EURÓPSKA ÚNIA

EURÓPSKY PARLAMENT **RADA**

V Bruseli 13. marca 2024
(OR. en)

2021/0136 (COD) **PE-CONS 68/23**

TELECOM 351
COMPET 1163
MI 1028
DATAPROTECT 329
JAI 1550
CODEC 2237

LEGISLATÍVNE AKTY A INÉ PRÁVNE AKTY

Predmet:	NARIADENIE EURÓPSKEHO PARLAMENTU A RADY, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2024/…

z ...,

ktorým sa mení nariadenie (EÚ) č. 910/2014,
pokiaľ ide o zriadenie európskeho rámca digitálnej identity

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],

so zreteľom na stanovisko Výboru regiónov[2],

konajúc v súlade s riadnym legislatívnym postupom[3],

---

1 Ú. v. EÚ C 105, 4.3.2022, s. 81.
2 Ú. v. EÚ C 61, 4.2.2022, s. 42.
3 Pozícia Európskeho parlamentu z 29. februára 2024 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z ... .

keďže:

(1) V oznámení Komisie z 19. februára 2020 s názvom „Formovanie digitálnej budúcnosti Európy“ sa ohlasuje revízia nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014[4] s cieľom zlepšiť jeho účinnosť, rozšíriť jeho prínosy na súkromný sektor a podporiť dôveryhodné digitálne identity pre všetkých Európanov.

(2) Európska rada vo svojich záveroch z 1. a 2. októbra 2020 vyzvala Komisiu, aby navrhla vytvorenie rámca Únie 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 politickom programe Digitálne desaťročie do roku 2030, ktorý sa zriadil rozhodnutím Európskeho parlamentu a Rady (EÚ) 2022/2481[5], sa stanovujú všeobecné a digitálne ciele rámca Únie, ktoré majú do roku 2030 viesť k rozsiahlemu zavádzaniu dôveryhodnej, dobrovoľnej a používateľsky kontrolovanej digitálnej identity, ktorá je uznávaná v celej Únii a umožňuje každému používateľovi kontrolovať svoje údaje v online interakciách.

---

[4] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).

[5] Rozhodnutie Európskeho parlamentu a Rady (EÚ) 2022/2481 zo 14. decembra 2022, ktorým sa zriaďuje politický program digitálne desaťročie do roku 2030 (Ú. v. EÚ L 323, 19.12.2022, s. 4).

(4) V Európskom vyhlásení o digitálnych právach a zásadách v digitálnom desaťročí, ktoré vydali Európsky parlament, Rada a Komisia[6] (ďalej len „vyhlásenie“), sa zdôrazňuje právo každého na prístup k digitálnym technológiám, produktom a službám, ktoré sú navrhnuté tak, aby boli bezpečné a chránené a aby chránili súkromie. Zahŕňa to aj zabezpečenie toho, aby sa všetkým ľuďom žijúcim v Únii ponúkla prístupná, bezpečná a dôveryhodná digitálna identita, ktorá umožní prístup k širokej škále online a offline služieb chránených pred rizikami kybernetickej bezpečnosti a počítačovou kriminalitou vrátane porušenia ochrany údajov a krádeže alebo manipulácie totožnosti. Vo vyhlásení sa tiež uvádza, že každý má právo na ochranu svojich osobných údajov. Toto právo zahŕňa kontrolu nad tým, ako sa údaje používajú a komu sa poskytujú.

(5) Občania Únie a osoby s pobytom v Únii by mali mať právo na digitálnu identitu, ktorá je pod ich výlučnou kontrolou a ktorá im umožňuje uplatňovať si práva v digitálnom prostredí a zúčastňovať sa na digitálnom hospodárstve. Na dosiahnutie tohto cieľa by sa mal zriadiť európsky rámec digitálnej identity, ktorý by občanom Únie a osobám s pobytom v Únii umožnil prístup k verejným a súkromným online a offline službám v celej Únii.

(6) Harmonizovaný rámec digitálnej identity by mal prispieť k vytvoreniu digitálne integrovanejšej Únie, pretože by zmenšil digitálne prekážky medzi členskými štátmi, umožnil by občanom Únie a osobám s pobytom v Únii využívať výhody digitalizácie a zároveň by zvýšil transparentnosť a ochranu ich práv.

---

[6] Ú. v. EÚ C 23, 23.1.2023, s. 1.

(7) Harmonizovanejší prístup k elektronickej identifikácii by mal znížiť riziká a náklady vyplývajúce zo súčasnej fragmentácie, ktorú spôsobuje používanie rozdielnych vnútroštátnych riešení alebo v niektorých členských štátoch neexistencia takýchto riešení elektronickej identifikácie. Takýmto prístupom by sa mal posilniť vnútorný trh tým, že sa občanom Únie, osobám s pobytom v Únii v zmysle vnútroštátneho práva a podnikom umožní identifikovať sa a poskytovať autentifikáciu svojej totožnosti online aj offline bezpečným, dôveryhodným, používateľsky ústretovým, pohodlným, prístupným a harmonizovaným spôsobom v celej Únii. Európska peňaženka digitálnej identity by mala fyzickým a právnickým osobám v celej Únii poskytnúť 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 prostredníctvom zlepšeného ekosystému dôveryhodných služieb a prostredníctvom overených dôkazov totožnosti a elektronických osvedčení atribútov, ako sú napríklad akademické kvalifikácie vrátane vysokoškolských titulov alebo iné dosiahnuté formy vzdelania alebo odbornej kvalifikácie. Cieľom európskeho rámca digitálnej identity je dosiahnuť posun od výlučného využívania vnútroštátnych riešení digitálnej identity k poskytovaniu elektronických osvedčení atribútov platných a právne uznávaných v celej Únii. Poskytovatelia elektronických osvedčení atribútov by mali profitovať z jasného a jednotného súboru pravidiel, zatiaľ čo verejné orgány by mali mať možnosť využívať elektronické dokumenty v určitom stanovenom formáte.

