokladá sa, že je v súlade s požiadavkami stanovenými v odseku 1.“;

- b) Odsek 2 sa nahrádza takto:

„2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem pre procesy odosielania a doručovania údajov. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

38. Článok 45 sa nahrádza takto:

„Článok 45

Požiadavky na kvalifikované certifikáty pre autentifikáciu webového sídla

1. Kvalifikované certifikáty pre autentifikáciu webového sídla musia spĺňať požiadavky stanovené v prílohe IV. Kvalifikované certifikáty pre autentifikáciu webového sídla sa považujú za vyhovujúce požiadavkám stanoveným v prílohe IV, ak spĺňajú normy uvedené v odseku 3.
2. Kvalifikované certifikáty pre autentifikáciu webového sídla uvedené v odseku 1 musia webové prehliadače uznávať. Na tieto účely webové prehliadače musia zabezpečiť, aby sa údaje o totožnosti poskytnuté pomocou ktorejkoľvek z metód zobrazovali používateľsky ústretovým spôsobom. Webové prehliadače musia zabezpečiť podporu kvalifikovaných certifikátov pre autentifikáciu

webového sídla uvedených v odseku 1 a interoperabilitu s nimi, s výnimkou podnikov, ktoré sa považujú za mikropodniky a malé podniky v súlade s odporúčaním Komisie 2003/361/ES počas prvých piatich rokov pôsobenia ako poskytovatelia služieb prehliadania webu.

3. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov stanoví špecifikácie a referenčné čísla noriem pre kvalifikované certifikáty pre autentifikáciu webového sídla uvedené v odseku 1. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

39. Za článok 45 sa vkladajú tieto oddiely 9, 10 a 11:

„ODDIEL 9

ELEKTRONICKÉ OSVEDČENIA ATRIBÚTOV

Článok 45a

Právne účinky elektronického osvedčenia atribútov

1. Právny účinok elektronického osvedčenia atribútov a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z dôvodu, že má elektronickú formu.
2. Kvalifikované elektronické osvedčenie atribútov má rovnaký právny účinok ako osvedčenie vydané v súlade so zákonom v papierovej podobe.
3. Kvalifikované elektronické osvedčenie atribútov vydané v jednom členskom štáte sa uznáva ako kvalifikované elektronické osvedčenie atribútov v ktoromkoľvek inom členskom štáte.

Článok 45b

Elektronické osvedčenia atribútov vo verejných službách

Ak sa podľa vnútroštátneho práva na prístup k online službe, ktorú poskytuje subjekt verejného sektora, vyžaduje elektronická identifikácia s použitím prostriedkov elektronickej identifikácie a autentifikácie, osobné identifikačné údaje v elektronickom osvedčení atribútov nenahrádzajú elektronickú identifikáciu prostredníctvom prostriedkov elektronickej identifikácie a autentifikáciu na účely elektronickej identifikácie, pokiaľ to výslovne nepovolí členský štát alebo subjekt verejného sektora. V takom prípade sa akceptuje aj kvalifikované elektronické osvedčenie atribútov z iných členských štátov.

Článok 45c

Požiadavky na kvalifikované osvedčenie atribútov

1. Kvalifikované elektronické osvedčenie atribútov musí spĺňať požiadavky stanovené v prílohe V. Kvalifikované elektronické osvedčenie atribútov sa považuje za vyhovujúce požiadavkám stanoveným v prílohe V, ak spĺňa normy uvedené v odseku 4.
2. Kvalifikované elektronické osvedčenia atribútov nesmú podliehať žiadnym povinným požiadavkám nad rámec požiadaviek stanovených v prílohe V.
3. Ak sa po počiatočnom vydaní kvalifikované elektronické osvedčenie atribútov zruší, stráca svoju platnosť okamihom zrušenia a jeho štatút sa za žiadnych okolností nesmie zmeniť na pôvodný.

4. Do 6 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia určí referenčné čísla noriem pre kvalifikované elektronické osvedčenia atribútov prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 10.

Článok 45d

Overovanie atribútov na základe autentických zdrojov

1. Členské štáty zabezpečia, aby sa aspoň v prípade atribútov uvedených v prílohe VI vždy, keď tieto atribúty využívajú autentické zdroje vo verejnom sektore, prijali opatrenia, ktoré kvalifikovaným poskytovateľom elektronických osvedčení atribútov umožnia na žiadosť používateľa elektronicky overiť pravosť atribútu priamo na základe príslušného autentického zdroja na vnútroštátnej úrovni alebo prostredníctvom určených sprostredkovateľov uznaných na vnútroštátnej úrovni v súlade s vnútroštátnym právom alebo právom Únie.
2. Komisia do 6 mesiacov od nadobudnutia účinnosti tohto nariadenia a s prihliadnutím na príslušné medzinárodné normy prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 10, stanoví minimálne technické špecifikácie, normy a postupy s odkazom na katalóg atribútov, systémy osvedčovania atribútov a overovacie postupy na kvalifikované elektronické osvedčovanie atribútov.

Článok 45e

Vydávanie elektronického osvedčenia atribútov európskym peňaženkami digitálnej identity

Poskytovatelia kvalifikovaných elektronických osvedčení atribútov poskytujú rozhranie s európskymi peňaženkami digitálnej identity vydanými v súlade s článkom 6a.

Článok 45f

Dodatočné pravidlá poskytovania služieb elektronického osvedčovania atribútov

1. Poskytovatelia služieb kvalifikovaného a nekvalifikovaného elektronického osvedčovania atribútov nesmú spájať osobné údaje týkajúce sa poskytovania týchto služieb s osobnými údajmi zo žiadnych iných služieb, ktoré ponúkajú.
2. Osobné údaje týkajúce sa poskytovania služieb elektronického osvedčovania atribútov sa uchovávali logicky oddelene od ostatných uchovávaných údajov.
3. Osobné údaje týkajúce sa poskytovania kvalifikovaných služieb elektronického osvedčovania atribútov sa uchovávali fyzicky a logicky oddelene od všetkých ostatných uchovávaných údajov.
4. Poskytovatelia kvalifikovaných služieb elektronického osvedčovania atribútov poskytujú takéto služby v rámci samostatnej právnickej osoby.

ODDIEL 10

KVALIFIKOVANÉ ELEKTRONICKÉ ARCHIVAČNÉ SLUŽBY

Článok 45g

Kvalifikované elektronické archivačné služby

Kvalifikovanú elektronickú archivačnú službu pre elektronické dokumenty môže poskytovať iba kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý používa postupy a technológie, ktoré umožňujú predĺžiť dôveryhodnosť elektronického dokumentu aj na obdobie po uplynutí technologickej platnosti.

Do 12 mesiacov po nadobudnutí účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí referenčné čísla noriem pre elektronické archivačné služby. Uvedené vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

ODDIEL 11

ELEKTRONICKÉ REGISTRE

Článok 45h

Právne účinky elektronických registrov

1. Právny účinok elektronického registra a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z toho dôvodu, že má elektronickú formu alebo že nespĺňa požiadavky pre kvalifikované elektronické registre.
2. Pri kvalifikovanom elektronickom registri platí domnienka jedinečnosti a pravosti údajov, ktoré obsahuje, správnosti ich dátumu a času a ich sekvenčného chronologického usporiadania v rámci daného registra.

