Rada
Európskej únie

V Bruseli 6. decembra 2022
(OR. en)

15706/22

Medziinštitucionálny spis:
2021/0136(COD)

TELECOM 519
COMPET 1006
MI 919
DATAPROTECT 352
JAI 1634
CODEC 1941

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	6. decembra 2022
Komu:	Delegácie
Č. predch. dok.:	14959/22 + ADD 1 + ADD 2
Č. dok. Kom.:	9471/21
Predmet:	Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o stanovenie rámca pre európsku digitálnu identitu – všeobecné smerovanie (6. decembra 2022)

Delegáciám v prílohe zasielame všeobecné smerovanie Rady k uvedenému návrhu, ktoré Rada (doprava, telekomunikácie a energetika) schválila na svojom 3 917. zasadnutí 6. decembra 2022.

Všeobecným smerovaním sa stanovuje predbežná pozícia Rady k tomuto návrhu a vytvára sa základ pre prípravu rokovaní s Európskym parlamentom.

PRÍLOHA

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 výboru[1],

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) V oznámení Komisie z 19. februára 2020 s názvom Formovanie digitálnej budúcnosti Európy[2] 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.

[1] Ú. v. EÚ C …, …, s. ….
[2] COM/2020/67 final.

(2) Európska rada vo svojich záveroch z 1. – 2. októbra 2020[3] vyzvala Komisiu, aby navrhla vytvorenie únijného 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 spôsob z 9. marca 2021[4] sa stanovuje cieľ v podobe únijného 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 posilní jednotný trh tým, že umožní občanom, ďalším obyvateľom vymedzeným podľa vnútroštátnych právnych predpisov a podnikom, aby sa pohodlným a jednotným spôsobom identifikovali online v celej Únii. Európska peňaženka digitálnej identity poskytne fyzickým a právnickým osobám v celej Únii harmonizovaný prostriedok elektronickej identifikácie, ktorý im umožní vykonávať autentifikáciu a zdieľať údaje súvisiace s ich totožnosťou. 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 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.

---

[3] https://www.consilium.europa.eu/sk/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/.

[4] COM/2021/118 final/2.

(4a) Niekoľko členských štátov zaviedlo a vo veľkej miere využíva prostriedky elektronickej identifikácie, ktoré poskytovatelia služieb v Únii v súčasnosti akceptujú. Okrem toho sa na základe súčasného nariadení eIDAS uskutočnili investície do vnútroštátnych aj cezhraničných riešení vrátane technickej infraštruktúry interoperability uzlov eIDAS. S cieľom zaručiť komplementárnosť a rýchle prijatie európskych peňaženiek digitálnej identity súčasnými používateľmi oznámených prostriedkov elektronickej identifikácie a minimalizovať vplyv na existujúcich poskytovateľov služieb sa očakáva, že európske peňaženky digitálnej identity budú ťažiť zo skúseností s existujúcimi prostriedkami elektronickej identifikácie a z využívania zavedenej infraštruktúry eIDAS na európskej a vnútroštátnej úrovni.

(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 poskytnuté, 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) 2016/679[5]. 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. Osobné údaje týkajúce sa poskytovania európskych peňaženiek digitálnej identity by sa mali uchovávať logicky oddelene od všetkých ostatných údajov uchovávaných vydavateľom. Toto nariadenie vydavateľom európskych peňaženiek digitálnej identity nebráni v tom, aby uplatňovali dodatočné technické opatrenia prispievajúce k ochrane osobných údajov, ako je fyzické oddelenie osobných údajov týkajúcich sa poskytovania peňaženiek od všetkých ostatných údajov uchovávaných vydavateľom.

---

[5] 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).

(7) Je potrebné stanoviť harmonizované podmienky na vytvorenie rámca pre európske peňaženky digitálnej identity, ktoré by mali poskytovať 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, súkromia, 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, aby sa spoliehajúce sa strany mohli na používanie európskych peňaženiek digitálnej identity spoľahnúť, a s cieľom chrániť používateľa pred nezákonným používaním citlivých údajov by sa spoliehajúce sa strany mali zaregistrovať v rámci procesu oznamovania. Požiadavky na oznamovanie, ktoré sa uplatňujú na spoliehajúce sa strany, by vo väčšine prípadov mali byť založené na poskytovaní obmedzeného množstva informácií potrebných na autentifikáciu spoliehajúcej sa strany v rámci európskej peňaženky digitálnej identity. Požiadavky by mali umožniť aj používanie automatizovaných alebo jednoduchých postupov podávania správ vrátane spoliehania sa na existujúce registre členských štátov a na ich využívanie. V prípade kategórií citlivých údajov môžu zároveň na vnútroštátnej úrovni alebo na úrovni Únie existovať osobitné režimy, ktoré môžu ukladať spoliehajúcim sa stranám prísnejšie požiadavky na registráciu a autorizáciu s cieľom zabrániť nezákonnému použitiu údajov v týchto prípadoch. V ostatných prípadoch použitia môžu byť spoliehajúce sa strany oslobodené od oznamovania svojho úmyslu spoliehať sa na európsku digitálnu peňaženku, napríklad ak si právo overovať konkrétne atribúty nevyžaduje autentifikáciu spoliehajúcej sa strany elektronickými prostriedkami alebo ju neumožňuje. V týchto osobných scenároch je používateľ zvyčajne schopný identifikovať spoliehajúcu sa stranu vďaka kontextu, napríklad pri interakcii so zamestnancom požičovne automobilov alebo s lekárnikom. Proces oznamovania sa má riadiť odvetvovými právnymi predpismi Únie alebo odvetvovými vnútroštátnymi právnymi predpismi, keďže to umožňuje zohľadniť rôzne prípady použitia, ktoré sa môžu líšiť z hľadiska požiadaviek na registráciu, spôsobu prevádzky (online/offline) alebo požiadavky na autentifikáciu zariadení schopných prepojenia s európskou peňaženkou digitálnej identity. Overovanie používania európskej peňaženky digitálnej identity spoliehajúcimi sa stranami by sa nemalo povinne presadzovať na úrovni európskej peňaženky digitálnej identity.

(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 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. Vydávanie európskych peňaženiek digitálnej identity, ich používanie na autentifikáciu a ich zrušenie je pre fyzické osoby bezplatné. Službám spoliehajúcim sa na používanie peňaženky môžu vzniknúť náklady, napríklad v súvislosti s vydávaním elektronických osvedčení atribútov peňaženky.

(9a) Je prospešné uľahčiť zavádzanie a používanie európskych peňaženiek digitálnej identity ich bezproblémovou integráciou do ekosystému verejných a súkromných digitálnych služieb, ktoré sa už zaviedli na vnútroštátnej, miestnej alebo regionálnej úrovni. Členské štáty môžu na dosiahnutie tohto cieľa stanoviť právne a organizačné opatrenia s cieľom zvýšiť flexibilitu pre vydavateľov európskych peňaženiek digitálnej identity a umožniť ďalšie funkcie európskych peňaženiek digitálnej identity nad rámec toho, čo je stanovené v tomto nariadení, a to aj prostredníctvom zvýšenej interoperability s existujúcimi vnútroštátnymi prostriedkami elektronickej identifikácie. Nemalo by to byť v žiadnom prípade na úkor poskytovania základných funkcií európskych peňaženiek digitálnej identity, ako sa stanovuje v tomto nariadení, ani na presadzovanie existujúcich vnútroštátnych riešení na úkor európskych peňaženiek digitálnej identity. Keďže tieto dodatočné funkcie presahujú rámec tohto nariadenia, nevzťahujú sa na ne ustanovenia o cezhraničnom spoliehaní sa na európske peňaženky digitálnej identity stanovené v tomto nariadení.

(10) V záujme dosiahnutia vysokej úrovne ochrany údajov, bezpečnosti a dôveryhodnosti by sa týmto nariadením mal stanoviť harmonizovaný rámec, v ktorom sa podrobne uvedú spoločné špecifikácie a požiadavky uplatniteľné na európske peňaženky digitálnej identity. Súlad európskych peňaženiek digitálnej identity s týmito požiadavkami by mali certifikovať akreditované orgány posudzovania zhody určené členskými štátmi. Certifikácia by sa mala opierať najmä o príslušné európske systémy certifikácie kybernetickej bezpečnosti alebo ich časti zriadené podľa nariadenia (EÚ) 2019/881[6], pokiaľ sa vzťahujú na požiadavky kybernetickej bezpečnosti uplatniteľné na európske peňaženky digitálnej identity. Spoliehanie sa na európske systémy certifikácie kybernetickej bezpečnosti by malo priniesť harmonizovanú úroveň dôvery v bezpečnosť európskych peňaženiek digitálnej identity bez ohľadu na to, kde v Únii sa vydávajú. Certifikácia kybernetickej bezpečnosti európskych peňaženiek digitálnej identity by mala vychádzať z úlohy vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti pri dohľade a monitorovaní súladu certifikátov vydaných orgánmi posudzovania zhody v rámci ich právomoci s príslušnými európskymi systémami kybernetickej bezpečnosti. Podobne by certifikácia mala podľa potreby vychádzať z noriem a technických špecifikácií, ako sa uvádza v nariadení (EÚ) 2019/881. Takéto špecifikácie sa môžu použiť ako najpokročilejšie dokumenty, ako sa uvádza v príslušných systémoch certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881. Ak sa žiadne relevantné európske systémy certifikácie kybernetickej bezpečnosti zriadené podľa nariadenia (EÚ) 2019/881 nevzťahujú na certifikáciu príslušných služieb alebo procesov prispievajúcich k bezpečnosti peňaženky, mali by sa vytvoriť vhodné systémy v súlade s hlavou III nariadenia (EÚ) 2019/881. Mal by sa zriadiť spoločný a harmonizovaný systém certifikácie európskych peňaženiek digitálnej identity na posúdenie ich súladu so spoločnými špecifikáciami a požiadavkami stanovenými v tomto nariadení, ktoré sa netýkajú kybernetickej bezpečnosti a ochrany údajov, najmä tých, ktoré sa týkajú funkčných a prevádzkových aspektov. Pokiaľ ide o túto certifikáciu, v záujme zabezpečenia vysokej úrovne dôvery a transparentnosti by sa mali zaviesť mechanizmy a postupy zamerané na podporu partnerského učenia a spolupráce medzi členskými štátmi v oblasti monitorovania a preskúmavania certifikačných orgánov a certifikátov a správ o certifikácii, ktoré vydávajú. Takýmto mechanizmom partnerského učenia by nemalo byť dotknuté nariadenie (ES) 2016/679 a nariadenie (EÚ) 2019/881. Certifikácia peňaženky podľa nariadenia (ES) 2016/679 je dobrovoľným nástrojom, ktorý možno okrem iného použiť na preukázanie súladu s požiadavkami stanovenými v nariadení (ES) 2016/679, keďže sa vzťahujú na európske peňaženky digitálnej identity a ich poskytovanie občanom Európskej únie.

[6] 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).

(10a) Zapojenie občanov a obyvateľov do európskej peňaženky digitálnej identity by sa malo uľahčiť spoliehaním sa na prostriedky elektronickej identifikácie vydané na úrovni zabezpečenia „vysoká“. Prostriedky elektronickej identifikácie vydané na úrovni zabezpečenia „pokročilá“ by sa mali využívať len v prípadoch, keď harmonizované technické a prevádzkové špecifikácie využívajúce prostriedky elektronickej identifikácie vydané na úrovni zabezpečenia „pokročilá“ v kombinácii s inými doplnkovými prostriedkami overenia totožnosti umožnia splnenie požiadaviek stanovených v tomto nariadení, pokiaľ ide o úroveň zabezpečenia „vysoká“. Takéto doplnkové prostriedky alebo opatrenia by mali byť pre používateľov spoľahlivé a ľahko použiteľné a mohli by vychádzať z možnosti používať postupy diaľkového zapojenia, kvalifikované certifikáty podložené kvalifikovanými podpismi, kvalifikované elektronické osvedčenie atribútov alebo ich kombináciu. S cieľom zabezpečiť dostatočné využívanie európskych peňaženiek digitálnej identity by sa vo vykonávacích aktoch mali stanoviť harmonizované technické a prevádzkové špecifikácie pre zapojenie používateľov použitím prostriedkov elektronickej identifikácie vrátane tých, ktoré boli vydané na úrovni zabezpečenia „pokročilá“.

(10b) Cieľom tohto nariadenia je poskytnúť používateľovi plne mobilnú, bezpečnú a používateľsky ústretovú európsku peňaženku digitálnej identity. S cieľom preukázať súlad s príslušnými požiadavkami nariadenia, pokiaľ ide o úroveň zabezpečenia peňaženky, sa európske peňaženky digitálnej identity môžu ako prechodné opatrenie až do dostupnosti certifikovaných riešení odolných proti neoprávnenej manipulácii, ako sú bezpečné prvky v zariadeniach používateľov, spoliehať na certifikované externé bezpečné prvky na ochranu kryptografického materiálu a iných citlivých údajov alebo na oznámené vnútroštátne riešenia s úrovňou zabezpečenia „vysoká“. Použitie uvedeného prechodného opatrenia by sa malo obmedziť na prípady použitia, ktoré si vyžadujú úroveň zabezpečenia „vysoká“, ako je napríklad zapojenie používateľa do peňaženky a autentifikácia prístupu k službám, ktoré si vyžadujú úroveň zabezpečenia „vysoká“. Európske peňaženky digitálnej identity by pri autentifikácii prístupu k službám, ktoré si vyžadujú úroveň zabezpečenia „pokročilá“, nemali vyžadovať použitie uvedeného prechodného opatrenia. Týmto nariadením by nemali byť dotknuté vnútroštátne podmienky vydávania a používania certifikovaného externého bezpečného prvku v prípade, že je toto prechodné opatrenie od neho závislé.