(8) Niekoľko členských štátov zaviedlo a využíva prostriedky elektronickej identifikácie, ktoré akceptujú poskytovatelia služieb v Únii. Okrem toho sa na základe nariadenia (EÚ) č. 910/2014 realizovali investície do vnútroštátnych aj cezhraničných riešení, ktoré zahŕňajú aj interoperabilitu oznámených schém elektronickej identifikácie podľa uvedeného nariadenia. Očakáva sa, že v záujme zaručenia komplementárnosti a rýchleho prijatia európskych peňaženiek digitálnej identity súčasnými používateľmi oznámených prostriedkov elektronickej identifikácie a v záujme minimalizovania vplyvu na existujúcich poskytovateľov služieb budú európske peňaženky digitálnej identity ťažiť zo skúseností, ktoré sa získali v súvislosti s existujúcimi prostriedkami elektronickej identifikácie, a z využívania infraštruktúry oznámených schém elektronickej identifikácie zavedených na úrovni Únie a na vnútroštátnej úrovni.

(9) Na všetky činnosti spracúvania osobných údajov podľa nariadenia (EÚ) č. 910/2014 sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679[7] a v relevantných prípadoch smernica Európskeho parlamentu a Rady 2002/58/ES[8]. V súlade s uvedenými pravidlami sú aj riešenia, ktoré sú súčasťou rámca interoperability stanoveného v tomto nariadení. V práve Únie v oblasti ochrany údajov sa stanovujú zásady ochrany údajov, ako je zásada minimalizácie údajov a obmedzenia účelu, a povinnosti, ako je špecificky navrhnutá a štandardná ochrana údajov.

---

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

[8] Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

(10) Na podporu konkurencieschopnosti podnikov v Únii by poskytovatelia online aj offline služieb mali mať možnosť využívať riešenia digitálnej identity uznávané v celej Únii bez ohľadu na členský štát, v ktorom sa tieto riešenia poskytujú, a tak profitovať z harmonizovaného únijného prístupu k dôvere, bezpečnosti a interoperabilite. Používatelia aj poskytovatelia služieb by mali mať možnosť využívať výhody, ktoré prináša rovnaká právna sila elektronických osvedčení atribútov v celej Únii. Harmonizovaný rámec digitálnej identity má vytvárať hospodársku hodnotu poskytovaním jednoduchšieho prístupu k tovaru a službám, výrazným znížením prevádzkových nákladov spojených s postupmi elektronickej identifikácie a autentifikácie, napríklad počas pripájania nových zákazníkov, obmedzením potenciálu páchať počítačovú kriminalitu, ako je krádež totožnosti, krádež údajov a online podvody, čím sa podporí zvýšenie efektívnosti a bezpečná digitálna transformácia mikropodnikov a malých a stredných podnikov (ďalej len „MSP“) v Únii.

(11) Európske peňaženky digitálnej identity by mali uľahčiť uplatňovanie zásady „jedenkrát a dosť“, a tým znížiť administratívne zaťaženie občanov Únie, osôb s pobytom v Únii a podnikov v celej Únii, podporiť ich cezhraničnú mobilitu a posilniť rozvoj interoperabilných služieb elektronickej verejnej správy v celej Únii.

(12) Na spracúvanie osobných údajov pri vykonávaní tohto nariadenia sa vzťahuje nariadenie (EÚ) 2016/679, nariadenie Európskeho parlamentu a Rady a (EÚ) 2018/1725[9] a smernica 2002/58/ES. V tomto nariadení by sa preto mali stanoviť osobitné záruky, aby sa poskytovateľom prostriedkov elektronickej identifikácie a elektronického osvedčenia atribútov zabránilo spájať osobné údaje, ktoré získavajú pri poskytovaní iných služieb, s osobnými údajmi, ktoré spracúvajú na účely poskytovania služieb, ktoré patria do rozsahu pôsobnosti tohto nariadenia. Osobné údaje súvisiace s poskytovaním európskych peňaženiek digitálnej identity by sa mali uchovávať logicky oddelene od všetkých ostatných údajov, ktoré uchováva poskytovateľ európskej peňaženky digitálnej identity. Toto nariadenie by poskytovateľom európskych peňaženiek digitálnej identity nemalo brániť v tom, aby uplatňovali dodatočné technické opatrenia, ktoré prispievajú k ochrane osobných údajov, ako je fyzické oddelenie osobných údajov súvisiacich s poskytovaním európskych peňaženiek digitálnej identity od všetkých ostatných údajov, ktoré uchováva poskytovateľ. Bez toho, aby bolo dotknuté nariadenie (EÚ) 2016/679, sa v tomto nariadení bližšie špecifikuje uplatňovanie zásad obmedzenia účelu, minimalizácie údajov a špecificky navrhnutej a štandardnej ochrany údajov.

---

[9] 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).

(13) Európske peňaženky digitálnej identity by mali mať zabudovanú funkciu spoločného prehľadu, aby sa zabezpečila vyššia miera transparentnosti a súkromia a aby mali používatelia väčšiu kontrolu nad svojimi osobnými údajmi. Uvedená funkcia by mala poskytovať jednoduché a používateľsky ústretové rozhranie s prehľadom o všetkých spoliehajúcich sa stranách, s ktorým používateľ zdieľa údaje, vrátane atribútov a druhu údajov zdieľaných s jednotlivými spoliehajúcimi sa stranami. Mala by používateľom umožniť sledovať všetky transakcie vykonané prostredníctvom európskej peňaženky digitálnej identity aspoň s týmito údajmi: čas a dátum transakcie, identifikácia protistrany, požadované osobné údaje a zdieľané údaje. Tieto informácie by sa mali uchovávať aj v prípade, že sa transakcia neuzavrela. Pravosť informácií obsiahnutých v histórii transakcií by nemalo byť možné poprieť. Takáto funkcia by mala byť automaticky aktívna. Používateľom by to malo umožniť priamo prostredníctvom európskej peňaženky digitálnej identity jednoducho požiadať, aby spoliehajúca sa strana bezodkladne vymazala osobné údaje podľa článku 17 nariadenia (EÚ) 2016/679, a jednoducho nahlásiť spoliehajúcu sa stranu príslušnému vnútroštátnemu orgánu pre ochranu údajov, ak dostanú údajne nezákonnú alebo podozrivú žiadosť o osobné údaje.