Článok 45i

Požiadavky pre kvalifikované elektronické registre

1. Kvalifikované elektronické registre musia spĺňať tieto požiadavky:
 - a) vytvoril ich jeden alebo viacerí kvalifikovaní poskytovatelia dôveryhodných služieb;
 - b) zabezpečujú jedinečnosť, pravosť a správnu postupnosť údajov zaznamenaných v registri;
 - c) zabezpečujú správne sekvenčné chronologické poradie údajov v registri a správnosť dátumu a času vloženia údajov;
 - d) zaznamenávajú údaje takým spôsobom, aby bolo možné okamžite zistiť akúkoľvek následnú zmenu údajov.
2. Ak elektronický register spĺňa normy uvedené v odseku 3, predpokladá sa, že je v súlade s požiadavkami stanovenými v odseku 1.
3. Komisia môže prostredníctvom vykonávacích aktov určiť referenčné čísla noriem pre procesy vykonávania a registrácie súboru údajov v kvalifikovanom elektronickom registri a jeho vytvorenie. Uvedené vykonávacie akty sa prijímajú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

40. Vkladá sa tento článok 48a:

„Článok 48a

Požiadavky na podávanie správ

1. Členské štáty zabezpečujú zber štatistických údajov v súvislosti s fungovaním európskych peňaženiek digitálnej identity a kvalifikovaných dôveryhodných služieb.
2. Štatistické údaje zozbierané v súlade s odsekom 1 obsahujú:
 - a) počet fyzických a právnických osôb s platnou európskou peňaženkou digitálnej identity;
 - b) typ a počet služieb, ktoré akceptujú používanie európskej peňaženky digitálnej identity;
 - c) incidenty a výpadky infraštruktúry na vnútroštátnej úrovni, ktoré bránia používaniu aplikácií peňaženky digitálnej identity.
3. Štatistické údaje uvedené v odseku 2 sa sprístupnia verejnosti v otvorenom a bežne používanom strojovo čitateľnom formáte.
4. Členské štáty každoročne do marca predložia Komisii správu o štatistických údajoch zozbieraných v súlade s odsekom 2.“

41. Článok 49 sa nahrádza takto:

„Článok 49

Preskúmanie

1. Komisia preskúma uplatňovanie tohto nariadenia a podá o ňom správu Európskemu parlamentu a Rade do 24 mesiacov po nadobudnutí jeho účinnosti. Komisia vyhodnotí najmä, či je vhodné zmeniť rozsah pôsobnosti tohto nariadenia alebo jeho konkrétne ustanovenia, pričom sa zohľadnia skúsenosti získané počas uplatňovania tohto nariadenia, ako aj vývoj v oblasti technológií, trhu a práva. V prípade potreby sa k uvedenej správe pripojí návrh na zmenu tohto nariadenia.
2. Hodnotiaca správa musí obsahovať posúdenie dostupnosti a použiteľnosti prostriedkov identifikácie vrátane európskych peňaženiek digitálnej identity v rozsahu pôsobnosti tohto nariadenia a posúdi sa v nej, či by všetci súkromní poskytovatelia online služieb, ktorí pri autentifikácii používateľov využívajú služby elektronickej identifikácie tretích strán, mali byť povinní akceptovať používanie oznámených prostriedkov elektronickej identifikácie a európskych peňaženiek digitálnej identity.
3. Komisia okrem toho každé štyri roky po správe uvedenej v prvom odseku podáva Európskemu parlamentu a Rade správu o pokroku pri plnení cieľov tohto nariadenia.“

42. Článok 51 sa nahrádza takto:

„Článok 51

Prechodné opatrenia

1. Bezpečné zariadenia na vyhotovenie podpisu, ktorých zhoda bola určená v súlade s článkom 3 ods. 4 smernice 1999/93/ES, sa naďalej považujú za zariadenia na vyhotovenie kvalifikovaného elektronického podpisu podľa tohto nariadenia do [dátum – Ú. v., vložte obdobie štyroch rokov od nadobudnutia účinnosti tohto nariadenia].

2. Kvalifikované certifikáty vydané fyzickým osobám podľa smernice 1999/93/ES sa naďalej považujú za kvalifikované certifikáty elektronických podpisov podľa tohto nariadenia do [dátum – PO, vložte obdobie štyroch rokov od nadobudnutia účinnosti tohto nariadenia].“
43. Príloha I sa mení v súlade s prílohou I k tomuto nariadeniu.
44. Príloha II sa nahrádza textom uvedeným v prílohe II k tomuto nariadeniu.
45. Príloha III sa mení v súlade s prílohou III k tomuto nariadeniu.
46. Príloha IV sa mení v súlade s prílohou IV k tomuto nariadeniu.
47. Dopĺňa sa nová príloha V tak, ako je uvedená v prílohe V k tomuto nariadeniu.
48. K tomuto nariadeniu sa dopĺňa nová príloha VI.

Článok 2

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

*Za Európsky parlament
predseda*

*Za Radu
predseda*

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Nariadenie Európskeho parlamentu a Rady o rámci pre európsku digitálnu identitu, ktorým sa mení nariadenie eIDAS

1.2. Príslušné oblasti politiky

Oblasť politiky: Vnútrotrh
Európa pripravená na digitálny vek

1.3. Návrh/iniciatíva sa týka:

- ☐ novej akcie
- ☐ novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu²⁸
- ☒ predĺženia trvania existujúcej akcie
- ☐ zlúčenia jednej alebo viacerých akcií do ďalšej/novej akcie alebo presmerovania jednej alebo viacerých akcií na ďalšiu/novú akciu

1.4. Ciele

1.4.1. Všeobecné ciele

Všeobecným cieľom tejto iniciatívy je zabezpečiť riadne fungovanie vnútorného trhu, najmä v súvislosti s poskytovaním a používaním cezhraničných a medzisektorových verejných a súkromných služieb, ktoré sa spoliehajú na dostupnosť a používanie vysoko bezpečných a dôveryhodných riešení v oblasti elektronickej totožnosti. Tento cieľ vychádza zo strategických cieľov stanovených v oznámení „Formovanie digitálnej budúcnosti Európy“.

1.4.2. Špecifické ciele

Špecifický cieľ č. 1

Poskytovať prístup k dôveryhodným a bezpečným riešeniam v oblasti digitálnej identity, ktoré možno používať cezhranične a spĺňajú očakávania používateľov a požiadavky trhu.

Špecifický cieľ č. 2

Zabezpečiť, aby sa verejné a súkromné služby mohli spoliehať na overené a bezpečné cezhraničné riešenia v oblasti digitálnej identity.

Špecifický cieľ č. 3

Umožniť občanom úplnú kontrolu nad ich osobnými údajmi a zaistiť ich bezpečnosť pri používaní riešení v oblasti digitálnej identity.

Špecifický cieľ č. 4

Zabezpečiť rovnaké podmienky poskytovania kvalifikovaných dôveryhodných služieb v EÚ a ich akceptáciu.

²⁸

Podľa článku 58 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

1.4.3. Očakávané výsledky a vplyv

Uvedte, aký vplyv by mal mať návrh/iniciatíva na prijímateľov/cieľové skupiny.