(11) Európske peňaženky digitálnej identity by mali zabezpečiť najvyššiu úroveň ochrany a 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. Spracúvanie biometrických údajov ako autentifikačný faktor v rámci silnej autentifikácie používateľa 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, spracúvanie biometrických údajov je povolené len na základe výnimiek uvedených v článku 9 ods. 2 nariadenia (EÚ) 2016/679 a vyžaduje si primerané záruky úmerné riziku, ktoré takéto spracúvanie môže predstavovať pre práva a slobody fyzických osôb.

(11a) Fungovanie európskych peňaženiek digitálnej identity by malo byť transparentné a malo by umožňovať overiteľné spracúvanie osobných údajov. V záujme dosiahnutie tohto cieľa sa členské štáty vyzývajú, aby zverejnili zdrojový kód softvérových komponentov európskych peňaženiek digitálnej identity, ktoré súvisia so spracúvaním osobných údajov a údajov právnických osôb. Zverejnenie takéhoto zdrojového kódu umožňuje spoločnosti vrátane používateľov a vývojárov pochopiť jeho fungovanie. Tento krok má tiež potenciál zvýšiť dôveru používateľov v ekosystém peňaženky a prispieť k bezpečnosti peňaženiek tým, že každému umožní nahlasovať zraniteľné miesta a chyby v kóde. Tým sa dodávateľom umožní poskytovať a udržiavať vysoko bezpečný výrobok. Členské štáty sa okrem toho tiež nabádajú, aby v náležitých prípadoch zdrojový kód sprístupnili na základe otvorenej licencie. Otvorená licencia umožňuje spoločnosti vrátane používateľov a vývojárov zdrojový kód upraviť a opätovne ho použiť.

(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 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) 2019/1157[7] 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 elektronickej identifikácie 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, ako sa stanovuje v systémoch certifikácie, ktoré sa majú zriadiť na úrovni Únie podľa nariadenia (EÚ) 2019/881, aby podporili svoje tvrdenia o zosúladení systémov alebo ich častí s požiadavkami nariadenia na interoperabilitu a bezpečnosť oznámených schém elektronickej identifikácie.

---

[7] 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).

(17a) Používanie jedinečných a trvalých identifikátorov vydaných členskými štátmi alebo vytvorených európskou peňaženkou digitálnej identity spolu s použitím osobných identifikačných údajov je nevyhnutné na zabezpečenie toho, aby bolo možné overiť totožnosť používateľa, najmä vo verejnom sektore a na základe vnútroštátneho práva alebo práva Únie. Týmto nariadením by sa malo zabezpečiť, aby európska peňaženka digitálnej identity mohla poskytnúť mechanizmus, ktorý umožní priraďovanie záznamov, a to aj prostredníctvom kvalifikovaných elektronických osvedčení atribútov, a umožniť zahrnutie jedinečných a trvalých identifikátorov do súboru osobných identifikačných údajov. Jedinečný a trvalý identifikátor môže pozostávať buď z jedného alebo viacerých identifikačných údajov, ktoré môžu byť špecifické pre daný sektor, pokiaľ slúži na jedinečnú identifikáciu používateľa v celej Únii. Európska peňaženka digitálnej identity by mala takisto poskytovať mechanizmus, ktorý umožní používať identifikátory špecifické pre spoliehajúcu sa stranu v prípadoch, keď sa použitie jedinečného a trvalého identifikátora vyžaduje podľa vnútroštátneho práva alebo práva Únie. Mechanizmus poskytovaný na uľahčenie priraďovania záznamov a používania jedinečných a trvalých identifikátorov by mal vo všetkých prípadoch zabezpečiť, aby bol používateľ chránený pred zneužitím osobných údajov podľa tohto nariadenia a uplatniteľného práva Únie, najmä nariadenia (EÚ) 2016/679, a to aj pred rizikom profilovania a sledovania v súvislosti s používaním európskej peňaženky digitálnej identity.

(17aa) Je nevyhnutné zohľadniť potreby používateľov, a tým zvýšiť dopyt po európskych peňaženkách digitálnej identity. Mali by existovať zmysluplné prípady použitia a online služby založené na dostupných európskych peňaženkách digitálnej identity. V záujme pohodlia používateľov a s cieľom zabezpečiť cezhraničnú dostupnosť takýchto služieb je dôležité prijať opatrenia na uľahčenie podobného prístupu k navrhovaniu, vývoju a vykonávaniu online služieb vo všetkých členských štátoch. Nezáväzné usmernenia o tom, ako navrhovať, vyvíjať a vykonávať online služby využívajúce európske peňaženky digitálnej identity, majú potenciál stať sa užitočným nástrojom na dosiahnutie tohto cieľa. Tieto usmernenia by sa mali vypracovať s náležitým ohľadom na rámec interoperability Únie. Členské štáty by pri ich prijímaní mali zohrávať vedúcu úlohu.

(18) V súlade so smernicou (EÚ) 2019/882[8] 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 rámcu dôvery pre kvalifikované dôveryhodné služby a ich poskytovateľov v tomto nariadení. Pri stanovovaní podmienok, za ktorých by sa rámce dôvery tretích krajín mohli považovať za rovnocenné rámcu dôvery pre kvalifikované dôveryhodné služby a poskytovateľov v tomto nariadení, by sa mal zabezpečiť aj súlad s príslušnými ustanoveniami smernice XXXX/XXXX (smernica NIS2) a nariadenia (EÚ) 2016/679, ako aj používanie dôveryhodných zoznamov ako základných prvkov na budovanie dôvery.

---

[8] 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).

(21) Toto nariadenie by malo vychádzať z aktov Únie, ktorými sa zabezpečujú konkurencieschopné a spravodlivé trhy v digitálnom sektore. Vychádza najmä z nariadenia (EÚ) 2022/1925, ktorým sa zavádzajú pravidlá pre poskytovateľov základných platformových služieb 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. 7 nariadenia 2022/1925 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 títo poskytovatelia používajú pri 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 poskytovať nové celoeurópske elektronické doručovacie služby pre registrované zásielky. S cieľom zabezpečiť, aby sa údaje pri použití kvalifikovanej elektronickej doručovacej služby pre registrované zásielky doručili správnemu adresátovi, by kvalifikované elektronické doručovacie služby pre registrované zásielky mali zabezpečiť identifikáciu adresáta s úplnou istotou, pričom pri identifikácii odosielateľ by postačovala vysoká úroveň spoľahlivosti. Členské štáty by mali poskytovateľov kvalifikovaných elektronických doručovacích služieb pre registrované zásielky nabádať k tomu, aby ich služby boli interoperabilné s kvalifikovanými elektronickými doručovacími službami pre registrované zásielky, ktoré poskytujú iní kvalifikovaní poskytovatelia dôveryhodných služieb, s cieľom ľahko prenášať elektronické údaje o registrovaných zásielkach medzi dvoma alebo viacerými kvalifikovanými poskytovateľmi dôveryhodných služieb a podporovať spravodlivé postupy na vnútornom trhu.

(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 naň, 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 spoliehajúce sa strany, ktoré poskytujú služby v oblasti dopravy, energetiky, bankovníctva, 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 silná autentifikácia používateľa. S cieľom uľahčiť používanie a akceptovanie európskej peňaženky digitálnej identity by sa mali zohľadniť všeobecne uznávané odvetvové normy a špecifikácie. 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 z hľadiska dostupnosti a použiteľnosti európskych peňaženiek digitálnej identity pre používateľa po 24 mesiacoch od ich zavedenia.

(29) Selektívne zverejňovanie je koncepcia, ktorá oprávňuje vlastníka údajov zverejniť len určité časti väčšieho súboru údajov tak, aby prijímajúci subjekt získal len informácie, ktoré sa vyžadujú, napr. aby používateľ poskytol spoliehajúcej sa strane len údaje, ktoré sú potrebné na poskytnutie služby vyžiadanej používateľom. Európska peňaženka digitálnej identity by mala technicky umožniť selektívne zverejňovanie atribútov spoliehajúcim sa stranám. Takéto selektívne zverejnené atribúty, a to vrátane prípadov, keď boli pôvodne časťami viacerých odlišných elektronických osvedčení, sa môžu následne kombinovať a predkladať spoliehajúcim sa stranám. Táto funkcia by sa mala stať základným prvkom štruktúry peňaženky, čím by sa posilnilo pohodlie a ochrana osobných údajov vrátane minimalizácie.

(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. Členské štáty by mali na vnútroštátnej úrovni zaviesť vhodné mechanizmy na zabezpečenie toho, aby kvalifikovaní poskytovatelia dôveryhodných služieb, ktorí vydávajú kvalifikované elektronické osvedčenie atribútov, boli schopní na základe súhlasu osoby, ktorej sa osvedčenie vydáva, overiť pravosť atribútov na základe autentických zdrojov. Vhodné mechanizmy môžu zahŕňať využívanie konkrétnych sprostredkovateľov alebo technických riešení v súlade s vnútroštátnym právom, ktoré umožňujú prístup k autentickým zdrojom. Zabezpečením dostupnosti mechanizmu, ktorý umožní overovanie atribútov pomocou autentických zdrojov, by sa malo uľahčiť, aby kvalifikovaní poskytovatelia dôveryhodných služieb poskytujúci kvalifikované elektronické osvedčenia atribútov dodržiavali svoje povinnosti stanovené v tomto nariadení. Príloha VI obsahuje zoznam kategórií atribútov, v prípade ktorých by členské štáty mali zabezpečiť prijatie opatrení, ktoré kvalifikovaným poskytovateľom elektronických osvedčení atribútov umožnia, aby elektronickými prostriedkami a na žiadosť používateľa overili pravosť týchto atribútov ich porovnaním s príslušným autentickým zdrojom. Na osobitných atribútoch, ktoré budú patriť do týchto kategórií, by sa mali dohodnúť členské štáty.

(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 sa podporilo plnenie prísnych požiadaviek na autentifikáciu zákazníka pri online identifikácii na účely prihlásenia sa do účtu a iniciovania transakcií v oblasti platobných služieb.

31a. S cieľom zabezpečiť konzistentnosť certifikačných postupov v celej EÚ by Komisia mala vydať usmernenia týkajúce sa certifikácie a opätovnej certifikácie zariadení na vyhotovenie kvalifikovaného elektronického podpisu a zariadení na vyhotovenie kvalifikovanej elektronickej pečate vrátane ich platnosti a časových obmedzení. Toto nariadenie nebráni členským štátom v tom, aby verejným alebo súkromným subjektom, ktoré majú certifikované zariadenia na vyhotovenie kvalifikovaného elektronického podpisu, povolili dočasné predĺženie platnosti certifikácie, ak by sa opätovná certifikácia toho istého zariadenia nemohla vykonať v zákonom stanovenom časovom rámci z iného dôvodu, ako je narušenie alebo bezpečnostný incident, a bez toho, aby bol dotknutý uplatniteľný certifikačný postup.