(14) Členské štáty by mali do európskej peňaženky digitálnej identity začleniť rôzne technológie na ochranu súkromia, ako je dôkaz s nulovou znalosťou. Tieto kryptografické metódy by mali umožniť spoliehajúcej sa strane validovať, či je vyhlásenie založené na identifikačných údajoch a osvedčení atribútov danej osoby pravdivé bez toho, aby sa odhalili akékoľvek údaje, na ktorých je toto vyhlásenie založené, čím sa zachová súkromie používateľa.

(15) V tomto nariadení sa stanovujú harmonizované podmienky na vytvorenie rámca pre európske peňaženky digitálnej identity, ktoré majú poskytovať členské štáty. Všetci občania Únie a osoby s pobytom v Únii v zmysle vymedzenia vo vnútroštátnom práve by mali byť oprávnení bezpečne požadovať, vyberať, kombinovať, uchovávať, vymazávať, zdieľať a prezentovať údaje súvisiace s ich totožnosťou a požadovať vymazanie svojich osobných údajov používateľsky ústretovým a pohodlným spôsobom, pod výlučnou kontrolou používateľa, a zároveň by mali byť oprávnení umožniť selektívne zverejnenie osobných údajov. Týmto nariadením sa zohľadňujú spoločné európske hodnoty a rešpektujú základné práva, právne záruky a zodpovednosť, čím sa poskytuje ochrana demokratickým spoločnostiam, občanom Únie a osobám s pobytom v Únii. Technológie, ktoré sa použijú na dosiahnutie týchto cieľov, by sa mali vyvíjať v záujme dosiahnutia najvyššej úrovne bezpečnosti, súkromia, jednoduchosti používania, dostupnosti, širokej použiteľnosti a bezproblémovej interoperability. Členské štáty by mali zabezpečiť pre všetkých svojich občanov a osoby s pobytom na ich území rovnaký prístup k elektronickej identifikácii. Členské štáty by nemali priamo ani nepriamo obmedzovať prístup k verejným alebo súkromným službám pre fyzické alebo právnické osoby, ktoré sa nerozhodnú používať európske peňaženky digitálnej identity, a mali by sprístupniť vhodné alternatívne riešenia.

(16) Členské štáty by mali využívať možnosti, ktoré ponúka toto nariadenie, na to, aby na vlastnú zodpovednosť poskytovali európske peňaženky digitálnej identity na používanie fyzickým a právnickým osobám s pobytom na ich území. S cieľom poskytnúť členským štátom flexibilitu a využiť najmodernejšie technológie by toto nariadenie malo umožňovať, aby európske peňaženky digitálnej identity poskytoval priamo členský štát, aby sa poskytovali na základe mandátu členského štátu alebo nezávisle od členského štátu, avšak na základe jeho uznania.

(17) Na účely registrácie by spoliehajúce sa strany mali poskytnúť informácie potrebné na ich elektronickú identifikáciu a autentifikáciu vo vzťahu k európskym peňaženkám digitálnej identity. Pri deklarovaní zamýšľaného ich použitia európskej peňaženky digitálnej identity by spoliehajúce sa strany mali poskytnúť informácie o údajoch, ktoré môžu požadovať na účely poskytovania svojich služieb, ako aj dôvod ich požadovania. Registrácia spoliehajúcej sa strany členským štátom uľahčí overovanie zákonnosti činností spoliehajúcich sa strán v súlade s právom Únie. Povinnosťou registrácie stanovenou v tomto nariadení by nemali byť dotknuté povinnosti stanovené v iných právnych predpisoch Únie alebo vnútroštátnych právnych predpisoch, ako sú informácie, ktoré sa majú poskytnúť dotknutým osobám podľa nariadenia (EÚ) 2016/679. Spoliehajúce sa strany by mali dodržiavať záruky stanovené v článkoch 35 a 36 uvedeného nariadenia, a to najmä vykonávaním posúdení vplyvu na ochranu údajov a konzultáciami s príslušnými orgánmi pre ochranu údajov pred spracúvaním údajov, ak z posúdení vplyvu na ochranu údajov vyplýva, že spracúvanie povedie k vysokému riziku. Takéto záruky by mali podporovať zákonné spracúvanie osobných údajov spoliehajúcimi sa stranami, najmä ak ide o osobitné kategórie údajov, ako sú napríklad zdravotné údaje. Cieľom registrácie spoliehajúcich sa strán je zvýšiť transparentnosť a dôveru v používanie európskych peňaženiek digitálnej identity. Registrácia by mala byť nákladovo efektívna a primeraná súvisiacim rizikám, aby sa zabezpečilo jej využívanie poskytovateľmi služieb. V tejto súvislosti by sa v rámci registrácie malo zabezpečiť využívanie automatizovaných postupov, čo zahŕňa aj spoliehanie sa na existujúce registre a ich využívanie členskými štátmi, a nemal by sa uplatňovať postup predbežného povoľovania. Proces registrácie by mal umožňovať rôzne prípady použitia, ktoré sa môžu líšiť z hľadiska spôsobu prevádzky, či už online alebo v offline režime, alebo z hľadiska požiadavky na autentifikáciu zariadení na účely prepojenia s európskou peňaženkou digitálnej identity. Registrácia by sa mala vzťahovať výlučne na spoliehajúce sa strany, ktoré poskytujú služby prostredníctvom digitálnej interakcie.

(18) Ochrana občanov Únie a osôb s pobytom v Únii pred neoprávneným alebo podvodným používaním európskych peňaženiek digitálnej identity má veľký význam pre zabezpečenie dôvery v európske peňaženky digitálnej identity a pre ich široké využívanie. Používateľom by sa mala pred takýmto zneužitím poskytnúť účinná ochrana. Najmä ak skutkovú podstatu podvodného alebo inak nezákonného používania európskej peňaženky digitálnej identity stanoví vnútroštátny súdny orgán v kontexte iného konania, orgány dohľadu, ktoré sú zodpovedné za vydavateľov európskej peňaženky digitálnej identity, by mali po oznámení prijať potrebné opatrenia na zabezpečenie toho, aby sa registrácia danej spoliehajúcej sa strany a jej začlenenie do mechanizmu autentifikácie zrušili alebo pozastavili dovtedy, kým oznamujúci orgán nepotvrdí, že zistené nezrovnalosti boli odstránené.