Celkovo sa očakáva, že najväčšie výhody budú mať z tejto iniciatívy koncoví používatelia/občania, poskytovatelia online služieb, poskytovatelia mobilnej aplikácie peňaženka a verejní a súkromní poskytovatelia služieb digitálnej identity. Očakáva sa, že iniciatívou sa zabezpečí prístup k dôveryhodným a bezpečným riešeniam v oblasti digitálnej identity, ktoré možno používať cezhranične a spĺňajú očakávania používateľov a požiadavky trhu; zabezpečí, aby sa verejné a súkromné služby mohli spoliehať na dôveryhodné a bezpečné cezhraničné riešenia v oblasti digitálnej identity; umožní občanom úplnú kontrolu nad ich osobnými údajmi a zaistí ich bezpečnosť pri používaní riešení v oblasti digitálnej identity a zabezpečia sa rovnaké podmienky poskytovania kvalifikovaných dôveryhodných služieb v EÚ a ich akceptácia.

Okrem nástroja na prístup k verejným aj súkromným službám by priamou výhodou pre občanov a podniky bola jednoduchosť a ľahká použiteľnosť rozhrania na autentifikáciu peňaženky a možnosť realizovať transakcie vyžadujúce všetky úrovne zabezpečenia (napr. od prihlásenia sa na sociálne médiá po aplikácie elektronického zdravotníctva).

Posilnený prístup ochrany súkromia už v štádiu návrhu by mohol priniesť ďalšie výhody, pretože peňaženka by v procese osvedčovania atribútov nevyžadovala sprostredkovateľov, vďaka čomu by občania mohli komunikovať priamo s poskytovateľmi služieb a potvrdení. Zvýšenou bezpečnosťou osobných údajov peňaženky by sa predchádzalo krádeži totožnosti a tým finančnej strate pre európskych občanov a podniky.

Z hľadiska hospodárskeho rastu sa očakáva, že zavedením systému založeného na normách sa zníži neistota účastníkov trhu, a takisto sa očakáva, že to bude mať pozitívny vplyv na inovácie.

A čo je dôležitejšie, očakáva sa tým zabezpečenie inkluzívnejšieho prístupu k verejným a súkromným službám v súvislosti s verejnými statkami ako vzdelanie a zdravotníctvo, ku ktorým majú niektoré sociálne skupiny v súčasnosti prístup s určitými prekážkami. Napríklad niektorí občania so zdravotným postihnutím, často osoby so zníženou mobilitou alebo žijúce vo vidieckych oblastiach, majú menší prístup k službám, ktoré si obvykle vyžadujú fyzickú prítomnosť, ak nie sú dodávané lokálne.

1.4.4. Ukazovatele výkonnosti

Uvedte ukazovatele na monitorovanie pokroku a dosiahnutých výsledkov.

Aspekt monitorovania a hodnotenia a príslušné ciele	Ukazovateľ	Zodpovednosť za získavanie	Zdroj(e)
Uplatňovanie			

Poskytovať všetkým občanom EÚ prístup k prostriedkom elektronickej identifikácie	Počet európskych občanov a podnikov, ktorým boli vydané oznámené elektronické identifikácie/európske peňaženky digitálnej identity a počet vydaných potvrdení totožnosti (osvedčení atribútov)	Európska komisia a príslušné vnútroštátne orgány	Ročný prieskum/údaje z monitorovania a hodnotenia získané príslušnými vnútroštátnymi orgánmi
Poskytovať všetkým občanom EÚ prístup k prostriedkom elektronickej identifikácie	Počet európskych občanov a podnikov aktívne používajúcich oznámené elektronické identifikácie/európske peňaženky digitálnej identity a potvrdenia totožnosti (osvedčenia atribútov)	Európska komisia a príslušné vnútroštátne orgány	Ročný prieskum/údaje z monitorovania a hodnotenia získané príslušnými vnútroštátnymi orgánmi
Zvýšiť cezhraničné uznávanie a akceptáciu schém elektronickej identifikácie s ambíciou dosiahnuť všeobecnú akceptáciu	Počet poskytovateľov online služieb, ktorí akceptujú oznámené elektronické identifikácie/európske peňaženky digitálnej identity a potvrdenia totožnosti (osvedčenia atribútov)	Európska komisia	Ročný prieskum
Zvýšiť cezhraničné uznávanie a akceptáciu schém elektronickej identifikácie s ambíciou dosiahnuť všeobecnú akceptáciu	Počet online transakcií uskutočnených s použitím oznámených elektronických identifikácií/európskych peňaženiek digitálnej identity a potvrdení totožnosti (osvedčení atribútov) (spolu a cezhranične)	Európska komisia	Ročný prieskum
Podporovať zavádzanie nových služieb digitálnej identity zo strany súkromného sektora a ich vývoj	Počet nových súkromných služieb vydávania osvedčení atribútov, ktoré spĺňajú normy pre začlenenie do európskej peňaženky digitálnej identity	Európska komisia a príslušné vnútroštátne orgány	Ročný prieskum
Kontextové informácie			
Podporovať zavádzanie nových služieb digitálnej identity zo strany súkromného sektora a ich vývoj	Veľkosť trhu s digitálnou identitou	Európska komisia	Ročný prieskum

Podporovať zavádzanie nových služieb digitálnej identity zo strany súkromného sektora a ich vývoj	Výdavky na verejné obstarávanie v súvislosti s digitálnou identitou	Európska komisia a príslušné vnútroštátne orgány	Ročný prieskum
Zvýšiť cezhraničné uznávanie a akceptáciu schém elektronickej identifikácie s ambíciou dosiahnuť všeobecnú akceptáciu	% podnikov s tržbami z elektronického obchodu s tovarom alebo službami	Európska komisia	Eurostat
Zvýšiť cezhraničné uznávanie a akceptáciu schém elektronickej identifikácie s ambíciou dosiahnuť všeobecnú akceptáciu	Podiel online transakcií, pri ktorých sa vyžaduje silná elektronická identifikácia zákazníka (celkom)	Európska komisia	Ročný prieskum
Poskytovať všetkým občanom EÚ prístup k prostriedkom elektronickej identifikácie	% osôb vykonávajúcich elektronický obchod % osôb využívajúcich prístup k online verejným službám	Európska komisia	Eurostat

1.5. Dôvody návrhu/iniciatívy

1.5.1. Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch. Členské štáty budú povinné vydať európsku peňaženku digitálnej identity do 24 až 48 mesiacov (orientačne) od prijatia nariadenia. Komisia bude splnomocnená prijímať vykonávacie akty, ktorým stanoví technické špecifikácie a referenčné normy pre technickú architektúru rámca európskej digitálnej identity, do 12 až 24 mesiacov (orientačne) od prijatia nariadenia.

1.5.2. Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

Dôvody na akciu na európskej úrovni (*ex ante*)

Vzhľadom na rastúci dopyt občanov, podnikov a poskytovateľov online služieb po používateľsky ústretových a bezpečných riešeniach v oblasti digitálnej identity, ktoré zohľadňujú ochranu súkromia a možno ich používať cezhranične, môžu ďalšie opatrenia na úrovni EÚ priniesť vyššiu hodnotu než opatrenia na úrovni jednotlivých členských štátov, ako to vyplýva z hodnotenia nariadenia eIDAS.