(32) Služby autentifikácie webových sídiel s vysokou úrovňou zabezpečenia poskytujú používateľom istotu, že za daným webovým sídlom stojí skutočný a legitímny subjekt, a to bez ohľadu na platformu použitú na jeho zobrazenie. Uvedené služby prispievajú k budovaniu dôvery a istoty v súvislosti s podnikaním online a k zníženiu počtu prípadov online podvodov. Používanie služieb autentifikácie webových sídiel webovými sídlami by malo byť 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 by sa mali stanoviť minimálne povinnosti týkajúce sa bezpečnosti a zodpovednosti poskytovateľov autentifikácie webových sídiel a ich služieb. Na tento účel by poskytovatelia webových prehliadačov mali zabezpečiť podporu kvalifikovaných certifikátov autentifikácie webových sídiel podľa nariadenia (EÚ) č. 910/2014 a interoperabilitu s nimi. Mali by uznávať kvalifikované certifikáty na autentifikáciu webového sídla a umožňovať zobrazovanie certifikovaných údajov o totožnosti koncovému používateľovi v prostredí prehliadača na základe špecifikácií stanovených v súlade s týmto nariadením. Uznaním kvalifikovaného certifikátu na autentifikáciu webového sídla ako kvalifikovaného certifikátu vydaného kvalifikovaným poskytovateľom dôveryhodných služieb by sa malo zabezpečiť, aby sa údaje o totožnosti uvedené v certifikáte mohli autentifikovať a overiť v súlade s týmto nariadením. Nemalo by to mať vplyv na možnosť poskytovateľov webových prehliadačov riešiť závažné nezrovnalosti v súvislosti s narušením bezpečnosti a stratou integrity jednotlivých certifikátov, čím sa prispeje k online bezpečnosti koncových používateľov. S cieľom ešte viac chrániť občanov a 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 údajov a súvisiace dôveryhodné služby. S cieľom zabezpečiť právnu istotu, dôveru a harmonizáciu vo všetkých členských štátoch by sa mal vytvoriť právny rámec pre kvalifikované elektronické archivačné služby inšpirovaný rámcom pre ostatné dôveryhodné služby stanoveným v tomto nariadení. Tento rámec by mal poskytovateľom dôveryhodných služieb a používateľom ponúknuť účinný súbor nástrojov, ktorý zahŕňa funkčné požiadavky na elektronickú archivačnú službu, ako aj jasné právne účinky pri používaní kvalifikovanej elektronickej archivačnej služby. Tieto ustanovenia by sa mali vzťahovať na dokumenty, ktoré vznikli elektronicky, ako aj na papierové dokumenty, ktoré boli naskenované a digitalizované. Tieto ustanovenia by mali umožňovať, aby sa uchovávané elektronické údaje v prípade potreby preniesli na rôzne médiá alebo do rôznych formátov na účely predĺženia ich trvácnosti a čitateľnosti nad rámec obdobia technologickej platnosti, pričom by sa v čo najväčšej možnej miere minimalizovali straty a zmeny. Ak elektronické údaje zaslané digitálnej archivačnej službe obsahujú jeden alebo viac kvalifikovaných elektronických podpisov alebo kvalifikovaných elektronických pečatí, služba by mala používať postupy a technológie schopné predĺžiť ich dôveryhodnosť počas obdobia uchovávania takýchto údajov, pričom by sa prípadne spoliehala na používanie iných kvalifikovaných dôveryhodných elektronických služieb zriadených týmto nariadením. Na vytváranie dôkazov o uchovávaní v prípade použitia elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok by sa mali používať kvalifikované dôveryhodné elektronické služby. Ak elektronické archivačné služby nie sú týmto nariadením harmonizované, členské štáty môžu v súlade s právom Únie zachovať alebo zaviesť vnútroštátne ustanovenia týkajúce sa týchto služieb, ako sú osobitné ustanovenia umožňujúce určité výnimky pre služby integrované do organizácie a používané výlučne pre „interné archívy“ tejto organizácie. V tomto nariadení by sa nemalo rozlišovať medzi dokumentmi, ktoré vznikli elektronicky, a papierovými dokumentmi, ktoré boli digitalizované.

(33a) Národné archívy a pamäťové inštitúcie ako organizácie zamerané na zachovanie dokumentárneho dedičstva vo verejnom záujme sú zvyčajne poverené vykonávaním svojich činností podľa vnútroštátneho práva a nemusia nevyhnutne poskytovať dôveryhodné služby v zmysle tohto nariadenia. Pokiaľ tieto inštitúcie takéto služby neposkytujú, ich fungovanie týmto nariadením nie je dotknuté.

(34) Elektronické registre sú sekvenciou záznamov elektronických údajov, ktoré zabezpečujú ich integritu a presnosť ich chronologického poradia. Účelom elektronických registrov je stanoviť chronologickú postupnosť záznamov údajov s cieľom zabrániť kopírovaniu digitálnych aktív a ich predaju viacerým príjemcom. Elektronické registre sa môžu napríklad použiť na digitálne záznamy vlastníctva v globálnom obchode, financovanie dodávateľského reťazca, digitalizáciu práv duševného vlastníctva alebo komodít, ako je elektrická energia. V spojení s inými technológiami môžu prispieť k riešeniam pre efektívnejšie a transformačnejšie verejné služby, ako sú elektronické hlasovanie, cezhraničná spolupráca colných orgánov, cezhraničná spolupráca akademických inštitúcií alebo zaznamenávanie vlastníctva nehnuteľností v decentralizovaných katastroch nehnuteľností. Kvalifikované elektronické registre vytvárajú právnu domnienku jedinečného a presného sekvenčného chronologického poradia a integrity záznamov údajov v registri. Osobitné atribúty elektronických registrov, t. j. sekvenčné chronologické poradie záznamov údajov, odlišujú elektronické registre od iných dôveryhodných služieb, ako sú elektronické časové pečiatky a elektronické doručovacie služby pre registrované zásielky. Konkrétne ani časová pečiatka digitálnych dokumentov, ani ich prenos prostredníctvom elektronických doručovacích služieb pre registrované zásielky by bez ďalších technických alebo organizačných opatrení nemohli dostatočne zabrániť tomu, aby sa rovnaké digitálne aktívum skopírovalo a predalo viac ako raz rôznym stranám. Postup vytvárania a aktualizácie elektronického registra závisí od typu použitého registra (centralizovaný alebo distribuovaný).

(35) S cieľom zabrániť fragmentácii vnútorného trhu by sa mal vytvoriť celoeurópsky právny rámec, ktorý umožní cezhraničné uznávanie dôveryhodných služieb na zaznamenávanie údajov v kvalifikovaných elektronických registroch. Poskytovateľom dôveryhodných služieb pre elektronické registre by mala byť uložená povinnosť zabezpečiť sekvenčné zaznamenávanie údajov do registra. Toto nariadenie sa uplatňuje bez ohľadu na akékoľvek právne povinnosti, ktoré sa môžu vzťahovať na používateľov elektronických registrov podľa práva Únie a vnútroštátneho práva. Napríklad prípady použitia, ktoré zahŕňajú spracúvanie osobných údajov, by mali byť v súlade s nariadením (EÚ) 2016/679. Prípady použitia, ktoré zahŕňajú kryptoaktíva, by mali byť zlučiteľné so všetkými uplatniteľnými finančnými pravidlami vrátane napríklad smernice o trhoch s finančnými nástrojmi[9], smernice o platobných službách[10], smernice o elektronických peniazoch[11], ako aj s možnými budúcimi právnymi predpismi o trhoch s kryptoaktívami a s pravidlami boja proti praniu špinavých peňazí, ktoré by mohli byť zahrnuté do nariadenia o prevode finančných prostriedkov[12], a mohli by vyžadovať, aby poskytovatelia služieb v oblasti kryptoaktív overovali totožnosť používateľov elektronických registrov s cieľom dodržiavať medzinárodné normy boja proti praniu špinavých peňazí.

---

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

10 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).

11 Smernica Európskeho parlamentu a Rady (EÚ) 2009/110/ES zo 16. septembra 2009 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva, ktorou sa menia a dopĺňajú smernice 2005/60/ES a 2006/48/ES a zrušuje smernica 2000/46/ES (Ú. v. EÚ L 267, 10.10.2009, s. 7 – 17).

12 Pozri návrh Komisie z 20. júla 2021 na prepracovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2015/847 z 20. mája 2015 o údajoch sprevádzajúcich prevody finančných prostriedkov, COM/2021/422 final.

(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][13] 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.

36a. Členské štáty by mali stanoviť pravidlá týkajúce sa sankcií za porušenia, ako sú priame alebo nepriame praktiky vedúce k zámene medzi nekvalifikovanými a kvalifikovanými dôveryhodnými službami alebo k zneužívaniu značky dôvery EÚ nekvalifikovanými poskytovateľmi dôveryhodných služieb. Značka dôvery EÚ by sa nemala používať za podmienok, ktoré priamo alebo nepriamo vedú k presvedčeniu, že akékoľvek nekvalifikované dôveryhodné služby ponúkané týmto poskytovateľom sú kvalifikované.

---

13 [Po prijatí vložte odkaz].

(36b) Týmto nariadením by sa mala zabezpečiť harmonizovaná úroveň kvality, dôveryhodnosti a bezpečnosti kvalifikovaných dôveryhodných služieb bez ohľadu na miesto, kde sa operácie vykonávajú. Kvalifikovaný poskytovateľ dôveryhodných služieb by preto mal mať možnosť vykonávať svoje činnosti súvisiace s poskytovaním kvalifikovanej dôveryhodnej služby prostredníctvom externých dodávateľov mimo Únie, pokiaľ poskytne záruky a zabezpečí, že činnosti dohľadu a audity možno vymáhať tak, ako keby sa tieto operácie vykonávali v Únii. Ak súlad s nariadením nemožno v plnej miere zabezpečiť, orgány dohľadu by mali mať možnosť prijať primerané a odôvodnené opatrenia vrátane odňatia kvalifikovaného štatútu poskytovanej dôveryhodnej službe.

(36c) Na zabezpečenie právnej istoty v súvislosti s platnosťou zdokonalených elektronických podpisov založených na kvalifikovaných certifikátoch je nevyhnutné určiť zložky zdokonaleného elektronického podpisu založeného na kvalifikovaných certifikátoch, ktoré by mala posúdiť spoliehajúca sa strana vykonávajúca validáciu tohto podpisu.

(36d) Poskytovatelia dôveryhodných služieb by s cieľom zaistiť bezpečnosť a spoľahlivosť svojich dôveryhodných služieb mali používať kryptografické algoritmy odzrkadľujúce súčasné najlepšie postupy a dôveryhodné vykonávanie týchto algoritmov.

(36e) V tomto nariadení by sa pre kvalifikovaných poskytovateľov dôveryhodných služieb mala stanoviť povinnosť overovať totožnosť fyzickej alebo právnickej osoby, ktorej sa kvalifikovaný certifikát vydáva, a to na základe rôznych harmonizovaných metód v celej EÚ. Takáto metóda môže zahŕňať spoliehanie sa na prostriedky elektronickej identifikácie, ktoré spĺňajú požiadavky úrovne zabezpečenia „pokročilá“ v kombinácii s dodatočnými harmonizovanými diaľkovými postupmi, ktoré zabezpečujú identifikáciu osoby s vysokou úrovňou spoľahlivosti.

(36f) Vydavatelia európskych peňaženiek digitálnej identity a vydavatelia oznámených prostriedkov elektronickej identifikácie konajúci v rámci obchodnej alebo odbornej činnosti, ktorí využívajú základné platformové služby, ktoré strážcovia prístupu ponúkajú na účely alebo počas poskytovania tovaru a služieb koncovým používateľom, by sa mali považovať za komerčných používateľov v súlade s článkom 2 ods. 21 nariadenia (EÚ) 2022/1925. Od strážcov prístupu by sa preto malo vyžadovať, aby bezplatne zabezpečili účinnú interoperabilitu s rovnakým operačným systémom, hardvérovými alebo softvérovými prvkami, ktoré sú dostupné alebo používané pri poskytovaní vlastných doplnkových a podporných služieb a hardvéru, a prístup k nim na účely interoperability. To by malo vydavateľom európskych peňaženiek digitálnej identity a vydavateľom oznámených prostriedkov elektronickej identifikácie umožniť prepojiť sa prostredníctvom rozhraní alebo podobných riešení s príslušnými funkciami tak účinne ako vlastné služby alebo hardvér strážcu prístupu.

(36g) Aby bolo toto nariadenie v súlade so súčasným vývojom a aby sa dodržiavali postupy na vnútornom trhu, mali by sa delegované a vykonávacie akty prijaté Komisiou pravidelne preskúmavať a v prípade potreby aktualizovať. Pri posudzovaní potreby týchto aktualizácií by sa mali zohľadniť nové technológie, postupy, normy alebo technické špecifikácie, ktoré sa objavili na vnútornom trhu.

(37) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1525 prebehla konzultácia s európskym dozorným úradníkom pre ochranu údajov[14].

(38) Nariadenie (EÚ) 910/2014 by sa preto malo zodpovedajúcim spôsobom zmeniť,

---

14 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:

aa) 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;

ab) stanovujú podmienky, za ktorých členské štáty poskytujú a uznávajú európske peňaženky digitálnej identity;

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 overovanie elektronických podpisov, elektronických pečatí a ich certifikátov, elektronické overovanie certifikátov pre autentifikáciu webového sídla, elektronické uchovávanie elektronických podpisov, elektronických pečatí a ich certifikátov, elektronickú archiváciu, elektronické osvedčovanie atribútov, správu zariadení na vyhotovenie elektronického podpisu a pečate na diaľku a pre elektronické registre.“;

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 poskytované 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 formy alebo sektorovo špecifických požiadaviek týkajúcich sa formy.“;

3. Článok 3 sa mení takto:

(X) Bod 1 sa nahrádza takto:

„1. „elektronická identifikácia“ je proces používania osobných identifikačných údajov v elektronickej forme, ktoré jedinečne reprezentujú fyzickú osobu alebo právnickú osobu alebo fyzickú osobu zastupujúcu fyzickú osobu alebo právnickú osobu;“;

a) Bod 2 sa nahrádza takto:

„2. „prostriedok elektronickej identifikácie“ je hmotná a/alebo nehmotná jednotka vrátane európskych peňaženiek digitálnej identity, ktorá obsahuje osobné identifikačné údaje a ktorá sa používa na autentifikáciu v rámci online služby alebo v náležitých prípadoch offline služby;“;

aa) Bod 3 sa nahrádza takto:

„3. „osobné identifikačné údaje“ sú súbor údajov vydaný v súlade s právom Únie alebo vnútroštátnym právom, ktorý umožňuje určiť totožnosť fyzickej osoby alebo právnickej osoby alebo fyzickej osoby zastupujúcej fyzickú osobu alebo právnickú osobu;“;

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 fyzické osoby alebo právnické osoby vydávajú prostriedky elektronickej identifikácie;“;

ba) Bod 5 sa nahrádza takto:

„5. „autentifikácia“ je elektronický proces, ktorý umožňuje potvrdiť elektronickú identifikáciu fyzickej osoby alebo právnickej osoby alebo pôvod a integritu údajov v elektronickej forme;“;

bb) Vkladá sa tento bod 5a:

„5a. „používateľ“ je fyzická osoba alebo právnická osoba alebo fyzická osoba zastupujúca fyzickú osobu alebo právnickú osobu, ktorá používa dôveryhodné služby alebo prostriedky elektronickej identifikácie poskytované podľa tohto nariadenia;“;

c) Bod 14 sa nahrádza takto:

„14. „certifikát pre elektronický podpis“ je elektronické osvedčenie, ktoré 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 odplatu a spočíva:

a) vo vydávaní certifikátov pre elektronické podpisy, certifikátov pre elektronické pečate, certifikátov pre autentifikáciu webového sídla alebo certifikátov pre poskytovanie iných dôveryhodných služieb;

aa) vo validácii certifikátov pre elektronické podpisy, certifikátov pre elektronické pečate, certifikátov pre autentifikáciu webového sídla alebo certifikátov pre poskytovanie iných dôveryhodných služieb;

b) vo vyhotovovaní elektronických podpisov alebo elektronických pečatí;

c) v overovaní elektronických podpisov alebo elektronických pečatí;

d) v uchovávaní elektronických podpisov, elektronických pečatí, certifikátov pre elektronické podpisy alebo certifikátov pre elektronické pečate;

e) v správe zariadení na vyhotovenie kvalifikovaného elektronického podpisu na diaľku alebo zariadení na vyhotovenie kvalifikovanej elektronickej pečate na diaľku;

f) vo vydávaní elektronických osvedčení atribútov;

fa) vo validácii elektronického osvedčenia atribútov;

g) vo vyhotovovaní elektronických časových pečiatok;

ga) vo validácii elektronických časových pečiatok;

gb) v poskytovaní elektronickej doručovacej služby pre registrované zásielky;

gc) vo validácii údajov prenášaných prostredníctvom elektronických doručovacích služieb pre registrované zásielky a súvisiacich dôkazov;

h) v elektronickej archivácii elektronických údajov; alebo

i) v zaznamenávaní elektronických údajov do elektronického registra;“;

da) Bod 18 sa nahrádza takto:

„18. „orgán posudzovania zhody“ je orgán vymedzený v článku 2 bode 13 nariadenia (ES) č. 765/2008, ktorý je v súlade s uvedeným nariadením akreditovaný ako orgán príslušný na posudzovanie zhody kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytujú, alebo na vykonávanie certifikácie európskej peňaženky digitálnej identity alebo prostriedku elektronickej identifikácie;“;

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 elektronického podpisu na diaľku“ je zariadenie na vyhotovenie kvalifikovaného elektronického podpisu spravované kvalifikovaným poskytovateľom dôveryhodných služieb v súlade s článkom 29a v mene podpisovateľa;

23b. „zariadenie na vyhotovenie kvalifikovanej elektronickej pečate na diaľku“ je zariadenie na vyhotovenie kvalifikovanej elektronickej pečate spravované kvalifikovaným poskytovateľom dôveryhodných služieb v súlade s článkom 39a v mene pôvodcu pečate;“;

g) Bod 29 sa nahrádza takto:

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

h) Bod 41 sa nahrádza takto:

„41. „validácia“ je proces overovania a potvrdenia, že údaje v elektronickej podobe sú platné v súlade s požiadavkami tohto nariadenia;“;

i) Dopĺňajú sa tieto body 42 až 55b:

„42. „európska peňaženka digitálnej identity“ je prostriedok elektronickej identifikácie, ktorý používateľovi umožňuje uchovávať a vyhľadávať údaje o totožnosti vrátane osobných identifikačných údajov a elektronické osvedčenia atribútov spojené s jeho totožnosťou, na požiadanie ich poskytovať spoliehajúcim sa stranám a používať ich na autentifikáciu online a v náležitých prípadoch offline na účely služby v súlade s článkom 6a; a umožňuje podpisovať pomocou kvalifikovaných elektronických podpisov a vyhotovovať pečate pomocou kvalifikovaných elektronických pečatí;

43. „atribút“ je charakteristika, vlastnosť, právo alebo povolenie fyzickej alebo právnickej osoby alebo predmetu;

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;

45a. „elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene“ je elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo subjektom verejného sektora, ktorý členský štát určil na vydávanie takýchto osvedčení atribútov v mene subjektov verejného sektora zodpovedných za autentické zdroje v súlade s článkom 45da a požiadavkami stanovenými v prílohe VII;

46. „autentický zdroj“ je register alebo systém, za ktorý je zodpovedný subjekt verejného sektora alebo súkromný subjekt, ktorý obsahuje a poskytuje atribúty o fyzickej alebo právnickej osobe a považuje sa za primárny zdroj týchto informácií alebo je v súlade s právom Únie alebo vnútroštátnym právom vrátane administratívnej praxe uznaný za autentický;

47. „elektronická archivácia“ je služba zabezpečujúca príjem, uchovávanie, vyhľadávanie a vymazávanie elektronických údajov s cieľom zaručiť ich trvácnosť a čitateľnosť, ako aj zachovať ich integritu, dôvernosť a dôkaz o pôvode počas celého obdobia uchovávania;

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

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

50. „silná autentifikácia používateľa“ je autentifikácia založená na použití najmenej dvoch autentifikačných faktorov z rôznych kategórií, ktorými sú buď znalosť (niečo, čo vie len používateľ), vlastníctvo (niečo, čo má len používateľ) alebo charakteristický znak (niečo, čím používateľ je), ktoré sú nezávislé a porušenie jedného prvku neohrozuje spoľahlivosť ostatných prvkov, a je navrhnutá tak, aby chránila dôvernosť autentifikačných údajov;

53. „elektronický register“ je sekvencia záznamov elektronických údajov, ktorá zabezpečuje ich integritu a presnosť ich chronologického usporiadania;

53a. „kvalifikovaný elektronický register“ je elektronický register, ktorý spĺňa požiadavky stanovené v článku 45i;

54. „osobné údaje“ sú všetky informácie v zmysle vymedzenia v článku 4 bode 1 nariadenia (EÚ) 2016/679;

55. „priraďovanie záznamov“ je proces, pri ktorom sa osobné identifikačné údaje, osobné identifikačné prostriedky, kvalifikované elektronické osvedčenie atribútov alebo osvedčenia atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene priradia k existujúcemu kontu patriacemu tej istej osobe alebo sa s ním prepoja;

55a. „jedinečný a trvalý identifikátor“ je identifikátor, ktorý môže pozostávať buď z jedného alebo viacerých vnútroštátnych alebo sektorových identifikačných údajov, je v rámci daného systému spojený s jediným používateľom a je z časového hľadiska trvalý;

55b. „záznam údajov“ sú zaznamenané elektronické údaje so súvisiacimi metaúdajmi (alebo atribútmi), ktoré podporujú spracovanie údajov;

55c. „offline používanie európskych peňaženiek digitálnej identity“ je interakcia medzi používateľom a spoliehajúcou sa stranou na fyzickom mieste, pri ktorej sa od peňaženky na účely interakcie nevyžaduje prístup k diaľkovým systémom prostredníctvom elektronických komunikačných sietí.“;

„*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 pred článok 6a vkladá tento nadpis:

„ODDIEL I

Európske peňaženky digitálnej identity;

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 cezhraničný prístup k verejným a súkromným službám, každý členský štát zabezpečí, aby európska peňaženka digitálnej identity bola poskytnutá do 24 mesiacov od nadobudnutia účinnosti vykonávacích aktov uvedených v odseku 11 a článku 6c ods. 4.

„2. Európske peňaženky digitálnej identity:

a) poskytuje členský štát;

b) sa poskytujú na základe poverenia členského štátu; alebo

c) sa poskytujú nezávisle od členského štátu, ale členský štát ich uznáva.

„3. Európske peňaženky digitálnej identity sú prostriedkom elektronickej identifikácie, ktorý používateľovi transparentne a spôsobom, ktorý je používateľom vysledovateľný, umožňuje:

a) bezpečne požadovať, vyberať, kombinovať, uchovávať, vymazávať a predkladať spoliehajúcim sa stranám elektronické osvedčenie atribútov a osobné identifikačné údaje vrátane autentifikácie online a v náležitých prípadoch offline s cieľom využívať verejné a súkromné služby, pričom by sa zabezpečila možnosť selektívneho zverejňovania údajov;

b) podpisovať pomocou kvalifikovaných elektronických podpisov a vyhotovovať pečate pomocou kvalifikovaných elektronických pečatí.

„4. Európske peňaženky digitálnej identity najmä:

a) zabezpečujú spoločný súbor rozhraní:

1. na vydávanie osobných identifikačných údajov, kvalifikovaných a nekvalifikovaných elektronických osvedčení atribútov alebo kvalifikovaných a nekvalifikovaných certifikátov pre európsku peňaženku digitálnej identity;

2. pre spoliehajúce sa strany, aby mohli požadovať osobné identifikačné údaje a elektronické osvedčenia atribútov;

3. na prezentáciu osobných identifikačných údajov alebo elektronického osvedčenia atribútov spoliehajúcim sa stranám online a náležitých prípadoch aj offline;

4. pre používateľa s cieľom umožniť interakciu s európskou peňaženkou digitálnej identity a zobraziť „značku dôvery EÚ pre peňaženku digitálnej identity;

b) neposkytujú poskytovateľom dôveryhodných služieb elektronických osvedčení atribútov žiadne informácie o používaní týchto atribútov po ich vydaní;

ba) zabezpečujú, aby identita spoliehajúcich sa strán mohla byť potvrdená zavedením autentifikačných mechanizmov v súlade s článkom 6b;

c) spĺňajú požiadavky stanovené v článku 8, pokiaľ ide o úroveň zabezpečenia „vysoká“, ktoré sa mutatis mutandis uplatňujú na správu a používanie osobných identifikačných údajov prostredníctvom peňaženky vrátane elektronickej identifikácie a autentifikácie;

e) zabezpečujú, aby osobné identifikačné údaje uvedené v článku 12 ods. 4 písm. d) jednoznačne a trvalo reprezentovali fyzickú osobu, právnickú osobu alebo fyzickú osobu zastupujúcu fyzickú osobu alebo právnickú osobu, ktorá je s peňaženkou spojená.

4a. Členské štáty stanovia postupy, ktoré používateľovi umožnia nahlásiť možnú stratu alebo zneužitie svojej peňaženky a požiadať o jej zrušenie.

„5. Členské štáty poskytujú mechanizmy validácie pre európske peňaženky digitálnej identity s cieľom:

a) zabezpečiť, aby bolo možné overiť ich pravosť a platnosť;

d) umožniť používateľovi autentifikovať spoliehajúce sa strany v súlade s článkom 6b;

„6. Európske peňaženky digitálnej identity sa vydávajú v rámci oznámenej schémy elektronickej identifikácie, ktorej úroveň zabezpečenia je „vysoká“.

6a Vydávanie európskych peňaženiek digitálnej identity, ich používanie na autentifikáciu a ich zrušenie je pre fyzické osoby bezplatné.

6b Bez toho, aby bol dotknutý článok 6db, môžu členské štáty v súlade s vnútroštátnym právom stanoviť dodatočné funkcie európskych peňaženiek digitálnej identity vrátane interoperability s existujúcimi vnútroštátnymi prostriedkami elektronickej identifikácie.

„7. Používatelia musia mať plnú kontrolu nad používaním európskej peňaženky digitálnej identity a nad údajmi vo svojej európskej peňaženke digitálnej identity. 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 nepožiadal. Osobné údaje týkajúce sa poskytovania európskych peňaženiek digitálnej identity sa uchovávajú logicky oddelene od všetkých ostatných údajov uchovávaných vydavateľom európskej peňaženky digitálnej identity. 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.

7a. Členské štáty bez zbytočného odkladu oznámia Komisii informácie o:

a) orgáne zodpovednom za vytvorenie a vedenie zoznamu oznámených spoliehajúcich sa strán, ktoré sa spoliehajú na európske peňaženky digitálnej identity v súlade s článkom 6b ods. 2;

b) orgánoch zodpovedných za poskytovanie európskych peňaženiek digitálnej identity v súlade s článkom 6a ods. 1;

c) orgánoch zodpovedných za zabezpečenie toho, aby sa osobné identifikačné údaje spájali s peňaženkou v súlade s článkom 6a ods. 4 písm. e);

Oznámenie obsahuje aj informácie o mechanizme, ktorý umožňuje validáciu osobných identifikačných údajov uvedených v článku 12 ods. 4, a identity spoliehajúcich sa strán.

Komisia prostredníctvom zabezpečeného kanálu sprístupňuje verejnosti informácie uvedené v tomto odseku v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

„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 vydavateľa európskych peňaženiek digitálnej identity.

„10. Európska peňaženka digitálnej identity sa sprístupní osobám so zdravotným postihnutím v súlade s požiadavkami na prístupnosť uvedenými v 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, 5 a 7a 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.

11a. Komisia stanoví technické a prevádzkové špecifikácie, ako aj referenčné normy s cieľom uľahčiť zapojenie používateľov do európskej peňaženky digitálnej identity pomocou prostriedkov elektronickej identifikácie na úrovni „vysoká“ alebo pomocou prostriedkov elektronickej identifikácie na úrovni „pokročilá“ v spojení s dodatočnými postupmi diaľkového zapojenia, ktoré spolu spĺňajú požiadavky úrovne zabezpečenia „vysoká“. 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, ktoré poskytujú súkromné alebo verejné služby, v úmysle využívať európske peňaženky digitálnej identity poskytované v súlade s týmto nariadením, oznámia to členskému štátu, v ktorom sú spoliehajúce sa strany usadené.