(19) Všetky európske peňaženky digitálnej identity by mali používateľom umožňovať cezhraničnú elektronickú identifikáciu a autentifikáciu online aj v offline režime na účely získania prístupu k širokej škále verejných a súkromných služieb. Bez toho, aby boli dotknuté výhradné práva členských štátov, pokiaľ ide o identifikáciu ich občanov a osôb s pobytom na ich území, európske peňaženky digitálnej identity môžu slúžiť aj na inštitucionálne potreby orgánov verejnej správy, medzinárodných organizácií a inštitúcií, orgánov, úradov a agentúr Únie. Autentifikácia v offline režime by bola dôležitá v mnohých odvetviach vrátane zdravotníctva, kde sa služby často poskytujú prostredníctvom osobnej interakcie, a v prípade elektronických receptov by mala existovať možnosť využívať na overenie pravosti kódy QR alebo podobné technológie. S cieľom splniť bezpečnostné požiadavky podľa tohto nariadenia by európske peňaženky digitálnej identity, ktoré sa spoliehajú na úroveň zabezpečenia „vysoká“ z hľadiska schém elektronickej identifikácie, mali využívať potenciál, ktorý ponúkajú riešenia odolné proti neoprávnenej manipulácii, ako sú napríklad bezpečnostné prvky. Európske peňaženky digitálnej identity by mali používateľom takisto umožniť vytvárať a používať kvalifikované elektronické podpisy a pečate akceptované v celej Únii. Po pripojení sa na európsku peňaženku digitálnej identity by fyzické osoby mali mať možnosť štandardne a bezplatne používať túto peňaženku na podpisovanie kvalifikovanými elektronickými podpismi bez toho, aby museli absolvovať akékoľvek dodatočné administratívne postupy. Používatelia by mali mať možnosť podpisovať alebo pečatiť vlastné tvrdenia alebo vlastné atribúty. V záujme dosiahnutia výhod zo zjednodušenia a zníženia nákladov pre osoby a podniky v celej Únii, okrem iného aj umožnením vydávania oprávnení na zastupovanie a elektronických mandátov, by členské štáty mali poskytovať európske peňaženky digitálnej identity, ktoré sú založené na spoločných normách a technických špecifikáciách, aby sa zabezpečila bezproblémová interoperabilita a primerane sa zvýšila bezpečnosť informačných technológií, posilnila odolnosť proti kybernetickým útokom, a tým výrazne znížili potenciálne riziká, ktoré z prebiehajúcej digitalizácie vyplývajú pre občanov Únie, osoby s pobytom v Únii a pre podniky.

Len príslušné orgány členských štátov môžu poskytnúť vysokú úroveň 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 skutočne danou osobou. Je preto potrebné, aby sa poskytovanie európskych peňaženiek digitálnej identity opieralo o právnu identitu občanov Únie, osôb s pobytom v Únii alebo právnických osôb. Opieranie sa o právnu identitu by nemalo používateľom európskej peňaženky digitálnej identity brániť v prístupe k službám na základe pseudonymu, ak sa na autentifikáciu nevzťahuje právna požiadavka na právnu identitu. Dôvera v európske peňaženky digitálnej identity by sa posilnila, ak by vydávajúce a spravujúce strany boli v súlade s nariadením (EÚ) 2016/679 povinné zaviesť primerané technické a organizačné opatrenia na zabezpečenie najvyššej úrovne bezpečnosti, ktorá zodpovedá rizikám, ktoré vznikajú v súvislosti s právami a slobodami fyzických osôb.

(20) Používanie kvalifikovaného elektronického podpisu na neprofesionálne účely by malo byť pre všetky fyzické osoby bezplatné. Členským štátom by sa malo umožniť zavádzať opatrenia na zabránenie používania kvalifikovaných elektronických podpisov pre fyzické osoby na profesionálne účely bezplatne, a zároveň zabezpečiť, aby boli všetky takéto opatrenia primerané zisteným rizikám a aby boli odôvodnené.

(21) Je vhodné 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 by na dosiahnutie tohto cieľa mali mať možnosť stanoviť právne a organizačné opatrenia s cieľom zvýšiť flexibilitu pre poskytovateľov európskych peňaženiek digitálnej identity a umožniť dodatočné funkcie európskych peňaženiek digitálnej identity popri tých, ktoré sú stanovené v tomto nariadení, a to aj prostredníctvom zvýšenej interoperability s existujúcimi vnútroštátnymi prostriedkami elektronickej identifikácie. Takéto dodatočné funkcie by nemali byť v žiadnom prípade na úkor poskytovania základných funkcií európskych peňaženiek digitálnej identity stanovených v tomto nariadení, ani by nemali presadzovať existujúce vnútroštátne riešenia namiesto 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.

(22) Európske peňaženky digitálnej identity by mali zahŕňať funkciu vytvárania pseudonymov, ktoré si vyberá a spravuje používateľ, na účely autentifikácie pri prístupe k online službám.

(23) S cieľom dosiahnuť vysokú úroveň bezpečnosti a dôveryhodnosti sa týmto nariadením stanovujú požiadavky na európske peňaženky digitálnej identity. Súlad európskych peňaženiek digitálnej identity s týmito požiadavkami by mali certifikovať akreditované orgány posudzovania zhody určené členskými štátmi.

(24) S cieľom zabrániť rozdielnym prístupom a harmonizovať vykonávanie požiadaviek stanovených v tomto nariadení by Komisia mala na účely certifikácie európskych peňaženiek digitálnej identity prijať vykonávacie akty s cieľom stanoviť zoznam referenčných noriem a v prípade potreby stanoviť špecifikácie a postupy na účely vyjadrenia podrobných technických špecifikácií týchto požiadaviek. Pokiaľ sa na certifikáciu súladu európskych peňaženiek digitálnej identity s príslušnými požiadavkami kybernetickej bezpečnosti nevzťahujú existujúce schémy certifikácie kybernetickej bezpečnosti uvedené v tomto nariadení a pokiaľ ide o iné ako kybernetickobezpečnostné požiadavky relevantné pre európske peňaženky digitálnej identity, členské štáty by mali zaviesť vnútroštátne schémy certifikácie podľa harmonizovaných požiadaviek stanovených v tomto nariadení a prijatých podľa neho. Členské štáty by mali zaslať svoje návrhy vnútroštátnych schém certifikácie skupine pre európsku spoluprácu v oblasti digitálnej identity, ktorá by mala môcť vydávať stanoviská a odporúčania.