Očakávaný prínos vytvorený Úniou (*ex post*)

Harmonizovanejším prístupom na úrovni EÚ založeným na významnom prechode od spoliehania sa výlučne na riešenia v oblasti digitálnej identity k poskytovaniu elektronických osvedčení atribútov by sa zabezpečilo, že občania a podniky by mali kdekoľvek v EÚ prístup k verejným a súkromným službám založeným na overených dokladoch totožnosti a atribútoch. Poskytovatelia online služieb by boli schopní akceptovať riešenia v oblasti digitálnej identity nezávisle od miesta, kde boli vydané, spoliehajú sa na spoločný európsky prístup k dôvere, bezpečnosti a operabilite. Pre používateľov aj poskytovateľov služieb môže byť výhodou aj rovnaká právna hodnota elektronických osvedčení atribútov v rámci celej EÚ, čo je osobitne dôležité, ak sú potrebné koordinované opatrenia, ako v prípade digitálnych zdravotných certifikátov. Dôveryhodné služby poskytujúce elektronické osvedčenia atribútov by mali prospech aj z dostupnosti európskeho trhu pre ich služby. Napríklad vynaložené náklady na zabezpečenie vysoko dôveryhodného a bezpečného prostredia na poskytovanie kvalifikovanej dôveryhodnej služby sa jednoduchšie kompenzujú na úrovni EÚ vďaka úsporám z rozsahu. Iba rámec EÚ môže zabezpečiť úplnú cezhraničnú prenosnosť právnych totožností a súvisiace elektronické osvedčenie atribútov, ktoré umožňuje dôverovať osvedčeniam totožnosti vykonaným inými členskými štátmi.

1.5.3. *Poznatky získané z podobných skúseností v minulosti*

Nariadenie eIDAS (nariadenie č. 910/2014) (eIDAS) je jediným cezhraničným rámcom pre dôveryhodnú elektronickú identifikáciu fyzických a právnických osôb a dôveryhodné služby. Hoci nariadenie eIDAS zohráva nespochybniteľnú úlohu na vnútornom trhu, od jeho prijatia sa veľa zmenilo. Nariadenie eIDAS prijaté v roku 2014 je založené na vnútroštátnych systémoch elektronickej identifikácie, ktoré vychádzajú z rozličných noriem a zameriavajú sa na relatívne malú časť potrieb občanov a podnikov v oblasti elektronickej identifikácie, a to na bezpečný cezhraničný prístup k verejným službám. Služby, na ktoré sa nariadenie zameriava, sa týkajú najmä 3 % obyvateľov EÚ s bydliskom v inom členskom štáte ako v členskom štáte, v ktorom sa narodili.

Odvtedy sa digitalizácia všetkých funkcií spoločnosti dramaticky zvýšila. V neposlednom rade aj pandémia ochorenia COVID-19 výrazne ovplyvnila rýchlosť digitalizácie. Z toho dôvodu rastie digitalizácia poskytovania verejných aj súkromných služieb. Občania a podniky očakávajú dosiahnutie vysokej bezpečnosti a jednoduchosti každej online činnosti, napríklad predkladanie daňových priznaní, zápis na zahraničnú univerzitu, otvorenie bankového účtu alebo podanie žiadosti o úver na diaľku, prenájom automobilu, založenie podniku v inom členskom štáte, overenie na účely internetových platieb, predloženie ponuky v rámci online výzvy na predkladanie ponúk a ďalšie.

V dôsledku toho sa radikálne zvýšil dopyt po prostriedkoch online identifikácie a autentifikácie, ako aj po prostriedkoch digitálnej výmeny informácií súvisiacich s našou totožnosťou, atribútmi alebo kvalifikáciou (totožnosť, adresy, vek, ale aj odborná kvalifikácia, vodičské preukazy a iné povolenia a platobné systémy), ktoré sú bezpečné a ponúkajú vysokú úroveň ochrany údajov.

To vyvolalo posun paradigmy smerom k vyspelým a jednoduchým riešeniam, ktoré sú schopné integrovať rôzne overiteľné údaje a certifikáty používateľa. Používatelia očakávajú prostredie, ktoré si určia sami a v ktorom môžu byť vedené a poskytované rôzne potvrdenia a atribúty, napríklad vaša vnútroštátna elektronická identifikácia, odborné certifikáty, lístky na verejnú dopravu alebo v niektorých prípadoch dokonca

digitálne lístky na koncert. Sú to tzv. peňaženky s nezávislou aplikáciou spravované prostredníctvom mobilného zariadenia používateľa, ktoré umožňujú bezpečný a jednoduchý prístup k rôznym službám, tak verejným, ako aj súkromným, pod úplnou kontrolou samotného používateľa.

1.5.4. *Zlučiteľnosť s viacročným finančným rámcom a možná synergie s inými vhodnými nástrojmi*

Iniciatívou sa podporuje úsilie o obnovu Európy tak, že občanom a podnikom sa poskytujú potrebné nástroje, napr. jednoduchá elektronická identifikácia a dôveryhodné služby, s cieľom pomôcť im vykonávať ich každodenné online činnosti dôveryhodným a bezpečným spôsobom. Je preto plne v súlade s cieľmi VFR.

Prevádzkové výdavky majú byť financované v rámci špecifického cieľa č. 5 programu Digitálna Európa. Verejné zákazky na podporu rozvoja noriem a technických špecifikácií, ako aj náklady na údržbu základných prvkov elektronickej identifikácie a dôveryhodných služieb sa odhadujú do výšky 3 – 4 mil. EUR ročne. O presnom rozdelení týchto rozpočtových potrieb sa rozhodne pri vymedzovaní budúcich pracovných programov. Dosiahnutie cieľov návrhu by vo veľkej miere podporili granty na podporu napojenia verejných a súkromných služieb na ekosystém elektronickej identifikácie. Náklady poskytovateľa služieb na integráciu potrebného API peňaženky s elektronickou identitou sa odhadujú približne na 25,000 EUR ako jednorazové náklady jedného poskytovateľa. Napojenie kritického množstva služieb by podporil rozpočet na granty do výšky 0,5 mil. EUR na každý členský štát, ak bude k dispozícii po prerokovaní rozdelenia rozpočtu na ďalší pracovný program.

Zasadnutia expertnej skupiny v súvislosti s vypracovaním vykonávacích aktov budú hradené z administratívnej časti programu Digitálna Európa v celkovej výške 0,5 mil. EUR.

Synergie s inými právnymi nástrojmi

Táto iniciatíva poskytne rámec na poskytovanie elektronickej totožnosti a služieb elektronickej identifikácie v EÚ, na ktoré sa konkrétne sektory môžu spoliehať pri plnení právnych požiadaviek špecifických pre daný sektor, napríklad v súvislosti s digitálnymi cestovnými dokladmi, digitálnymi vodičskými preukazmi atď. Rovnako je návrh zosúladený s cieľmi nariadenia 2019/1157, ktorým sa posilňuje bezpečnosť preukazov totožnosti a dokladov o pobyte. V súlade s týmto nariadením sú členské štáty povinné do augusta 2021 zaviesť nové preukazy totožnosti s modernými ochrannými prvkami. Po ich vytvorení by členské štáty mohli modernizovať nové doklady totožnosti, aby mohli byť oznámené ako schémy elektronickej identifikácie v zmysle nariadenia eIDAS.