1a. Postup oznamovania je nákladovo efektívny a primeraný riziku a zabezpečuje, aby spoliehajúce sa strany poskytovali aspoň informácie potrebné na autentifikáciu prístupu do európskych peňaženiek digitálnej identity. To by malo zahŕňať aspoň členský štát, v ktorom sú usadené, názov spoliehajúcej sa strany a prípadne jej registračné číslo, ako sa uvádza v úradných záznamoch.

1b. Oznamovacia povinnosť sa uplatňuje bez toho, aby boli dotknuté iné požiadavky na oznamovanie a registráciu v súlade s právom Únie alebo vnútroštátnym právom, ako sú požiadavky uplatniteľné na osobitné kategórie osobných údajov, ktoré si môžu vyžadovať dodatočné požiadavky na autorizáciu.

1c. Členské štáty môžu oslobodiť spoliehajúce sa strany od oznamovacej povinnosti, ak sa v práve Únie alebo vo vnútroštátnom práve nestanovujú osobitné požiadavky na oznamovanie alebo registráciu s cieľom získať prístup k informáciám poskytovaným prostredníctvom európskej peňaženky digitálnej identity. Oslobodené spoliehajúce sa strany nemusia autentifikovať prístup do európskej peňaženky digitálnej identity.

1d. Spoliehajúce sa strany oznámené v súlade s týmto článkom bezodkladne informujú členský štát o každej následnej zmene pôvodne poskytnutých informácií.

„2. Spoliehajúce sa strany zabezpečia zavedenie autentifikačných mechanizmov uvedených v článku 6a ods. 4 písm. ba).

„3. Spoliehajúce sa strany sú zodpovedné za vykonanie postupu autentifikácie osôb a validácie elektronických osvedčení atribútov pochádzajúcich z európskych peňaženiek digitálnej identity získaných prostredníctvom spoločného rozhrania podľa článku 6a ods. 4 písm. a) bodu 2.

„4. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia stanoví technické a prevádzkové špecifikácie pre požiadavky uvedené v odsekoch 1, 1a a 1d prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 11. Tento vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 6c

Certifikácia európskych peňaženiek digitálnej identity

„1. Súlad európskych peňaženiek digitálnej identity s požiadavkami stanovenými v článku 6a ods. 3, 4 a 5, s požiadavkou na logické oddelenie stanovenou v článku 6a ods. 7 a prípadne s požiadavkami stanovenými v článku 6a ods. 11a certifikujú orgány posudzovania zhody akreditované v súlade s článkom 60 aktu o kybernetickej bezpečnosti a so systémami, špecifikáciami, normami a postupmi uvedenými v súlade s odsekom 4 písm. a), aa) a aaa) a určenými členskými štátmi. Certifikácia nesmie presiahnuť päť rokov a je podmienená pravidelným dvojročným posúdením zraniteľnosti. Ak sa zistia zraniteľnosti a neodstránia sa do troch mesiacov, certifikácia sa zruší.

„2. Pokiaľ ide o súlad s požiadavkami na ochranu údajov podľa článku 6a ods. 7, certifikáciu podľa odseku 1 možno doplniť o certifikáciu podľa článku 42 nariadenia (EÚ) 2016/679.

„3. Zhodu európskych peňaženiek digitálnej identity alebo ich častí s požiadavkami týkajúcimi sa kybernetickej bezpečnosti stanovenými v článku 6a ods. 3, 4, 5, 7 a prípadne v článku 11a certifikujú orgány posudzovania zhody uvedené v odseku 1 v rámci príslušných systémov certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881, ako sa na ne odkazuje v súlade s odsekom 4 písm. a) a odsekom 4 písm. aa).

3a. Na certifikované európske peňaženky digitálnej identity sa nevzťahujú požiadavky uvedené v článkoch 7 a 9.

„4. Do 6 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí:

a) zoznam systémov certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 požadovaných na certifikáciu európskych peňaženiek digitálnej identity, ako sa uvádza v odseku 3;

aa) špecifikácie, postupy a referenčné normy na ich používanie v rámci príslušných systémov certifikácie kybernetickej bezpečnosti uvedených v súlade s písmenom a);

aaa) zoznam špecifikácií, postupov a referenčných noriem, ktorými sa stanovujú spoločné požiadavky na certifikáciu, na ktoré sa nevzťahujú príslušné systémy certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 na účely certifikácie uvedenej v odseku 1, s cieľom preukázať, že európska peňaženka digitálnej identity spĺňa požiadavky uvedené v odseku 1;

b) technické, procedurálne, organizačné a prevádzkové špecifikácie na určenie orgánov posudzovania zhody uvedených v odseku 1, a pokiaľ ide o požiadavky na certifikáciu stanovené podľa písmena aaa), na monitorovanie a preskúmanie systémov certifikácie a súvisiacich metód hodnotenia, ktoré tieto orgány používajú, ako aj certifikátov a správ o certifikácii, ktoré vydávajú;

„5. Členské štáty oznámia Komisii názvy a adresy verejných alebo súkromných subjektov, ktoré sú uvedené v odseku 1. Komisia sprístupní tieto informácie členským štátom.

„6. Vykonávacie akty uvedené v odseku 4 sa prijímajú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 6d

Uverejnenie zoznamu certifikovaných európskych peňaženiek digitálnej identity

„1. Členské štáty bez zbytočného odkladu informujú Komisiu o európskych peňaženkách digitálnej identity, ktoré boli poskytnuté podľa článku 6a a certifikované subjektmi uvedenými v článku 6c ods. 1. Bez zbytočného odkladu ju informujú aj o zrušení certifikácie.

„2. Komisia na základe získaných informácií vypracuje, zverejní a aktualizuje strojovo čitateľný 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 a 2 prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 11. Tento vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 6da

Narušenie bezpečnosti európskych peňaženiek digitálnej identity

„1. Ak sú európske peňaženky digitálnej identity poskytnuté podľa článku 6a alebo mechanizmy validácie uvedené v článku 6a ods. 5 písm. a), d) alebo e) narušené alebo čiastočne skompromitované spôsobom, ktorý ovplyvňuje ich spoľahlivosť alebo spoľahlivosť iných európskych peňaženiek digitálnej identity, vydavateľ dotknutých peňaženiek bez zbytočného odkladu pozastaví vydávanie a používanie európskej peňaženky digitálnej identity. Členský štát, v ktorom boli dotknuté peňaženky poskytnuté, bez zbytočného odkladu informuje členské štáty a Komisiu. Vydavateľ dotknutých peňaženiek alebo členský štát o tom informuje spoliehajúce sa strany a používateľov.

„2. Po náprave narušenia alebo skompromitovania uvedeného v odseku 1 vydavateľ peňaženky obnoví vydávanie a používanie európskej peňaženky digitálnej identity. Členský štát, v ktorom boli dotknuté peňaženky poskytnuté, bez zbytočného odkladu informuje členské štáty a Komisiu. Vydavateľ dotknutých peňaženiek alebo členský štát bez zbytočného odkladu informuje spoliehajúce sa strany a používateľov.

„3. Ak sa narušenie alebo skompromitovanie uvedené v odseku 1 neodstráni do troch mesiacov od pozastavenia, príslušný členský štát stiahne predmetnú európsku peňaženku digitálnej identity a informuje o tom ostatné členské štáty a Komisiu. Ak je to odôvodnené závažnosťou narušenia, príslušná európska peňaženka digitálnej identity sa stiahne bez zbytočného odkladu.

„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, 2 a 3 prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 11. Tento vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 6db

Cezhraničné využívanie európskych peňaženiek digitálnej identity

„1. Ak členské štáty na prístup k online službe, ktorú poskytuje subjekt verejného sektora, vyžadujú elektronickú identifikáciu s použitím prostriedkov elektronickej identifikácie a autentifikáciou, akceptujú na autentifikáciu aj európske peňaženky digitálnej identity poskytnuté v súlade s týmto nariadením.

„2. Ak sa podľa vnútroštátneho práva alebo práva Únie od súkromných spoliehajúcich sa strán, ktoré poskytujú služby, s výnimkou mikropodnikov a malých podnikov vymedzených v odporúčaní Komisie 2003/361/ES, 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, finančných služieb, sociálneho zabezpečenia, zdravotníctva, pitnej vody, poštových služieb, digitálnej infraštruktúry, vzdelávania alebo telekomunikácií, súkromné spoliehajúce sa strany najneskôr do 12 mesiacov odo dňa poskytnutia európskych peňaženiek digitálnej identity podľa článku 6a ods. 1 a výlučne na základe dobrovoľnej žiadosti používateľa akceptujú aj používanie európskych peňaženiek digitálnej identity poskytovaných v súlade s týmto nariadením, pokiaľ ide o minimálne údaje potrebné pre konkrétnu online službu, pre ktorú sa požaduje autentifikácia používateľa.

„3. Ak veľmi veľké online platformy vymedzené v článku 25 ods. 1 nariadenia [odkaz na nariadenie o digitálnych službách] vyžadujú, aby sa používatelia autentifikovali na prístup k online službám, akceptujú aj používanie európskych peňaženiek digitálnej identity poskytnutých v súlade s týmto nariadením na autentifikáciu používateľa výlučne na základe dobrovoľnej žiadosti používateľa a s minimálnymi údajmi potrebnými pre konkrétnu online službu, pre ktorú sa autentifikácia požaduje.

„4. Komisia v spolupráci s členskými štátmi podporuje a uľahčuje vypracúvanie kódexov správania s cieľom prispieť k širokej dostupnosti a použiteľnosti európskych peňaženiek digitálnej identity v rozsahu pôsobnosti tohto nariadenia. Týmito kódexmi správania sa uľahčuje 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 24 mesiacov po zavedení európskych peňaženiek digitálnej identity posúdi, či na základe dôkazov preukazujúcich dopyt po európskej peňaženke digitálnej identity a jej dostupnosť a použiteľnosť bude ďalším súkromným poskytovateľom online služieb uložená povinnosť akceptovať používanie európskej peňaženky digitálnej identity výlučne na základe dobrovoľnej žiadosti používateľa. Kritériá posudzovania zahŕňajú rozsah používateľskej základne, cezhraničnú prítomnosť poskytovateľov služieb, technologický vývoj, vývoj modelov používania a dopyt spotrebiteľov.“;

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, ktoré tak ešte neurobili, oznámia do 24 mesiacov od nadobudnutia účinnosti vykonávacích aktov uvedených v článku 6a ods. 11 a článku 6c ods. 4 aspoň jednu schému elektronickej identifikácie zahŕňajúcu aspoň jeden prostriedok identifikácie s úrovňou zabezpečenia „vysoká“. Schéma elektronickej identifikácie sa oznamuje podľa článku 9 ods. 1 za predpokladu, že sú splnené všetky tieto podmienky:;

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.“;

12. Vkladá sa tento článok 11a:

„*Článok 11a*

Priraďovanie záznamov

„1. Ak sa na autentifikáciu používajú oznámené prostriedky elektronickej identifikácie alebo európske peňaženky digitálnej identity, členské štáty, ak konajú ako spoliehajúce sa strany, musia zabezpečiť priraďovanie záznamov.

„2. Členské štáty na účely poskytovania európskej peňaženky digitálnej identity musia do minimálneho súboru osobných identifikačných údajov uvedených v článku 12 ods. 4 písm. d) zahrnúť najmenej jeden jedinečný a trvalý identifikátor v súlade s právom Únie a vnútroštátnym právom na identifikáciu používateľa na jeho žiadosť v tých prípadoch, keď sa identifikácia používateľa vyžaduje podľa právnych predpisov.

„2a. Členské štáty stanovia technické a organizačné opatrenia na zabezpečenie vysokej úrovne ochrany osobných údajov používaných na priraďovanie záznamov a na zabránenie profilovaniu používateľov.

2aa. Členské štáty môžu v súlade s vnútroštátnym právom stanoviť, že používateľ európskej peňaženky digitálnej identity musí mať možnosť požiadať, aby sa jedinečný a trvalý identifikátor zahrnutý v minimálnom súbore osobných identifikačných údajov a spojený s peňaženkou v súlade s článkom 6a ods. 4 písm. e) nahradil iným jedinečným a trvalým identifikátorom, ktorý vydal členský štát.