(25) Certifikácia súladu s požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení by sa mala, pokiaľ možno, opierať o príslušné európske schémy certifikácie kybernetickej bezpečnosti zriadené podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881[10], ktorým sa zriaďuje dobrovoľný európsky rámec certifikácie kybernetickej bezpečnosti produktov, procesov a služieb informačných a komunikačných technológií.

---

[10] 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).

(26) S cieľom priebežne posudzovať a zmierňovať riziká spojené s bezpečnosťou by certifikované európske peňaženky digitálnej identity mali podliehať pravidelným posúdeniam zraniteľnosti s cieľom odhaliť akúkoľvek zraniteľnosť v certifikovaných zložkách európskej peňaženky digitálnej identity súvisiacich s produktom, postupom a službou.

(27) Ochranou používateľov a podnikov pred kybernetickobezpečnostnými rizikami prispievajú základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení aj k posilneniu ochrany osobných údajov a súkromia jednotlivcov. Prostredníctvom spolupráce medzi Komisiou, európskymi normalizačnými organizáciami, Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA), Európskym výborom pre ochranu údajov zriadeným nariadením (EÚ) 2016/679 a vnútroštátnymi orgánmi dohľadu pre ochranu údajov by sa mali zvážiť synergie v oblasti normalizácie a certifikácie aspektov kybernetickej bezpečnosti.

(28) Pripájanie občanov Únie a osôb s pobytom v Únii k európskej peňaženke digitálnej identity by sa malo uľahčiť využívaním prostriedkov elektronickej identifikácie vydaných na úrovni záruky „vysoká“. Prostriedky elektronickej identifikácie vydané na úrovni záruky „významná“ by sa mali využívať len vtedy, keď harmonizované technické špecifikácie a postupy využívajúce prostriedky elektronickej identifikácie vydané na úrovni záruky „významná“ v kombinácii s doplnkovými prostriedkami overenia totožnosti umožnia splnenie požiadaviek stanovených v tomto nariadení, pokiaľ ide o úroveň záruky „vysoká“. Takéto doplnkové prostriedky by mali byť spoľahlivé a ľahko použiteľné a mohli by vychádzať z možnosti používať postupy diaľkového pripojenia, kvalifikované certifikáty podložené kvalifikovanými elektronickými 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 špecifikácie a postupy pre pripojenie používateľov pomocou prostriedkov elektronickej identifikácie vrátane tých, ktoré boli vydané na úrovni záruky „významná“.

(29) Cieľom tohto nariadenia je poskytnúť používateľovi plne mobilnú, bezpečnú a používateľsky ústretovú európsku peňaženku digitálnej identity. S cieľom preukázať súlad s príslušnými požiadavkami tohto nariadenia, pokiaľ ide o úroveň zabezpečenia európskej peňaženky digitálnej identity by európske peňaženky digitálnej identity prechodne, pokým nebudú k dispozícii certifikované riešenia odolné proti neoprávnenej manipulácii, ako sú bezpečnostné prvky v zariadeniach používateľov, mali mať možnosť využívať certifikované externé bezpečnostné prvky na ochranu kryptografického materiálu a iných citlivých údajov alebo oznámené prostriedky elektronickej identifikácie s úrovňou záruky „vysoká“. Týmto nariadením by nemali byť dotknuté vnútroštátne podmienky týkajúce sa vydávania a používania certifikovaného externého bezpečnostného prvku, ak od neho závisí prechodné opatrenie.

(30) Európske peňaženky digitálnej identity by mali zabezpečiť najvyššiu úroveň ochrany a bezpečnosti údajov na účely elektronickej identifikácie a autentifikácie, aby uľahčili prístup k verejným a súkromným službám, bez ohľadu na to, či sa takéto údaje uchovávajú lokálne alebo na cloude, pričom sa náležite zohľadnia rôzne úrovne rizika.

(31) Európske peňaženky digitálnej identity by mali byť bezpečné už v štádiu návrhu a mali by obsahovať pokročilé bezpečnostné prvky na ochranu pred krádežou totožnosti a iných údajov, vyradením služby a akoukoľvek inou kybernetickou hrozbou. Súčasťou takéhoto zabezpečenia by mali byť najmodernejšie metódy šifrovania a uchovávania, ktoré sú prístupné len používateľovi a dešifrovateľné len zo strany používateľa, pričom využívajú komunikáciu s inými európskymi peňaženkami digitálnej identity a spoliehajúcimi sa stranami, ktorá je šifrovaná bez medzifáz. Okrem toho by si európske peňaženky digitálnej identity mali vyžadovať bezpečné, explicitné a aktívne potvrdenie od používateľa v prípade operácií vykonávaných prostredníctvom európskych peňaženiek digitálnej identity.

(32) Bezplatné používanie európskych peňaženiek digitálnej identity by nemalo viesť k spracúvaniu údajov nad rámec údajov, ktoré sú potrebné na poskytovanie služieb európskej peňaženky digitálnej identity. Toto nariadenie by nemalo poskytovateľovi európskej peňaženky digitálnej identity umožňovať, aby spracúval osobné údaje uchovávané v európskej peňaženke digitálnej identity, alebo vyplývajúce z jej používania, na iné účely, než je poskytovanie služieb európskej peňaženky digitálnej identity. Na zabezpečenie súkromia by poskytovatelia európskej peňaženky digitálnej identity mali zabezpečiť nepozorovateľnosť tým, že nebudú zbierať údaje a nebudú mať prehľad o transakciách používateľov európskej peňaženky digitálnej identity. Takáto nepozorovateľnosť znamená, že poskytovatelia nemajú možnosť vidieť podrobnosti transakcií, ktoré uskutočňuje používateľ. V osobitných prípadoch a na základe výslovného predchádzajúceho súhlasu používateľa v každom z týchto osobitných prípadov, a v plnom súlade s nariadením (EÚ) 2016/679 by sa však poskytovateľom európskych peňaženiek digitálnej identity mohol udeliť prístup k informáciám, ktoré sú potrebné na poskytovanie konkrétnej služby súvisiacej s európskymi peňaženkami digitálnej identity.