Iniciatíva prispeje aj k transformácii v colnej oblasti na „bezpapierové“ elektronické prostredie v kontexte iniciatívy na vytvorenie prostredia centrálného elektronického priečinka EÚ pre colníctvo. Treba takisto poznamenať, že budúcim návrhom sa prispeje k európskym politikám mobility uľahčením právnych požiadaviek na prevádzkovateľov námornej dopravy týkajúcich sa ohlasovania stanovených v kontexte európskeho prostredia jednotnej námornej platformy, ktoré sa začne uplatňovať od 15. augusta 2025. To isté platí o formulovaní nariadenia o elektronických údajoch o nákladnej doprave, ktoré zaväzuje orgány členských štátov akceptovať elektronické informácie o nákladnej doprave. Aplikácia európska

peňaženka digitálnej identity bude schopná spracúvať potvrdenia, ktoré sa týkajú vodičov, vozidiel a činností, požadovaných právnym rámcom EÚ v oblasti cestnej dopravy (napr. digitálne vodičské preukazy/smernica 2006/126/ES). Špecifikácie sa ďalej rozpracujú v kontexte tohto rámca. Budúca iniciatíva by mohla prispieť aj k formovaniu budúcich iniciatív v oblasti koordinácie sociálneho zabezpečenia, napríklad k možnému vývoju európskeho preukazu sociálneho zabezpečenia, ktorý by mohol stavať na zárukách dôvery ponúkaných oznámenými identifikáciami podľa nariadenia eIDAS.

Touto iniciatívou sa podporuje vykonávanie všeobecného nariadenia o ochrane údajov (nariadenie 2016/679), pretože dáva používateľovi právo kontrolovať, ako sa osobné údaje používajú. Zabezpečuje sa ňou vysoká úroveň komplementárnosti s novým aktom o kybernetickej bezpečnosti a jeho spoločnými schémami certifikácie kybernetickej bezpečnosti. Aj potreba jedinečnej totožnosti v rámci internetu vecí vyplývajúca z nariadenia eIDAS zabezpečuje konzistentnosť s aktom o kybernetickej bezpečnosti a potrebu pokryť okrem osôb a spoločností širšiu škálu aktérov, napríklad stroje, predmety, dodávateľov a zariadenia internetu vecí.

Nariadenie o jednotnej digitálnej bráne má takisto významné styčné body s touto iniciatívou a je v súlade s ňou. Cieľom nariadenia o jednotnej digitálnej bráne je plne modernizovať služby verejnej správy a uľahčiť online prístup k informáciám, administratívnym postupom a asistenčným službám, ktoré občania a podniky potrebujú, ak bývajú alebo pôsobia v inej krajine EÚ. Táto iniciatíva poskytuje základné prvky na podporu cieľa zaviesť do praxe v rámci jednotnej digitálnej brány zásadu „jedenkrát a dost“.

Okrem toho existuje súlad s Európskou dátovou stratégiou a navrhovaným nariadením o európskej správe údajov, pričom sa poskytuje rámec na podporu aplikácií založených na údajoch v prípadoch, keď sa vyžaduje prenos osobných údajov o totožnosti, a umožňuje sa používateľom mať nad nimi kontrolu, ako aj ich úplnú anonymizáciu.

1.5.5. *Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia*

Iniciatíva bude stavať na základných prvkoch elektronickej identifikácie a dôveryhodných služieb, ktoré boli vytvorené v rámci programu Nástroj na prepájanie Európy a sú integrované do programu Digitálna Európa.

Členské štáty môžu okrem toho požiadať o financovanie vytvorenia/zlepšenia potrebnej infraštruktúry z Mechanizmu na podporu obnovy a odolnosti.

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

☐ obmedzené trvanie

☐ v platnosti od [DD/MM]RRRR do [DD/MM]RRRR

☐ Finančný vplyv na viazané rozpočtové prostriedky od RRRR do RRRR a na platobné rozpočtové prostriedky od RRRR do RRRR.

☒ neobmedzené trvanie

Počiatočná fáza vykonávania bude trvať od RRRR do RRRR,

a potom bude vykonávanie pokračovať v plnom rozsahu.

1.7. Plánovaný spôsob riadenia²⁹

☒ Priame riadenie na úrovni Komisie

☒ prostredníctvom jej útvarov vrátane zamestnancov v delegáciách Únie

☐ prostredníctvom výkonných agentúr

☐ Zdieľané riadenie s členskými štátmi

☐ Nepriame riadenie, pri ktorom sa plnením rozpočtu poveria:

☐ tretie krajiny alebo subjekty, ktoré tieto krajiny určili,

☐ medzinárodné organizácie a ich agentúry (uved'te),

☐ Európska investičná banka (EIB) a Európsky investičný fond,

☐ subjekty uvedené v článkoch 70 a 71 nariadenia o rozpočtových pravidlách,

☐ verejnoprávne subjekty,

☐ súkromnoprávne subjekty poverené vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,

☐ súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú dostatočné finančné záruky,

☐ osoby poverené vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte.

V prípade viacerých spôsobov riadenia uved'te v oddiele „Poznámky“ presnejšie vysvetlenie.

Poznámky

[...]

[...]

²⁹ Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovom sídle BudgWeb:
<https://myintracom.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

Uveďte frekvenciu a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Nariadenie bude po prvýkrát preskúmané po dvoch rokoch po jeho úplnom uplatnení a potom každé štyri roky. Komisia musí predložiť zistenia Európskemu parlamentu a Rade.

Okrem toho v rámci uplatňovania opatrení členské štáty zbierajú štatistiku týkajúcu sa používania a fungovania európskej peňaženky digitálnej identity a kvalifikovaných dôveryhodných služieb. Štatistika sa zahrnie do správy, ktorá sa každoročne predkladá Komisii.

2.2. Systémy riadenia a kontroly

2.2.1. *Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly*

Nariadením sa stanovujú harmonizovanejšie pravidlá pre poskytovanie elektronickej identifikácie a dôveryhodných služieb na vnútornom trhu pri zaistení rešpektovania dôvery a kontroly používateľa nad svojimi vlastnými údajmi. V týchto nových pravidlách sa vyžaduje vypracovanie technických špecifikácií a noriem, ako aj koordinovanie činností vnútroštátnych orgánov a dohl'ad nad nimi. Navyše súvisiace základné prvky elektronickej identifikácie, elektronického podpisovania atď. budú spravované a poskytované v rámci programu Digitálna Európa. Treba zohľadniť aj zdroje potrebné na komunikáciu a rokovanie s tretími stranami o zmluve o vzájomnom uznávaní dôveryhodných služieb.

Na tieto úlohy je potrebné vybaviť útvary Komisie primeranými zdrojmi. Odhaduje sa, že presadzovanie nového nariadenia si vyžiada 11 ekvivalentov plného pracovného času; 4 – 5 ekvivalentov plného pracovného času na právne činnosti, 4 – 5 ekvivalentov plného pracovného času na zameranie sa na technické práce a 2 ekvivalenty plného pracovného času na koordináciu, medzinárodnú osvetovú činnosť a administratívnu podporu.

2.2.2. *Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie*

Jedným z hlavných problémov, ktoré vedú k nedostatkom súčasného legislatívneho rámca, je nedostatočná harmonizácia vnútroštátnych systémov. Aby sa tento problém vyriešil v rámci súčasnej iniciatívy, bude sa vo veľkej miere vychádzať z referenčných noriem a technických špecifikácií, ktoré sa vymedzia vo vykonávacích aktoch.

Komisiu bude pri vypracúvaní týchto vykonávacích aktov podporovať expertná skupina. Komisia okrem toho už spolupracuje s členskými štátmi na dohode o technickej povahe budúceho systému, aby sa predišlo ďalšej fragmentácii počas rokovaní o návrhu.