„3. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia podrobnejšie vymedzí opatrenia uvedené v odseku 1 prostredníctvom vykonávacieho aktu. Tento vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

3a. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia stanoví podrobnosti opatrení uvedených v odsekoch 2 a 2aa prostredníctvom vykonávacieho aktu. Tento vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

13. Článok 12 sa mení takto:

Spolupráca a interoperabilita

a) V odseku 3 sa vypúšťa písmeno 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 osoby, právnickej osoby alebo fyzickej osoby zastupujúcej fyzické osoby alebo právnické osoby;“;

ba) V odseku 5 sa dopĺňa písmeno c):

„c) o podobný prístup k online službám, ktoré akceptujú používanie európskych peňaženiek digitálnej identity poskytovaných v súlade s týmto nariadením;“;

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, priraďovania záznamov a úrovní zabezpečenia;“;

ca) V odseku 6 sa dopĺňa písmeno e):

„e) vo výmene informácií, skúseností a osvedčených postupov a vydávaní usmernení, pokiaľ ide o to, ako online služby navrhovať, vyvíjať a vykonávať na účely využívania európskych digitálnych peňaženiek.“;

14. Vkladajú sa tieto články 12a a 12b:

„*Článok 12a*

Certifikácia schém elektronickej identifikácie

1. Zhoda schém elektronickej identifikácie, ktoré sa majú oznamovať, s požiadavkami stanovenými v tomto nariadení sa certifikuje na preukázanie súladu takýchto schém alebo ich častí s požiadavkami uvedenými v článku 8 ods. 2, pokiaľ ide o úroveň zabezpečenia schém elektronickej identifikácie v rámci príslušného systému certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 alebo jeho častí, pokiaľ sa certifikát kybernetickej bezpečnosti alebo jeho časti na požiadavky stanovené v článku 8 ods. 2 týkajúce sa úrovní zabezpečenia schém elektronickej identifikácie vzťahujú. Certifikácia nesmie presiahnuť päť rokov a je podmienená pravidelným dvojročným posúdením zraniteľnosti. Ak sa zistia zraniteľnosti a neodstránia sa do troch mesiacov, certifikácia sa zruší.

   Certifikáciu vykonávajú akreditované verejné alebo súkromné orgány posudzovania zhody určené členskými štátmi a v súlade s nariadením (ES) č. 765/2008.

„2. Partnerské preskúmanie schém elektronickej identifikácie uvedené v článku 12 ods. 6 písm. c) sa nevzťahuje na schémy elektronickej identifikácie alebo na časť takýchto schém, ktoré sú certifikované v súlade s odsekom 1.

„2a. Bez ohľadu na odsek 2 tohto článku môžu členské štáty od oznamujúceho členského štátu požadovať dodatočné informácie o schémach elektronickej identifikácie alebo ich časti certifikovaných podľa odseku 2 tohto článku.

„3. Členské štáty oznámia Komisii názvy a adresy verejných alebo súkromných subjektov, ktoré sú uvedené v odseku 1. Komisia sprístupní tieto informácie členským štátom.“;

„Článok 12b

Prístup k hardvérovým a softvérovým funkciám

Vydavatelia európskych peňaženiek digitálnej identity a vydavatelia oznámených prostriedkov elektronickej identifikácie konajúci v rámci obchodnej alebo odbornej činnosti a využívajúci základné platformové služby vymedzené v článku 2 ods. 2 nariadenia (EÚ) 2022/1925 na účely alebo počas poskytovania služieb európskej peňaženky digitálnej identity a prostriedkov elektronickej identifikácie koncovým používateľom sú komerčnými používateľmi v súlade s článkom 2 ods. 21 nariadenia (EÚ) 2022/1925.;

17. V článku 13 sa odsek 1 nahrádza takto:

„1. Bez ohľadu na odsek 2 tohto článku sú poskytovatelia dôveryhodných služieb zodpovední za škodu, ktorú spôsobia úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že nesplnia svoje povinnosti podľa tohto nariadenia.

Dôkazné bremeno týkajúce sa preukázania úmyslu alebo nedbanlivosti nekvalifikovaného poskytovateľa dôveryhodných služieb spočíva na fyzickej alebo právnickej osobe, ktorá žiada o náhradu škody uvedenej v prvom pododseku.

V prípade kvalifikovaného poskytovateľa dôveryhodných služieb sa škoda uvedená v prvom pododseku považuje za spôsobenú úmyselne alebo z nedbanlivosti, pokiaľ tento kvalifikovaný poskytovateľ dôveryhodných služieb nepreukáže opak.“;

18. Článok 14 sa nahrádza takto:

„*Článok 14*

Medzinárodné aspekty

1. Dôveryhodné služby, ktoré poskytujú poskytovatelia dôveryhodných služieb usadení v tretej krajine alebo medzinárodné inštitúcie, sa uznávajú za právne rovnocenné s kvalifikovanými dôveryhodnými službami, ktoré poskytujú kvalifikovaní poskytovatelia dôveryhodných služieb usadení v Únii, ak sú dôveryhodné služby s pôvodom z tretej krajiny alebo medzinárodnej organizácie uznané vykonávacím rozhodnutím alebo dohodou uzavretou medzi Úniou a treťou krajinou alebo medzinárodnou organizáciou v súlade s článkom 218 zmluvy.

2. Vykonávacie rozhodnutia a dohody uvedené v odseku 1 zabezpečia, aby poskytovatelia dôveryhodných služieb z tretej krajiny alebo medzinárodné organizácie, ako aj dôveryhodné služby, ktoré poskytujú, spĺňali požiadavky uplatniteľné na kvalifikovaných poskytovateľov dôveryhodných služieb usadených v Únii a kvalifikované dôveryhodné služby, ktoré poskytujú. Tretie krajiny a medzinárodné organizácie predovšetkým vytvoria, vedú a uverejňujú dôveryhodný zoznam uznaných poskytovateľov dôveryhodných služieb.

   Dohody uvedené v odseku 1 zabezpečia, aby kvalifikované dôveryhodné služby, ktoré poskytujú kvalifikovaní poskytovatelia dôveryhodných služieb usadení v Únii, sa uznávali ako právne rovnocenné s dôveryhodnými službami, ktoré poskytujú poskytovatelia dôveryhodných služieb z tretích krajín alebo medzinárodné organizácie, s ktorými sa dohoda uzatvára.

3. Vykonávacie rozhodnutia uvedené v odseku 1 sa prijímajú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

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 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) a orgány dohľadu určené podľa článku 17 tohto nariadenia v ostatných dotknutých členských štátoch. Ak informovaný orgán dohľadu usúdi, že zverejnenie narušenia bezpečnosti alebo integrity je vo verejnom záujme, informuje o ňom verejnosť, alebo o to požiada poskytovateľa dôveryhodných služieb;“;

2. Písmeno f) nahrádza takto:

„f) spolupracovať s príslušnými orgánmi dohľadu zriadenými podľa nariadenia (EÚ) 2016/679, najmä ich bez zbytočného odkladu informovať, ak sa zdá, že boli porušené pravidlá ochrany osobných údajov, a o narušeniach bezpečnosti, u ktorých sa zdá, že predstavujú porušenia 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 prijme usmernenia týkajúce sa vykonávania úloh uvedených v odseku 4 orgánmi dohľadu a prostredníctvom vykonávacích aktov prijatých v súlade s postupom preskúmania uvedeným v článku 48 ods. 2 vymedzí formáty a postupy pre správu uvedenú v odseku 6.“;

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]. Orgány dohľadu požiadajú príslušné vnútroštátne orgány podľa smernice XXXX/XXXX [NIS2], aby vykonali opatrenia dohľadu na overenie dodržiavania požiadaviek podľa smernice XXXX/XXXX [NIS2] zo strany poskytovateľov dôveryhodných služieb, aby od poskytovateľov dôveryhodných služieb vyžadovali nápravu akéhokoľvek nedodržania týchto požiadaviek, aby včas poskytli výsledky všetkých činností dohľadu spojených s poskytovateľmi dôveryhodných služieb a aby informovali 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. 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 prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

21a. Vkladá sa tento článok 19a:

„Požiadavky na nekvalifikovaných poskytovateľov dôveryhodných služieb“

„1. Nekvalifikovaný poskytovateľ dôveryhodných služieb, ktorý poskytuje nekvalifikované dôveryhodné služby:

a) má vhodné politiky a prijíma zodpovedajúce opatrenia na riadenie právnych, obchodných, prevádzkových a iných priamych alebo nepriamych rizík pre poskytovanie nekvalifikovanej dôveryhodnej služby. Bez ohľadu na ustanovenia článku 18 smernice EÚ XXXX/XXX [NIS2] tieto opatrenia zahŕňajú minimálne:

i) opatrenia týkajúce sa postupov registrácie a zapojenia sa do služby;

ii) opatrenia týkajúce sa procesných alebo administratívnych kontrol;

iii) opatrenia týkajúce sa riadenia a vykonávania služieb.

b) bez zbytočného odkladu a v každom prípade najneskôr do 24 hodín po tom, ako sa o nich dozvedel, oznámi orgánu dohľadu, identifikovateľným dotknutým osobám, verejnosti – ak je to vo verejnom záujme a prípadne iným relevantným príslušným orgánom všetky porušenia alebo narušenia poskytovania služby alebo vykonávania opatrení uvedených v písmene a) bodoch i), ii) a iii), ktoré majú významný vplyv na poskytovanú dôveryhodnú službu alebo osobné údaje, ktoré sa v nej uchovávajú.

„2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov upresní technické charakteristiky opatrení uvedených v odseku 1 písm. a). Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

22. Článok 20 sa mení takto:

a) Odsek 1 sa nahrádza takto:

„1. Orgán posudzovania zhody vykonáva aspoň každých 24 mesiacov audity kvalifikovaných poskytovateľov dôveryhodných služieb na ich vlastné náklady. Audit 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 výslednú správu o posúdení zhody orgánu dohľadu do troch pracovných dní od jej doručenia.“;

aa) Vkladá sa tento odsek:

„1a. Členské štáty môžu stanoviť, že kvalifikovaní poskytovatelia dôveryhodných služieb vopred informujú orgán dohľadu o plánovaných auditoch a na požiadanie umožnia orgánu dohľadu účasť ako pozorovateľa.“;

b) V odseku 2 sa posledná veta nahrádza takto:

„Ak sa zdá, že boli porušené predpisy týkajúce sa ochrany osobných údajov, orgán dohľadu bez zbytočného odkladu informuje príslušné 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 dotknutej službe, ktorú poskytuje, kvalifikovaný štatút.

3a. Ak príslušné vnútroštátne orgány informujú orgán dohľadu podľa smernice (EÚ) XXXX/XXXX [NIS2] o tom, že kvalifikovaný poskytovateľ dôveryhodných služieb nespĺňa niektorú z požiadaviek stanovených v článku 18 smernice (EÚ) XXXX/XXXX [NIS2], orgán dohľadu môže, berúc do úvahy najmä rozsah, trvanie a dôsledky tohto pochybenia, odňať príslušnému poskytovateľovi alebo dotknutej službe, ktorú poskytuje, kvalifikovaný štatút.

3b. Ak orgány dohľadu podľa nariadenia (EÚ) 2016/679 informujú orgán dohľadu o tom, že kvalifikovaný poskytovateľ dôveryhodných služieb nespĺňa niektorú z požiadaviek stanovených v nariadení (EÚ) 2016/679, orgán dohľadu môže, berúc do úvahy najmä rozsah, trvanie a dôsledky tohto pochybenia, odňať príslušnému poskytovateľovi alebo dotknutej službe, ktorú poskytuje, kvalifikovaný štatút.

3c. Orgán dohľadu informuje kvalifikovaného poskytovateľa dôveryhodných služieb o odňatí jeho kvalifikovaného štatútu alebo kvalifikovaného štatútu dotknutej služby. Orgán dohľadu informuje orgán uvedený v článku 22 ods. 3 na účely aktualizácie dôveryhodných zoznamov uvedených v článku 22 ods. 1 a príslušný vnútroštátny orgán uvedený v smernici XXXX [NIS2].

„4. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí technické špecifikácie a referenčné čísla noriem pre:

a) akreditáciu orgánov posudzovania zhody a správu o posúdení zhody uvedenú v odseku 1;

b) požiadavky na audit pre orgány posudzovania zhody na vykonávanie posudzovania zhody kvalifikovaných poskytovateľov dôveryhodných služieb uvedených v odseku 1;

c) systémy posudzovania zhody na vykonávanie posudzovania zhody kvalifikovaných poskytovateľov dôveryhodných služieb orgánmi posudzovania zhody a na poskytnutie správy uvedenej v odseku 1.

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 prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

23. Článok 21 sa mení takto:

„1. Ak majú poskytovatelia dôveryhodných služieb v úmysle začať poskytovať kvalifikovanú dôveryhodnú službu, predložia orgánu dohľadu oznámenie o svojom zámere spolu so správou o posúdení zhody vydanou orgánom posudzovania zhody, ktorou sa potvrdzuje splnenie požiadaviek stanovených v tomto nariadení a v článku 18 smernice (EÚ) XXXX/XXXX [NIS2].“;

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 bez zbytočného odkladu a najneskôr do dvoch mesiacov od doručenia tejto žiadosti príslušným orgánom uvedeným v smernici XXXX [NIS2]. Ak sa overovanie neukončí do dvoch mesiacov od oznámenia, príslušné orgány uvedené v smernici XXXX [NIS2] informujú orgán dohľadu a oznámia mu dôvody omeškania a lehotu, v ktorej sa overovanie má ukončiť.

Ak orgán dohľadu usúdi, že poskytovateľ dôveryhodných služieb a dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky stanovené v tomto nariadení, 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. 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 prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

25. Článok 24 sa mení takto:

a) Odsek 1 sa nahrádza takto:

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

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

a) prostredníctvom európskej peňaženky digitálnej identity alebo oznámených prostriedkov elektronickej identifikácie, ktoré spĺňajú požiadavky stanovené v článku 8, pokiaľ ide o úroveň zabezpečenia „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 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.“;

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 prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

c) Odsek 2 sa mení takto:

0. Písmeno a) sa mení takto:

„a) informuje orgán dohľadu aspoň jeden mesiac pred vykonaním akejkoľvek zmeny v poskytovaní svojich kvalifikovaných dôveryhodných služieb alebo aspoň tri mesiace v prípade zámeru tieto činnosti ukončiť. Orgán dohľadu môže pred udelením povolenia na vykonanie zamýšľaných zmien kvalifikovaných dôveryhodných služieb požiadať o dodatočné informácie alebo výsledok posúdenia zhody. 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.