(33) Transparentnosť európskych peňaženiek digitálnej identity a zodpovednosť ich poskytovateľov sú kľúčovými prvkami z hľadiska vytvorenia sociálnej dôvery a naštartovania akceptácie príslušného rámca. Fungovanie európskych peňaženiek digitálnej identity by preto malo byť transparentné a malo by najmä umožňovať overiteľné spracúvanie osobných údajov. V záujme dosiahnutia tohto cieľa by členské štáty mali zverejňovať zdrojový kód softvérových komponentov používateľskej aplikácie európskych peňaženiek digitálnej identity vrátane tých, ktoré súvisia so spracúvaním osobných údajov a údajov právnických osôb. Uverejnenie tohto zdrojového kódu na základe otvorenej licencie by malo spoločnosti vrátane používateľov a vývojárov umožniť pochopiť jeho fungovanie a uskutočňovať jeho audit a preskúmanie. Zvýšila by sa tým dôvera používateľov v príslušný ekosystém a prispelo by to k bezpečnosti európskych peňaženiek digitálnej identity, keďže ktokoľvek by mohol nahlasovať zraniteľné miesta a chyby v kóde. Celkovo by to malo dodávateľov motivovať k tomu, aby dodávali a udržiavali vysoko bezpečný výrobok. V určitých prípadoch by však zverejnenie zdrojového kódu použitých knižníc, komunikačného kanála alebo iných prvkov, ktoré nie sú umiestnené v zariadení používateľa, mohli členské štáty z riadne opodstatnených dôvodov obmedziť, najmä na účely verejnej bezpečnosti.

(34) Používanie európskych peňaženiek digitálnej identity, ako aj ukončenie ich používania by malo byť výlučným právom a rozhodnutím používateľov. Členské štáty by mali vypracovať jednoduché a bezpečné postupy, na základe ktorých budú môcť používatelia požiadať o bezodkladné zrušenie platnosti európskych peňaženiek digitálnej identity, a to aj v prípade straty alebo krádeže. Mal by sa zriadiť mechanizmus, ktorý by v prípade úmrtia používateľa alebo ukončenia činnosti právnickej osoby umožnil orgánu zodpovednému za vysporiadanie dedičstva po fyzickej osobe alebo majetku právnickej osoby požiadať o bezodkladné zneplatnenie európskej peňaženky digitálnej identity.

(35) S cieľom podporiť zavádzanie európskych peňaženiek digitálnej identity a širšie využívanie digitálnych identít by členské štáty mali nielen propagovať výhody príslušných služieb, ale mali by v spolupráci so súkromným sektorom, výskumnými pracovníkmi a akademickou obcou vypracovať aj programy odbornej prípravy zamerané na posilnenie digitálnych zručností svojich občanov a osôb s pobytom na ich území, najmä pre zraniteľné skupiny, ako sú osoby so zdravotným postihnutím a staršie osoby. Členské štáty by mali takisto prostredníctvom komunikačných kampaní zvyšovať informovanosť o prínosoch a rizikách európskych peňaženiek digitálnej identity.

(36) S cieľom zabezpečiť, aby bol európsky rámec digitálnej identity otvorený inováciám, technologickému vývoju a aby bol nadčasový, sa členské štáty nabádajú 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 MSP, startupov a individuálnych inovátorov a výskumných pracovníkov, ako aj príslušných zainteresovaných strán z odvetvia. Takéto iniciatívy by mali zvyšovať a posilňovať regulačný súlad a technickú spoľahlivosť európskych peňaženiek digitálnej identity, ktoré sa majú poskytovať občanom Únie a osobám s pobytom v Únii, čím sa zabráni vývoju riešení, ktoré nie sú v súlade s právom Únie v oblasti ochrany údajov alebo ktoré sú zraniteľné z hľadiska bezpečnosti.

(37) Nariadením Európskeho parlamentu a Rady (EÚ) 2019/1157[11] sa posilňuje bezpečnosť preukazov totožnosti zlepšenými bezpečnostnými prvkami do augusta 2021. Členské štáty by mali zvážiť, či je ich možné oznamovať v rámci schém elektronickej identifikácie, s cieľom rozšíriť cezhraničnú dostupnosť prostriedkov elektronickej identifikácie.

(38) 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, ktoré môžu oznámiť ako vnútroštátne schémy elektronickej identifikácie podľa nariadenia (EÚ) č. 910/2014.

(39) Zjednodušením súčasných postupov oznamovania a vzájomného preskúmania sa zabráni rôznorodým prístupom k posudzovaniu rôznych oznámených schém elektronickej identifikácie a uľahčí sa budovanie dôvery medzi členskými štátmi. Nové zjednodušené mechanizmy sú určené na podporu spolupráce členských štátov v oblasti bezpečnosti a interoperability ich oznámených schém elektronickej identifikácie.

(40) Na zabezpečenie súladu s požiadavkami tohto nariadenia a príslušných vykonávacích aktov prijatých na jeho základe by členské štáty 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 kontexte schém certifikácie, ktoré sa majú zriadiť na úrovni Únie podľa nariadenia (EÚ) 2019/881, aby podporili svoje tvrdenia o zosúladení schém alebo ich častí s nariadením (EÚ) č. 910/2014.

---

[11] 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).

(41) Poskytovatelia verejných služieb používajú osobné identifikačné údaje dostupné z prostriedkov elektronickej identifikácie podľa nariadenia (EÚ) č. 910/2014 na spárovanie elektronickej totožnosti používateľov z iných členských štátov s osobnými identifikačnými údajmi, ktoré sa týmto používateľom poskytli v členskom štáte, ktorý vykonáva postup cezhraničného párovania totožnosti. V mnohých prípadoch si však napriek použitiu minimálneho súboru údajov poskytovaných v rámci oznámených schém elektronickej identifikácie zabezpečenie presného spárovania totožnosti, keď členské štáty konajú ako spoliehajúce sa strany, vyžaduje dodatočné informácie o používateľovi a osobitné doplnkové postupy jedinečnej identifikácie, ktoré je potrebné vykonať na vnútroštátnej úrovni. S cieľom ďalej podporiť použiteľnosť prostriedkov elektronickej identifikácie, poskytovať lepšie online verejné služby a zvýšiť právnu istotu, pokiaľ ide o elektronickú identitu používateľov, by sa v nariadení (EÚ) č. 910/2014 malo od členských štátov vyžadovať, aby prijali osobitné online opatrenia na zabezpečenie jednoznačného spárovania totožnosti, keď majú používatelia v úmysle získať prístup k online cezhraničným verejným službám.