2.2.3. *Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)*

Pokiaľ ide o výdavky na zasadnutia expertnej skupiny, vzhľadom na nízku hodnotu na jednu transakciu (napr. preplatenie cestovných nákladov delegátovi za jedno zasadnutie, ak ide o fyzické zasadnutie) sa štandardné postupy vnútornej kontroly zdajú byť dostatočné.

Bežné štandardné postupy GR CNECT by mali byť dostatočné aj pre skúšobné projekty, ktoré sa majú vykonávať v rámci programu Digitálna Európa.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uvedte existujúce a plánované preventívne a ochranné opatrenia, napr. zo stratégie boja proti podvodom.

Existujúce opatrenia boja proti podvodom uplatniteľné na Komisiu sa budú vzťahovať na dodatočné rozpočtové prostriedky potrebné pre toto nariadenie.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

Existujúce rozpočtové riadky

V poradi, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo		krajín EZVO ³¹	kandidátskych krajín ³²	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
2	02 04 05 01 Zavedenie	DRP/	ÁNO	NIE	/NIE	NIE
2	02 01 30 01 Výdavky na podporu programu Digitálna Európa	ND				
7	20 02 06 Administratívne výdavky	ND	NIE			

Požadované nové rozpočtové riadky

V poradi, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo		krajín EZVO	kandidátskych krajín	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
	[XX.YY.YY.YY]		ÁNO/NIE	ÁNO/NIE	ÁNO/NIE	ÁNO/NIE

³⁰ DRP = diferencované rozpočtové prostriedky / NRP = nediferencované rozpočtové prostriedky.

³¹ EZVO: Európske združenie voľného obchodu.

³² Kandidátske krajiny a prípadne potenciálni kandidáti zo západného Balkánu.

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky

- ☐ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov.
- ☒ Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca	Číslo	2
---	--------------	---

GR: CNECT			Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027		SPOLU
○ Operačné rozpočtové prostriedky			O rozdelení rozpočtu sa rozhodne počas tvorby pracovných programov. Uvedené hodnoty predstavujú minimálnu hodnotu potrebnú na údržbu a modernizáciu ³³ .							
Rozpočtový riadok 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
Rozpočtový riadok	Závazky	(1b)								
	Platby	(2b)								
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov ³⁵										
Rozpočtový riadok 02 01 03 01		(3)	0,048	0,144	0,144	0,072	0,072	0,072		0,552
Rozpočtové prostriedky pre GR CNECT SPOLU	Závazky	= 1a + 1b + 3	2,048	4,144	4,144	4,072	4,072	4,072		22,552
	Platby	= 2a + 2b	1,048	3,144	4,144	4,072	4,072	4,072	2,000	22,552

³³ Ak skutočné náklady presiahnu uvedené sumy, náklady budú financované z rozpočtového riadka 02 04 05 01.

³⁴ Podľa oficiálnej rozpočtovej nomenklatúry.

³⁵ Technická a/alebo administratívna pomoc a výdavky určené na financovanie vykonávania programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

		+3								
--	--	----	--	--	--	--	--	--	--	--

○ Operačné rozpočtové prostriedky SPOLU	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
○ Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU		(6)	0,048	0,144	0,144	0,072	0,072	0,072		0,552
Rozpočtové prostriedky OKRUHU 2 viacročného finančného rámca SPOLU	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 viacročného finančného rámca	7	„Administratívne výdavky“
---	----------	---------------------------

Tento oddiel treba vyplniť s použitím rozpočtových údajov administratívnej povahy, ktoré sa najprv uvedú v [prílohe k legislatívnemu finančnému výkazu](#) (príloha V k interným pravidlám), ktorá sa na účely medziútarovej konzultácie nahrá do aplikácie DECIDE.

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	SPOLU
GR: CNECT								
○ Ľudské zdroje		0,776	1,470	1,470	1,470	1,470	1,318	7,974
○ Ostatné administratívne výdavky		0,006	0,087	0,087	0,087	0,016	0,016	0,299
GR CNECT SPOLU	Rozpočtové prostriedky	0,782	1,557	1,557	1,557	1,486	1,334	8,273

Rozpočtové prostriedky OKRUHU 7 viacročného finančného rámca SPOLU	(Závazky spolu = Platby spolu)	0,782	1,557	1,557	1,557	1,486	1,334	8,273
---	-----------------------------------	-------	-------	-------	-------	-------	-------	-------

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027		SPOLU
Rozpočtové prostriedky OKRUHOV 1 až 7 viacročného finančného rámca SPOLU	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. Odhadované výsledky financované z operačných rozpočtových prostriedkov

viazané rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Uved'te ciele a výstupy			Rok 2022		Rok 2023		Rok 2024		Rok 2025		Rok 2026		Rok 2027		SPOLU	
	⇓	Druh ³⁶	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu
ŠPECIFICKÝ CIEĽ č. 1 ³⁷ ...			Poskytovať prístup k dôveryhodným a bezpečným riešeniam v oblasti digitálnej identity, ktoré možno používať cezhranične a spĺňajú očakávania používateľov a požiadavky trhu													
Ročné prieskumy/štúdie			1	0,050	1	0,050	1	0,050,05	1	0,050	1	0,050	1	0,050	6	0,300
Špecifický cieľ č. 1 medzisúčet			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
ŠPECIFICKÝ CIEĽ č. 2...			Zabezpečiť, aby sa verejné a súkromné služby mohli spoliehať na dôveryhodné a bezpečné cezhraničné riešenia v oblasti digitálnej identity;													
Prieskumy/štúdie			1	0,050	1	0,050	1	0,050,05	1	0,050	1	0,050	1	0,050	6	0,300
Špecifický cieľ č. 2 medzisúčet			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
ŠPECIFICKÝ CIEĽ č. 3...			Umožniť občanom úplnú kontrolu nad ich osobnými údajmi a zaistiť ich bezpečnosť pri používaní riešení v oblasti digitálnej identity;													
Prieskumy/štúdie			1	0,050	1	0,050	1	0,050,05	1	0,050	1	0,050	1	0,050	6	0,300
Špecifický cieľ č. 3 medzisúčet			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
ŠPECIFICKÝ CIEĽ č. 4...			Zabezpečiť rovnaké podmienky poskytovania kvalifikovaných dôveryhodných služieb v EÚ a ich akceptáciu.													
Prieskumy/štúdie			1	0,050	1	0,050	1	0,050,05	1	0,050	1	0,050	1	0,050	6	0,300

³⁶ Výstupy znamenajú dodané produkty a služby (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

³⁷ Ako je uvedené v bode 1.4.2. „Špecifické ciele...“.

Špecifický cieľ č. 4 medzisúčtet	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
SPOLU	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	24	1,200

3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov.

☒ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

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

OKRUH 7 viacročného finančného rámca							
Ludské zdroje	0,776	1,470	1,470	1,470	1,470	1,318	7,974
Ostatné administratívne výdavky	0,006	0,087	0,087	0,087	0,0162	0,0162	0,299
Medzisúčet OKRUHU 7 viacročného finančného rámca	0,782	1,557	1,557	1,557	1,486	1,334	8,273

Mimo OKRUHU 7³⁸ viacročného finančného rámca							
Ludské zdroje							
Ostatné administratívne výdavky							
Zahrnúť administratívne výdavky do programu Digitálna Európa	0,048	0,144	0,144	0,072	0,072	0,072	0 552
Medzisúčet mimo OKRUHU 7 viacročného finančného rámca	0,048	0,144	0,144	0,072	0,072	0,072	0 552

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

Rozpočtové prostriedky potrebné na ľudské zdroje a na ostatné administratívne výdavky budú pokryté rozpočtovými prostriedkami GR, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu pridelovania zdrojov a v závislosti od rozpočtových obmedzení.