1. Písmená d) a e) sa nahrádzajú 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;“;

„e) používa dôveryhodné systémy a produkty chránené proti pozmeneniu a zabezpečí technickú bezpečnosť a spoľahlivosť procesov, ktoré podporujú, vrátane používania vhodných kryptografických algoritmov, dĺžok kľúča a hašovacích funkcií v systémoch, produktoch a procesoch, ktoré podporujú;“;

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) bez zbytočného odkladu a v každom prípade najneskôr do 24 hodín po incidente, oznámi orgánu dohľadu, identifikovateľným dotknutým osobám, prípadne iným relevantným príslušným orgánom, na žiadosť orgánu dohľadu, verejnosti – ak je to vo verejnom záujme, všetky porušenia alebo narušenia poskytovania služby alebo vykonávania opatrení uvedených v písmene fa) bodoch i), ii) a iii), ktoré majú významný vplyv na poskytovanú dôveryhodnú službu alebo osobné údaje, ktoré sa v nej uchovávajú.

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 kvalifikovaných elektronických osvedčení atribútov.“;

e) Odsek 5 sa nahrádza takto:

„5. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí technické špecifikácie, postupy a referenčné čísla noriem pre požiadavky uvedené v odseku 2. Ak sú uvedené technické špecifikácie, postupy a normy splnené, predpokladá sa, že sa dosiahol súlad s požiadavkami stanovenými v tomto článku. 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 prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

f) Vkladá sa tento odsek 6:

„6. Komisia je splnomocnená prijímať vykonávacie akty, v ktorých sa vymedzujú technické charakteristiky opatrení uvedených v odseku 2 písm. fa).“;

25a) Článok 26 sa mení takto:

„2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí technické špecifikácie a referenčné čísla noriem pre zdokonalené elektronické podpisy. Ak zdokonalený elektronický podpis spĺňa tieto špecifikácie a normy, predpokladá sa, že sa dosiahol súlad s požiadavkami na zdokonalené elektronické podpisy. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

25a) Článok 27 sa mení takto:

Odsek 4 sa vypúšťa.

26. V článku 28 sa odsek 6 nahrádza takto:

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

27. V článku 29 sa dopĺňa tento nový odsek 1a:

„1a. Generovanie, správu údajov na vyhotovenie elektronického podpisu v mene podpisovateľa alebo duplikáciu týchto údajov na vyhotovenie podpisu na účely zálohovania 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 kvalifikovaného 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 môže duplikovať údaje na vyhotovenie elektronického podpisu len na účely zálohovania za predpokladu, že sú splnené tieto požiadavky:

i. bezpečnosť duplikovaných súborov údajov musí byť na rovnakej úrovni ako v prípade pôvodných súborov údajov;

ii. 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 vydanej podľa článku 30.

„2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí technické špecifikácie a referenčné čísla noriem na účely odseku 1.“;

29. V článku 30 sa vkladá tento odsek 3a:

„3a. Platnosť certifikácie uvedenej v odseku 1 nepresiahne 5 rokov a je podmienená pravidelným dvojročným posúdením zraniteľnosti. Ak sa zistia zraniteľnosti 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 prijmú 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 špecifikácie a 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 poskytne špecifikácie a referenčné čísla noriem na validáciu kvalifikovaných elektronických podpisov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

31a. Vkladá sa tento článok 32a:

Požiadavky na validáciu zdokonalených elektronických podpisov založených na kvalifikovaných certifikátoch

„1. Procesom validácie zdokonaleného elektronického podpisu založeného na kvalifikovanom certifikáte sa potvrdí platnosť zdokonaleného elektronického podpisu založeného na kvalifikovanom certifikáte, ak:

a) certifikát, ktorý potvrdzuje podpis, bol v čase podpísania kvalifikovaným certifikátom pre elektronický podpis v súlade s prílohou I;

b) kvalifikovaný certifikát vydal kvalifikovaný poskytovateľ dôveryhodných služieb a v čase podpísania bol platný;

c) údaje na validáciu podpisu zodpovedajú údajom poskytnutým spoliehajúcej sa strane;

d) sa jedinečný súbor údajov reprezentujúcich podpisovateľa v certifikáte správne poskytol spoliehajúcej sa strane;

e) sa použitie pseudonymu jasne oznámilo spoliehajúcej sa strane v prípade, že sa v čase podpísania použil pseudonym;

f) nebola narušená integrita podpísaných údajov;

g) v čase podpísania boli dodržané požiadavky stanovené v článku 26. Ak validácia zdokonalených elektronických podpisov založených na kvalifikovaných certifikátoch spĺňa špecifikácie a normy uvedené v odseku 3, predpokladá sa, že je v súlade s požiadavkami stanovenými v prvom pododseku.

„2. Systém použitý na validáciu zdokonaleného elektronického podpisu založeného na kvalifikovanom certifikáte poskytuje spoliehajúcej sa strane správny výsledok procesu validácie a umožňuje spoliehajúcej sa strane odhaliť akékoľvek problémy súvisiace s bezpečnosťou.

„3. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov poskytne špecifikácie a referenčné čísla noriem na validáciu zdokonalených elektronických podpisov založených na kvalifikovaných certifikátoch. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

31b. Článok 33 sa mení takto:

„1. Kvalifikovanú službu validácie kvalifikovaných elektronických podpisov môže poskytovať iba kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý:“;

„2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí technické špecifikácie a referenčné čísla noriem pre kvalifikovanú službu validácie uvedenú v odseku 1. Ak služba validácie kvalifikovaných elektronických podpisov spĺňa uvedené špecifikácie a normy, predpokladá sa, že je v súlade s požiadavkami stanovenými v odseku 1. Uvedené vykonávacie akty sa prijmú 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 špecifikácie a 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 technické špecifikácie a referenčné čísla noriem pre kvalifikovanú službu uchovávania kvalifikovaných elektronických podpisov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

32a. V článku 36 sa dopĺňa nový odsek 2:

„2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí technické špecifikácie a referenčné čísla noriem pre zdokonalené elektronické pečate.

Ak zdokonalená elektronická pečať spĺňa tieto špecifikácie a normy, predpokladá sa, že sa dosiahol súlad s požiadavkami na zdokonalené elektronické pečate. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

33. Článok 37 sa mení takto:

Odsek 4 sa vypúšťa.;

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 špecifikácie a 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 technické špecifikácie a referenčné čísla noriem pre kvalifikované certifikáty pre elektronické pečate. Uvedené vykonávacie akty sa prijmú 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 kvalifikovanej elektronickej pečate na diaľku

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

35a. Vkladá sa tento článok 40a:

„*Článok 40a*

Požiadavky na validáciu zdokonalených elektronických pečatí založených na kvalifikovaných certifikátoch

(1) Článok 32a sa uplatňuje mutatis mutandis na validáciu zdokonalených elektronických pečatí založených na kvalifikovaných certifikátoch.“;

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 špecifikácie a 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 technické špecifikácie a referenčné čísla noriem na spojenie dátumu a času s údajmi a pre presné zdroje času. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

36a. V článku 43 sa dopĺňa nový odsek 3:

„2a. Kvalifikovaná elektronická doručovacia služba pre registrované zásielky v jednom členskom štáte sa uznáva ako kvalifikovaná elektronická doručovacia služba pre registrované zásielky v ktoromkoľvek inom členskom štáte.“;

37. Článok 44 sa mení takto:

a) Vkladá sa tento odsek 1a:

„1a. Ak proces odosielania a doručovania údajov spĺňa špecifikácie a 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 technické špecifikácie a referenčné čísla noriem pre procesy odosielania a doručovania údajov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

c) Vkladajú sa tieto odseky 3 a 4:

3. Poskytovatelia kvalifikovaných elektronických doručovacích služieb pre registrované zásielky sa môžu dohodnúť na interoperabilite medzi kvalifikovanými elektronickými doručovacími službami pre registrované zásielky, ktoré poskytujú. Takýto rámec interoperability musí spĺňať požiadavky stanovené v odseku 1. Súlad potvrdzuje orgán posudzovania zhody.“;

„4. Komisia môže prostredníctvom vykonávacieho aktu stanoviť technické špecifikácie a referenčné čísla noriem s cieľom uľahčiť prenos údajov medzi dvoma alebo viacerými kvalifikovanými poskytovateľmi dôveryhodných služieb. Technické špecifikácie a obsah noriem musia byť nákladovo efektívne a primerané. Vykonávací akt sa prijme 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. Hodnotenie súladu s požiadavkami stanovenými v prílohe IV sa vykonáva v súlade so špecifikáciami a normami uvedenými v odseku 4.

„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.

„4. 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 a 2. Uvedené vykonávacie akty sa prijmú 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 alebo že nespĺňa požiadavky pre kvalifikované elektronické osvedčenia atribútov.

„2. Kvalifikované elektronické osvedčenie atribútov a osvedčenia atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene má rovnaký právny účinok ako zákonne vydané osvedčenia v papierovej forme.

„3. Kvalifikované elektronické osvedčenie atribútov vydané v jednom členskom štáte sa uznáva ako kvalifikované elektronické osvedčenie atribútov v ktoromkoľvek inom členskom štáte.

„4. Osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene sa uznáva ako osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj vo všetkých členských štátoch alebo v jeho mene.

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. V takom prípade sa akceptuje aj kvalifikované elektronické osvedčenie atribútov z iných členských štátov.

Článok 45c

Požiadavky na kvalifikované elektronické osvedčenie atribútov

„1. Kvalifikované elektronické osvedčenie atribútov musí spĺňať požiadavky stanovené v prílohe V.

„1a. Hodnotenie súladu s požiadavkami stanovenými v prílohe V sa vykonáva v súlade so špecifikáciami a normami uvedenými 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 technické špecifikácie a referenčné čísla noriem pre kvalifikované elektronické osvedčenia atribútov prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 11.

Článok 45d

Overovanie atribútov na základe autentických zdrojov

„1. Členské štáty do 24 mesiacov od nadobudnutia účinnosti vykonávacích aktov uvedených v článku 6a ods. 11 a článku 6c ods. 4 zabezpečia, aby sa aspoň v prípade atribútov uvedených v prílohe VI vždy, keď sa tieto atribúty využívajú autentické vo verejnom sektore, prijali opatrenia, ktoré kvalifikovaným poskytovateľom elektronických osvedčení atribútov umožnia na žiadosť používateľa overiť tieto atribúty elektronickými prostriedkami a 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. 11, stanoví minimálne technické špecifikácie, normy a postupy s odkazom na katalóg atribútov, systémy osvedčovania atribútov a overovacie postupy na kvalifikované elektronické osvedčovanie atribútov.

Článok 45da

Požiadavky na elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene.

„1. Elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene musí spĺňať tieto požiadavky:

a) požiadavky uvedené v prílohe VII;

b) kvalifikovaný certifikát podporujúci kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať subjektu verejného sektora uvedeného v článku 3 bode 45a, ktorý je určený ako vydavateľ uvedený v prílohe VII písm. b), musí obsahovať osobitný súbor certifikovaných atribútov vo forme vhodnej na automatizované spracovanie, v ktorom sa:

i) uvádza, že vydávajúci orgán je zriadený v súlade s vnútroštátnym právom alebo právom Únie ako orgán zodpovedný za autentický zdroj na základe ktorého sa vydáva elektronické osvedčenie atribútov, alebo ako orgán určený konať v jeho mene;

ii) poskytuje súbor údajov jednoznačne reprezentujúcich autentický zdroj uvedený v písmene i); a

iii) určuje vnútroštátne právo alebo právo Únie uvedené v písmene i).

„2. Členský štát, v ktorom sú subjekty verejného sektora uvedené v článku 3 bode 45a usadené, zabezpečí, aby subjekty verejného sektora, ktoré vydávajú elektronické osvedčenia atribútov, spĺňali rovnakú úroveň spoľahlivosti ako kvalifikovaní poskytovatelia dôveryhodných služieb v súlade s článkom 24.

„2a. Členské štáty oznámia Komisii subjekty verejného sektora uvedené v článku 3 bode 45a. Toto oznámenie zahŕňa správu o posúdení zhody vydanú orgánom posudzovania zhody, ktorou sa potvrdzuje, že požiadavky stanovené v odsekoch 1, 2 a 6 tohto článku sú splnené. Komisia prostredníctvom zabezpečeného kanálu sprístupňuje verejnosti zoznam subjektov verejného sektora uvedených v článku 3 bode 45a v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

„3. Ak bolo elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene po počiatočnom vydaní zrušené, stráca svoju platnosť okamihom zrušenia. Zrušený štatút elektronického osvedčenia sa po zrušení nesmie zmeniť na pôvodný.

„4. Elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene sa považuje za osvedčenie spĺňajúce požiadavky stanovené v odseku 1 tohto článku, ak spĺňa normy uvedené v odseku 5.

„5. Do 6 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia určí technické špecifikácie a referenčné čísla noriem pre elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 11.

5a. Do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia vymedzí formáty, postupy, špecifikácie a normy na účely odseku 2a prostredníctvom vykonávacieho aktu o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 6a ods. 11.