(42) Pri vývoji európskych peňaženiek digitálnej identity je nevyhnutné zohľadniť potreby používateľov. K dispozícii by mali byť zmysluplné možnosti použitia a online služby využívajúce európske peňaženky 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 zavádzaniu online služieb vo všetkých členských štátoch. Nezáväzné usmernenia o tom, ako navrhovať, vyvíjať a zavádzať online služby využívajúce európske peňaženky digitálnej identity, majú potenciál stať sa užitočným nástrojom na dosiahnutie tohto cieľa. Takéto usmernenia by sa mali vypracovať s ohľadom na rámec Únie pre interoperabilitu. Vedúcu úlohu pri prijímaní týchto usmernení by mali zohrávať členské štáty.

(43) V súlade so smernicou Európskeho parlamentu a Rady (EÚ) 2019/882[12] 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.

(44) S cieľom zabezpečiť účinné presadzovanie tohto nariadenia by sa mala stanoviť minimálna výška čo najväčšieho počtu správnych pokút pre kvalifikovaných aj nekvalifikovaných poskytovateľov dôveryhodných služieb. Členské štáty by mali stanoviť účinné, primerané a odrádzajúce sankcie. Pri určovaní sankcií by sa mala náležite zohľadniť veľkosť dotknutých subjektov, ich obchodné modely a závažnosť porušení.

(45) 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 vytvárajú dojem, že kvalifikovanými sú akékoľvek nekvalifikované dôveryhodné služby ponúkané týmito poskytovateľmi.

(46) 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 v práve Únie alebo vo vnútroštátnom práve. Nemalo by mať ani vplyv na vnútroštátne požiadavky na formu v súvislosti s verejnými registrami, konkrétne s obchodným registrom a katastrom nehnuteľností.

---

[12] 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).

(47) Poskytovanie a využívanie dôveryhodných služieb a výhody z hľadiska pohodlia a právnej istoty v kontexte cezhraničných transakcií, najmä pri využívaní kvalifikovaných dôveryhodných služieb, sú čoraz dôležitejšie pre medzinárodný obchod a spoluprácu. Medzinárodní partneri Únie vytvárajú rámce dôvery inšpirované nariadením (EÚ) č. 910/2014. S cieľom uľahčiť uznávanie kvalifikovaných dôveryhodných služieb a ich poskytovateľov môže Komisia prijať vykonávacie akty na účely stanovenia podmienok, za ktorých by sa rámce dôvery tretích krajín mohli považovať za rovnocenné s rámcom dôvery pre kvalifikované dôveryhodné služby a ich poskytovateľov podľa tohto nariadenia. Takýto prístup by mal dopĺňať možnosť vzájomného uznávania dôveryhodných služieb a ich poskytovateľov usadených v Únii a v tretích krajinách v súlade s článkom 218 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“). Pri stanovovaní podmienok, za ktorých by sa rámce dôvery tretích krajín mohli považovať za rovnocenné s rámcom dôvery pre kvalifikované dôveryhodné služby a ich poskytovateľov podľa nariadenia (EÚ) č. 910/2014, by sa mal zabezpečiť súlad s príslušnými ustanoveniami smernice Európskeho parlamentu a Rady (EÚ) 2022/2555[13] a nariadenia (EÚ) 2016/679, ako aj používanie dôveryhodných zoznamov ako základných prvkov budovania dôvery.

[13] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).

(48) Týmto nariadením by sa mala podporiť možnosť výberu a možnosť prechodu medzi európskymi peňaženkami digitálnej identity, ak členský štát schválil na svojom území viac ako jedno riešenie európskej peňaženky digitálnej identity. S cieľom zabrániť efektu odkázanosti na určitého poskytovateľa v takýchto situáciách by poskytovatelia európskych peňaženiek digitálnej identity, ak je to technicky možné, mali zabezpečiť účinnú prenosnosť údajov na žiadosť používateľov európskej peňaženky digitálnej identity a nemali by mať možnosť používať zmluvné, hospodárske ani technické prekážky na to, aby bránili účinnému prechodu medzi rôznymi európskymi peňaženkami digitálnej identity alebo aby od neho odrádzali.

(49) Na zabezpečenie riadneho fungovania európskych peňaženiek digitálnej identity potrebujú ich poskytovatelia účinnú interoperabilitu a spravodlivé, primerané a nediskriminačné podmienky pre európske peňaženky digitálnej identity, pokiaľ ide o prístup k osobitným hardvérovým a softvérovým prvkom mobilných zariadení. Tieto komponenty by mohli zahŕňať najmä antény komunikácie na krátku vzdialenosť a bezpečnostné prvky vrátane univerzálnych kariet s integrovaným obvodom, zabudovaných bezpečnostných prvkov, mikroSD kariet a rozhrania Bluetooth Low Energy. Prístup k týmto komponentom by mohol byť pod kontrolou prevádzkovateľov mobilných sietí a výrobcov zariadení. Ak je to preto potrebné na poskytovanie služieb európskych peňaženiek digitálnej identity, výrobcovia originálneho vybavenia mobilných zariadení alebo poskytovatelia elektronických komunikačných služieb by nemali odmietnuť prístup k takýmto komponentom. Okrem toho by sa na podniky, ktoré sú určené za strážcov prístupu pre základné platformové služby uvedené na zozname Komisie podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2022/1925[14], mali naďalej vzťahovať osobitné ustanovenia uvedeného nariadenia na základe jeho článku 6 ods. 7.

---

[14] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/1925 zo 14. septembra 2022 o súťažeschopných a spravodlivých trhoch digitálneho sektora a o zmene smerníc (EÚ) 2019/1937 a (EÚ) 2020/1828 (akt o digitálnych trhoch) (Ú. v. EÚ L 265, 12.10.2022, s. 1).