³⁸ Technická a/alebo administratívna pomoc a výdavky určené na financovanie vykonávania programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

3.2.4. Odhadované potreby ľudských zdrojov

- ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.
- ☒ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

odhady sa vyjadrujú v jednotkách ekvivalentu plného pracovného času

	Rok 2022	Rok 20 23	Rok 20 24	Rok 20 25	Rok 20 26	Rok 2027
20 01 02 01 (ústredie a zastúpenia Komisie)	4	8	8	8	8	7
20 01 02 03 (delegácie)						
01 01 01 01 (nepriamy výskum)						
01 01 01 11 (priamy výskum)						
Iné rozpočtové riadky (uved'te)						
20 02 01 (ZZ, VNE, DAZ z celkového finančného krytia)	2	3	3	3	3	3
20 02 03 (ZZ, MZ, VNE, DAZ, PED v delegáciách)						
XX 01 xx yy zz ³⁹	– ústredie					
	– delegácie					
01 01 01 02 (ZZ, VNE, DAZ – nepriamy výskum)						
01 01 01 12 (ZZ, VNE, DAZ – priamy výskum)						
Iné rozpočtové riadky (uved'te)						
SPOLU	6	11	11	11	11	10

XX predstavuje príslušnú oblasť politiky alebo rozpočtovú hlavu.

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu pridelit' riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	Úradníci budú vykonávať najmä právnické činnosti, koordinačné činnosti a rokovania s tretími krajinami a orgánmi v súvislosti so vzájomným uznávaním dôveryhodných služieb.
Externí zamestnanci	Národní experti by mali pomôcť s technickým a funkčným nastavením systému. ZZ by takisto mali poskytovať podporu v oblasti technických úloh vrátane spravovania základných prvkov.

³⁹ Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

3.2.5. Súlad s platným viacročným finančným rámcom

Návrh/iniciatíva:

- ☒ môže byť v plnej miere financovaná prerozdelením v rámci príslušného okruhu viacročného finančného rámca (VFR).

Vysvetlite požadovanú zmenu v plánovaní a uveďte príslušné rozpočtové riadky a zodpovedajúce sumy. V prípade väčšieho preprogramovania poskytnite tabuľku vo formáte Excel.

- ☐ si vyžaduje použitie nepridelenej rezervy v rámci príslušného okruhu VFR a/alebo použitie osobitných nástrojov vymedzených v nariadení o VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky, zodpovedajúce sumy a nástroje, ktorých použitie sa navrhuje.

- ☐ si vyžaduje revíziu VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky a zodpovedajúce sumy.

3.2.6. Príspevky od tretích strán

Návrh/iniciatíva:

- ☒ nezahŕňa spolufinancovanie tretími stranami
- ☐ zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok N ⁴⁰	Rok N+1	Rok N+2	Rok N+3	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			Spolu
Uveďte spolufinancujúci subjekt								
Prostriedky zo spolufinancovania SPOLU								

⁴⁰

Rok N je rok, v ktorom sa návrh/iniciatíva začína uskutočňovať. Nahraďte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

3.3. Odhadovaný vplyv na príjmy

- ☒ Návrh/iniciatíva nemá finančný vplyv na príjmy.
- ☐ Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:

☐ vplyv na vlastné zdroje,

☐ vplyv na iné príjmy,

Uved'te, či sú príjmy pripísané rozpočtovým riadkom výdavkov ☐

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový riadok príjmov:	Rozpočtové prostriedky k dispozícii v bežnom rozpočtovom roku	Vplyv návrhu/iniciatívy ⁴¹					
		Rok N	Rok N+1	Rok N+2	Rok N+3	Uved'te všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)	
Článok							

V prípade pripísaných príjmov uved'te príslušné rozpočtové riadky výdavkov.

[...]

Ďalšie poznámky (napr. spôsob/vzorec použitý na výpočet vplyvu na príjmy alebo akékoľvek ďalšie informácie).

[...]

⁴¹ Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. h rubé sumy po odčítaní 20 % na náklady na výber.

PRÍLOHA
k LEGISLATÍVNEMU FINANČNÉMU VÝKAZU

Názov návrhu/iniciatívy:

Návrh nariadenia o rámci pre európsku digitálnu identitu, ktorým sa mení nariadenie eIDAS

- 1. POTREBNÉ ĽUDSKÉ ZDROJE A NEVYHNUTNÉ NÁKLADY NA TIETO ZDROJE**
- 2. NÁKLADY NA OSTATNÉ ADMINISTRATÍVNE VÝDAVKY**
- 3. CELKOVÉ ADMINISTRATÍVNE NÁKLADY**
- 4. METÓDY VÝPOČTU POUŽITÉ NA ODHAD NÁKLADOV**
 - 4.1. Ľudské zdroje**
 - 4.2. Ostatné administratívne výdavky**

Táto príloha musí byť priložená k legislatívnemu finančnému výkazu počas konzultácie útvarov.

Tabuľky s údajmi sú použité ako zdroj tabuliek nachádzajúcich sa v legislatívnom finančnom výkaze. Slúžia výlučne na vnútorné použitie v rámci Komisie.

(1) Náklady na ľudské zdroje považované za nevyhnutné

☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.

☒ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

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. Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu pridelovania zdrojov v závislosti od rozpočtových obmedzení.

4.4.

4.5.

Mimo OKRUHU 7 viacročného finančného rámca		Rok 2022		Rok 2023		Rok 2024		Rok 2025		Rok 2026		Rok 2027		SPOLU	
		FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky
01 01 01 01 nepriamy výskum ⁴² 01 01 01 11 priamy výskum Iné (uveďte)	AD														
	AST														
Externí zamestnanci financovaní z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“)	– ústredie	ZZ													
		VNE													
		DAZ													
	– delegácie Únie	ZZ													
		MZ													
		VNE													
		DAZ													
		PED													
01 01 01 02 nepriamy výskum 01 01 01 12 priamy výskum Iné (uveďte) ⁴³	ZZ														
	VNE														
	DAZ														
Iné rozpočtové riadky týkajúce sa LZ (uveďte)															

⁴² Vyberte príslušný rozpočtový riadok alebo v prípade potreby uveďte ďalší. Ak sa to týka viacerých rozpočtových riadkov, zamestnanci by mali byť rozlíšení podľa každého príslušného rozpočtového riadka.

⁴³ Vyberte príslušný rozpočtový riadok alebo v prípade potreby uveďte ďalší. Ak sa to týka viacerých rozpočtových riadkov, zamestnanci by mali byť rozlíšení podľa každého príslušného rozpočtového riadka.

Medzisúčtet LZ – mimo OKRUHU 7															
Spolu LZ (všetky okruhy VFR)		6	0,776	11	1,470	11	1,470	11	1,470	11	1,470	10	1,318	60	7,974

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu pridelovania zdrojov v závislosti od rozpočtových obmedzení.