„6. Subjekty verejného sektora uvedené v článku 3 bode 45a vydávajúce elektronické osvedčenie atribútov poskytujú rozhranie s európskymi peňaženkami digitálnej identity poskytnutými v súlade s článkom 6a.

Článok 45e

Vydávanie elektronického osvedčenia atribútov európskym peňaženkám digitálnej identity

Poskytovatelia kvalifikovaných elektronických osvedčení atribútov poskytujú rozhranie s európskymi peňaženkami digitálnej identity poskytnutými 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 alebo ktoré ponúkajú ich obchodní partneri.

„2. Osobné údaje týkajúce sa poskytovania služieb elektronického osvedčovania atribútov sa uchovávajú logicky oddelene od ostatných údajov uchovávaných poskytovateľom elektronického osvedčenia atribútov.

„4. Poskytovatelia kvalifikovaných služieb elektronického osvedčovania atribútov zavedú funkčné oddelenie na poskytovanie takýchto služieb.

ODDIEL 10

ELEKTRONICKÉ ARCHIVAČNÉ SLUŽBY

Článok 45g

Právny účinok elektronickej archivačnej služby

„1. Právny účinok elektronických údajov uchovávaných prostredníctvom elektronickej archivačnej služby sa nesmie odmietnuť výlučne z dôvodu, že majú elektronickú formu alebo že nie sú uchované prostredníctvom kvalifikovanej elektronickej archivačnej služby.

„2. Na elektronické údaje uchovávané prostredníctvom kvalifikovanej elektronickej archivačnej služby sa vzťahuje domnienka ich integrity a pôvodu počas obdobia uchovávania kvalifikovaným poskytovateľom dôveryhodných služieb.

„3. Kvalifikovaná elektronická archivačná služba v jednom členskom štáte sa uznáva ako kvalifikovaná elektronická archivačná služba v ktoromkoľvek inom členskom štáte.

Článok 45ga

Požiadavky na kvalifikované elektronické archivačné služby

„1. Kvalifikované elektronické archivačné služby musia spĺňať tieto požiadavky:

a) poskytujú ich kvalifikovaní poskytovatelia dôveryhodných služieb;

b) využívajú postupy a technológie schopné predĺžiť trvácnosť a čitateľnosť elektronických údajov nad rámec obdobia technologickej platnosti a aspoň počas celého zákonného alebo zmluvného obdobia uchovávania pri zachovaní ich integrity a pôvodu;

c) zabezpečujú, aby sa elektronické údaje uchovávali tak, aby boli chránené pred stratou a zmenou, s výnimkou zmien týkajúcich sa ich nosiča alebo elektronického formátu;

d) umožňujú oprávneným spoliehajúcim sa stranám automatizovaným spôsobom prijať správu, ktorou sa potvrdí, že na elektronické údaje získané z kvalifikovaného elektronického archívu sa vzťahuje domnienka integrity údajov od začiatku obdobia uchovávania až do okamihu získania. Táto správa sa poskytuje spoľahlivým a účinným spôsobom a obsahuje kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať poskytovateľa kvalifikovanej elektronickej archivačnej služby.

„2. Do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia Komisia prostredníctvom vykonávacích aktov určí technické špecifikácie a referenčné čísla noriem pre kvalifikované elektronické archivačné služby. Ak kvalifikovaná elektronická archivačná služba spĺňa tieto špecifikácie a normy, predpokladá sa, že sa dosiahla súlad s požiadavkami na kvalifikované elektronické archivačné služby. Uvedené vykonávacie akty sa prijmú 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. Na záznamy údajov obsiahnuté v kvalifikovanom elektronickom registri sa vzťahuje domnienka ich jedinečného a presného sekvenčného chronologického poradia a ich integrity.

„3. Kvalifikovaný elektronický register v jednom členskom štáte sa uznáva ako kvalifikovaný elektronický register v ktoromkoľvek inom členskom štáte.

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) stanovujú pôvod záznamov údajov v registri;

c) zabezpečujú jedinečné sekvenčné chronologické poradie záznamov údajov v registri;

d) zaznamenávajú údaje takým spôsobom, aby bolo možné okamžite zistiť akúkoľvek následnú zmenu údajov, pričom po celý čas zabezpečujú ich integritu.

„2. Ak elektronický register spĺňa špecifikácie a normy uvedené v odseku 3, predpokladá sa, že je v súlade s požiadavkami stanovenými v odseku 1.

„3. Komisia prostredníctvom vykonávacích aktov určí technické špecifikácie a referenčné čísla noriem pre vytváranie a fungovanie kvalifikovaných elektronických registrov. Uvedené vykonávacie akty sa prijmú 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 po tom, ako sa začnú poskytovať na ich území.

„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) súhrnnú správu vrátane údajov o incidentoch, ktoré bránia používaniu európskej 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 31. 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 36 mesiacov po nadobudnutí jeho účinnosti. Komisia vyhodnotí najmä rozsah pôsobnosti článku 6 a článku 6db, ako aj to, či je vhodné zmeniť rozsah pôsobnosti tohto nariadenia alebo jeho konkrétne ustanovenia, pričom sa zohľadnia skúsenosti získané počas uplatňovania tohto nariadenia, ako aj dopyt zákazníkov, 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 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 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 36 mesiacov 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 24 mesiacov od nadobudnutia účinnosti tohto nariadenia.“.

„2a. Správa zariadení na vyhotovenie kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate na diaľku kvalifikovanými poskytovateľmi dôveryhodných služieb inými ako kvalifikovanými poskytovateľmi dôveryhodných služieb poskytujúcimi kvalifikované dôveryhodné služby na správu zariadení na vyhotovenie kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate na diaľku v súlade s článkami 29a a 39a sa naďalej akceptuje bez toho, aby bolo potrebné získať kvalifikovaný štatút na poskytovanie týchto služieb správy, a to do 24 mesiacov od nadobudnutia účinnosti tohto nariadenia.

2b. Kvalifikovaní poskytovatelia dôveryhodných služieb, ktorým bol udelený kvalifikovaný štatút podľa tohto nariadenia pred [dátum nadobudnutia účinnosti pozmeňujúceho nariadenia], ktorí používajú metódy overovania totožnosti na vydávanie kvalifikovaných certifikátov v súlade s článkom 24 ods. 1, predložia orgánu dohľadu správu o posúdení zhody preukazujúcu súlad s článkom 24 ods. 1 čo najskôr, najneskôr však do 30 mesiacov od nadobudnutia účinnosti pozmeňujúceho nariadenia. Až do predloženia tejto správy o posúdení zhody a do ukončenia jej posúdenia orgánom dohľadu môže kvalifikovaný poskytovateľ dôveryhodných služieb naďalej používať metódy overovania totožnosti stanovené v článku 24 ods. 1 nariadenia (EÚ) č. 910/2014.

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 52

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim 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	Za Radu
predseda/predsedníčka	predseda/predsedníčka

PRÍLOHA I

V prílohe I sa písmeno i) nahrádza takto:

„i) informácie o službách alebo lokalitu služieb, ktoré možno využiť na zistenie štatútu platnosti kvalifikovaného certifikátu;“.

PRÍLOHA II

POŽIADAVKY NA KVALIFIKOVANÉ ZARIADENIA NA VYHOTOVENIE ELEKTRONICKÝCH PODPISOV

„1. Kvalifikované zariadenia na vyhotovenie elektronických podpisov musia vhodnými technickými a procedurálnymi prostriedkami zabezpečovať prinajmenšom, aby:

(a) v primeranej miere bola zaručená dôvernosť údajov na vyhotovenie elektronického podpisu použitých na vyhotovenie elektronického podpisu;

(b) sa údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu mohli v praxi objaviť iba raz;

(c) údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu nebolo možné s primeranou úrovňou zabezpečenia odvodiť a elektronický podpis bol spoľahlivo chránený proti falšovaniu pomocou aktuálne dostupných technológií;

(d) oprávnený podpisovateľ mohol údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu spoľahlivo chrániť pred použitím inými osobami.

„2. Kvalifikované zariadenia na vyhotovenie elektronických podpisov nesmú meniť údaje, ktoré sa majú podpísať, ani brániť, aby sa takéto údaje podpisovateľovi pred podpísaním zobrazili.

PRÍLOHA III

V prílohe III sa písmeno i) nahrádza takto:

„i) informácie o službách alebo lokalitu služieb, ktoré možno využiť na zistenie štatútu platnosti kvalifikovaného certifikátu;“.

PRÍLOHA IV

V prílohe IV sa písmeno j) nahrádza takto:

„j) informácie o službách alebo lokalitu služieb súvisiacich so štatútom platnosti certifikátov, ktoré sa môžu využiť na zistenie štatútu platnosti kvalifikovaného certifikátu.“

PRÍLOHA V

POŽIADAVKY NA KVALIFIKOVANÉ ELEKTRONICKÉ OSVEDČENIE ATRIBÚTOV

Kvalifikované elektronické osvedčenie atribútov obsahuje:

(e) údaj, aspoň vo forme vhodnej na automatizované spracovanie, že osvedčenie bolo vydané ako kvalifikované elektronické osvedčenie atribútov;

(f) súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované elektronické osvedčenie atribútov, zahŕňajúci aspoň členský štát, v ktorom je poskytovateľ usadený, a:

– v prípade právnickej osoby: názov a prípadne registračné číslo tak, ako sa uvádza v úradných záznamoch,

– v prípade fyzickej osoby: meno osoby;

(g) súbor údajov jednoznačne reprezentujúcich subjekt, na ktorý sa osvedčené atribúty vzťahujú; ak sa použije pseudonym, musí to byť jasne uvedené;

(h) osvedčený atribút alebo atribúty, prípadne vrátane informácií potrebných na identifikáciu rozsahu týchto atribútov;

(i) údaje o začiatku a konci obdobia platnosti osvedčenia;

(j) identifikačný kód osvedčenia, ktorý musí byť jedinečný pre kvalifikovaného poskytovateľa dôveryhodných služieb, a v prípade potreby uvedenie systému osvedčení, ktorého je osvedčenie atribútov súčasťou;

(k) kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať vydávajúceho kvalifikovaného poskytovateľa dôveryhodných služieb;

(l) lokalitu, na ktorej je certifikát pre kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať podľa písmena g) dostupný bezplatne;

(m) informácie o službách alebo lokalitu služieb, ktoré možno využiť na zistenie štatútu platnosti kvalifikovaného osvedčenia.

PRÍLOHA VI

MINIMÁLNY ZOZNAM ATRIBÚTOV

V nadväznosti na článok 45d členské štáty zabezpečia, aby sa prijali opatrenia, ktoré kvalifikovaným poskytovateľom elektronických osvedčení atribútov umožnia na žiadosť používateľa elektronickými prostriedkami overiť pravosť týchto atribútov na základe príslušného autentického zdroja na vnútroštátnej úrovni alebo prostredníctvom určených sprostredkovateľov uznaných na vnútroštátnej úrovni v súlade s vnútroštátnym právom alebo právom Únie a v prípadoch, keď sa tieto atribúty opierajú o autentické zdroje vo verejnom sektore:

1. adresa;
2. vek;
3. pohlavie;
4. osobný stav;
5. zloženie rodiny;
6. štátna príslušnosť alebo občianstvo;
7. vzdelanie, tituly a oprávnenia;
8. odborná kvalifikácia, tituly a oprávnenia;
9. verejné povolenia a licencie;
10. finančné údaje a údaje o spoločnostiach.

PRÍLOHA VII

POŽIADAVKY NA ELEKTRONICKÉ OSVEDČENIE ATRIBÚTOV VYDANÉ VEREJNÝM SUBJEKTOM ZODPOVEDNÝM ZA AUTENTICKÝ ZDROJ ALEBO V JEHO MENE

Elektronické osvedčenie atribútov vydané verejným subjektom zodpovedným za autentický zdroj alebo v jeho mene obsahuje:

a) údaj, aspoň vo forme vhodnej na automatizované spracovanie, že osvedčenie bolo vydané ako elektronické osvedčenie atribútov vydané verejným orgánom zodpovedným za autentický zdroj alebo v jeho mene;
b) súbor údajov jednoznačne reprezentujúcich verejný subjekt, ktorý elektronické osvedčenie atribútov vydáva, zahŕňajúci aspoň členský štát, v ktorom je tento verejný subjekt usadený, jeho názov a prípadne jeho registračné číslo, ako sa uvádza v úradných záznamoch;
c) súbor údajov jednoznačne reprezentujúcich subjekt, na ktorý sa osvedčené atribúty vzťahujú; ak sa použije pseudonym, musí to byť jasne uvedené;
d) osvedčený atribút alebo atribúty, prípadne vrátane informácií potrebných na identifikáciu rozsahu týchto atribútov;
e) údaje o začiatku a konci obdobia platnosti osvedčenia;
f) identifikačný kód osvedčenia, ktorý musí byť jedinečný pre vydávajúci verejný subjekt, a v prípade potreby uvedenie systému osvedčení, ktorého je osvedčenie atribútov súčasťou;
g) kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať vydávajúceho subjektu;
h) lokalitu, na ktorej je certifikát pre kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať podľa písmena g) dostupný bezplatne;
i) informácie o službách alebo lokalitu služieb, ktoré možno využiť na zistenie štatútu platnosti osvedčenia.