4.6. **Náklady na ostatné administratívne výdavky**

4.7. ☐ **Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov.**

4.8. ☒ **Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:**

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

OKRUH 7 viacročného finančného rámca	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Spolu
Na ústredí alebo na území EÚ:							
20 02 06 01 – Výdavky na služobné cesty a reprezentáciu	0 006	0 015	0 015	0 015	0 015	0 015	0,081
20 02 06 02 – Náklady na konferencie a zasadnutia							
20 02 06 03 – Výbory ⁴⁴		0,072	0,072	0,072	0,0012	0,012	0,218
20 02 06 04 Štúdie a konzultácie							
20 04 – Výdavky na IT (firemné) ⁴⁵							
Iné rozpočtové riadky netýkajúce sa LŽ (ak je to potrebné, uveďte)							
Delegácie Únie:							
20 02 07 01 – Náklady na služobné cesty, konferencie a reprezentáciu							
20 02 07 02 – Ďalšie odborné vzdelávanie zamestnancov							
20 03 05 – Infraštruktúra a logistika							
Iné rozpočtové riadky netýkajúce sa LŽ (ak je to potrebné, uveďte)							
Medzisúččet ostatné – OKRUH 7 viacročného finančného rámca	0,006	0,087	0,087	0,087	0,016	0,016	0,299

⁴⁴ Uveďte typ výboru a skupinu, do ktorej patrí.

⁴⁵ Stanovisko GR DIGIT – vyžaduje sa tým pre investície do IT [pozri usmernenia k financovaniu IT, C(2020) 6126 final z 10.9.2020, s. 7].

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Mimo OKRUHU 7 viacročného finančného rámca	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Spolu
Výdavky na technickú a administratívnu pomoc (okrem externých zamestnancov) z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“)	0,048	0,144	0,144	0,072	0,072	0,072	0,552
– ústredie							
– delegácie Únie							
Ostatné výdavky na riadenie v oblasti výskumu							
Výdavky na operačné programy v oblasti politiky IT ⁴⁶							
Výdavky na operačné programy v oblasti firemných IT ⁴⁷							
Iné rozpočtové riadky netýkajúce sa LZ (ak je to potrebné, uveďte)							
Medzisúčet ostatné – mimo OKRUHU 7 viacročného finančného rámca	0,048	0,144	0,144	0,072	0,072	0,072	0,552
Ostatné administratívne výdaje spolu (všetky okruhy VFR)	0,054	0,231	0,231	0,159	0,088	0,088	0,851

⁴⁶ Stanovisko GR DIGIT – vyžaduje sa tím pre investície do IT [pozri usmernenia k financovaniu IT, C(2020)6126 final z 10.9.2020, s. 7].

⁴⁷ Táto položka zahŕňa miestne administratívne systémy a príspevky na spolufinancovanie firemných IT systémov [pozri usmernenia k financovaniu IT, C(2020)6126 final z 10.9.2020].

5. CELKOVÉ ADMINISTRATÍVNE NÁKLADY (VŠETKY OKRUHY VFR)

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Zhrnutie	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Spolu
Okruh 7 – Ľudské zdroje	0,776	1,470	1,470	1,470	1,470	1,318	7,974
Okruh 7 – Ostatné administratívne výdavky	0,006	0,087	0,087	0,087	0,016	0,016	0,218
Medzisúččet okruhu 7							
Mimo okruhu 7 – Ľudské zdroje							
Mimo okruhu 7 – Ostatné administratívne výdavky	0,048	0,144	0,144	0,072	0,072	0,072	0,552
Medzisúččet iné okruhy							
1. SPOLU							
2. OKRUH 7 a mimo OKRUHU 7	0,830	1,701	1,701	1,629	1,558	1,406	8,825

- (1) Požadované administratívne rozpočtové prostriedky budú pokryté rozpočtovými prostriedkami, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené, a v prípade potreby budú doplnené rozpočtovými prostriedkami, ktoré sa môžu pridelit' riadiacemu GR v rámci ročného postupu pridel'ovania zdrojov v závislosti od rozpočtových obmedzení.

6. METÓDY VÝPOČTU POUŽITÉ NA ODHAD NÁKLADOV

a) Ľudské zdroje

V tejto časti sa stanovuje metóda výpočtu použitá na odhad ľudských zdrojov považovaných za potrebné [predpokladané pracovné zaťaženie vrátane konkrétnych pracovných miest (pracovné profily Sysper 2), kategórií zamestnancov a zodpovedajúcich priemerných nákladov].

1.	OKRUH 7 viacročného finančného rámca
2.	<u>Pozn.: Priemerné náklady na každú kategóriu zamestnancov v ústrediach sú k dispozícii na webovom sídle BudgWeb:</u>
3.	<u>https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx.</u>
4.	☐ Úradníci a dočasní zamestnanci
5.	<u>7 úradníkov AD (vrátane 1 z CNECT/F.3 v rokoch 2023 – 2024) x 152 000 EUR ročne v rokoch 2023 až 2027 (polovica z tejto sumy v roku 2022 z dôvodu očakávaného prijatia v polovici roka 2022);</u>
6.	<u>1 úradník AST x 152 000 EUR ročne v rokoch 2023 až 2027 (polovica z tejto sumy v roku 2022 z dôvodu očakávaného prijatia v polovici roka 2022).</u>
7.	
8.	☐ Externí zamestnanci
9.	<u>ZZ: 1 x 82 000 EUR ročne v rokoch 2023 až 2027 (polovica z tejto sumy v roku 2022 z dôvodu očakávaného prijatia v polovici roka 2022) (použitý faktor indexácie);</u>
10.	<u>2 VNE x 86 000 EUR ročne v rokoch 2023 až 2027 (polovica z tejto sumy v roku 2022 z dôvodu očakávaného prijatia v polovici roka 2022) (použitý faktor indexácie).</u>
11.	

12.	Mimo OKRUHU 7 viacročného finančného rámca
13.	☐ Len miesta financované z rozpočtu na výskum
14.	
15.	☐ Externí zamestnanci
16.	

7. OSTATNÉ ADMINISTRATÍVNE VÝDAVKY

Uveďte podrobnosti o metóde výpočtu použitej pri každom rozpočtovom riadku, a najmä východiskové predpoklady (napr. počet zasadnutí za rok, priemerné náklady atď.)

17.	OKRUH 7 viacročného finančného rámca
18.	<u>Zasadnutia výboru každé dva mesiace x 12 000 EUR na jedno zasadnutie v rokoch 2022 až 2024 na účely prijatia vykonávacích aktov. Potom každoročné zasadnutia výboru na účely prijatia aktualizovaných vykonávacích aktov.</u>
19.	<u>Služobné cesty sú najmä cesty medzi Luxemburskom a Bruselom, ale aj účasť na konferenciách, stretnutia s členskými štátmi a inými zainteresovanými stranami.</u>
20.	

21.	Mimo OKRUHU 7 viacročného finančného rámca
22.	<u>Zasadnutia expertnej skupiny budú hradené z administratívneho riadka programu Digitálna Európa.</u>
23.	<u>Očakáva sa, že zasadnutia sa budú uskutočňovať každý mesiac (12 000 EUR na jedno zasadnutie) počas prípravy vykonávacieho aktu (od polovice roka 2022 do roka 2024) a mimo uvedeného obdobia by sa zasadnutiami plánovanými každé dva mesiace mala zabezpečiť koordinácia vrámci celej EÚ v súvislosti s technickou realizáciou.</u>
24.	