(50) S cieľom zefektívniť povinnosti v oblasti kybernetickej bezpečnosti ukladané poskytovateľom dôveryhodných služieb, ako aj umožniť týmto poskytovateľom a ich príslušným orgánom využívať právny rámec ustanovený smernicou (EÚ) 2022/2555 sa od dôveryhodných služieb vyžaduje, aby prijali primerané technické a organizačné opatrenia podľa uvedenej smernice, ako sú opatrenia na riešenie systémových zlyhaní, ľudskej chyby, zlomyseľného konania alebo prírodných javov v záujme riadenia rizík, ktoré predstavujú pre bezpečnosť sietí a informačných systémov, ktoré títo poskytovatelia používajú pri poskytovaní svojich služieb, ako aj aby oznamovali závažné incidenty a kybernetické hrozby v súlade s uvedenou smernicou. 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, poškodením sieťových káblov alebo incidentov, ku ktorým došlo v súvislosti s identifikáciou osôb. Požiadavky na riadenie kybernetických rizík a oznamovacie povinnosti podľa smernice (EÚ) 2022/2555 by sa mali považovať za doplnkové k požiadavkám, ktoré sa poskytovateľom dôveryhodných služieb ukladajú podľa tohto nariadenia. Príslušné orgány určené podľa smernice (EÚ) 2022/2555 by v prípade potreby mali naďalej uplatňovať zavedené vnútroštátne postupy alebo usmernenia týkajúce sa uplatňovania požiadaviek na bezpečnosť a oznamovanie a vykonávania dohľadu nad dodržiavaním takýchto požiadaviek podľa nariadenia (EÚ) č. 910/2014. Týmto nariadením nie je dotknutá povinnosť oznamovať prípady porušenia ochrany osobných údajov podľa nariadenia (EÚ) 2016/679.

(51) Náležitá pozornosť by sa mala venovať zabezpečeniu účinnej spolupráce medzi orgánmi dohľadu určenými podľa článku 46b nariadenia (EÚ) č. 910/2014 a príslušnými orgánmi určenými alebo zriadenými podľa článku 8 ods. 1 smernice (EÚ) 2022/2555. Ak sa takýto orgán dohľadu líši od takéhoto príslušného orgánu, mali by úzko a včas spolupracovať prostredníctvom výmeny relevantných informácií, aby sa zabezpečil účinný dohľad a aby poskytovatelia dôveryhodných služieb plnili požiadavky stanovené v nariadení (EÚ) č. 910/2014 a v smernici (EÚ) 2022/2555. Orgány dohľadu určené podľa nariadenia (EÚ) č. 910/2014 by predovšetkým mali byť oprávnené požiadať príslušné orgány určené alebo zriadené podľa smernice (EÚ) 2022/2555, aby poskytli relevantné informácie potrebné na udelenie kvalifikovaného štatútu a aby vykonávali opatrenia dohľadu s cieľom overiť, či poskytovatelia dôveryhodných služieb dodržiavajú príslušné požiadavky podľa smernice (EÚ) 2022/2555, alebo od nich požadovať nápravu ich nedodržiavania.

(52) Je nevyhnutné, 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 celoúnijné 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 odosielateľa 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 propagovať spravodlivé postupy na vnútornom trhu.

(53) Občania Únie a osoby s pobytom v Únii si vo väčšine prípadov nemôžu vymieňať digitálne informácie týkajúce sa ich totožnosti, ako je ich adresa, vek, odborná kvalifikácia, vodičský preukaz a iné povolenia a platobné údaje, cezhranične a s vysokou úrovňou ochrany údajov.

(54) Malo by byť možné vydávať a spracúvať dôveryhodné elektronické atribúty a prispievať k znižovaniu administratívneho zaťaženia tým, že sa občanom Únie a osobám s pobytom v Únii umožní využívať ich v súkromných a verejných transakciách. Občania Únie a osoby s pobytom v Únii by mali mať napríklad možnosť preukázať vlastníctvo platného vodičského preukazu vydaného orgánom v jednom členskom štáte, ktoré môžu príslušné orgány v iných členských štátoch overiť a spoľahnúť sa na naň, ako aj možnosť využívať v cezhraničnom kontexte svoje potvrdenia o sociálnom zabezpečení alebo budúce digitálne cestovné doklady.

(55) Každý poskytovateľ služieb, ktorý vydáva v elektronickej forme osvedčené atribúty, ako sú diplomy, licencie, rodné listy alebo splnomocnenia a mandáty na zastupovanie fyzických alebo právnických osôb alebo na konanie v ich mene, by sa mal považovať za poskytovateľa dôveryhodných služieb elektronického osvedčenia atribútov. Elektronickému osvedčeniu atribútov by sa nemal odopierať právny účinok z dôvodu, že je v elektronickej forme alebo že nespĺňa požiadavky na kvalifikované elektronické osvedčenie atribútov. Mali by sa stanoviť všeobecné požiadavky na zabezpečenie toho, aby kvalifikované elektronické osvedčenie atribútov malo rovnocenný právny účinok ako osvedčenia v listinnej 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.

(56) Široká dostupnosť a použiteľnosť európskych peňaženiek digitálnej identity by mala zvýšiť ich akceptáciu a dôveru v ne zo strany súkromných osôb aj súkromných poskytovateľov služieb. Súkromné spoliehajúce sa strany, ktoré poskytujú služby napríklad v oblasti dopravy, energetiky, bankovníctva, finančných služieb, sociálneho zabezpečenia, zdravia, pitnej vody, poštových služieb, digitálnej infraštruktúry, telekomunikácií alebo vzdelávania, by preto mali akceptovať používanie európskych peňaženiek digitálnej identity na poskytovanie služieb, ak sa podľa práva Únie alebo vnútroštátneho práva alebo na základe zmluvnej povinnosti vyžaduje silná autentifikácia používateľa na účely online identifikácie. Každá žiadosť spoliehajúcej sa strany o informácie od používateľa európskej peňaženky digitálnej identity by mala byť potrebná a primeraná z hľadiska zamýšľaného použitia v danom prípade, mala by byť v súlade so zásadou minimalizácie údajov a mala by sa pri nej zabezpečiť transparentnosť, pokiaľ ide o to, ktoré údaje sa zdieľajú a na aké účely. S cieľom uľahčiť používanie a akceptáciu európskych peňaženiek digitálnej identity by sa mali pri ich zavádzaní zohľadniť všeobecne uznávané odvetvové normy a špecifikácie.

(57) Ak veľmi veľké online platformy vyžadujú od používateľov, aby boli autentifikovaní na účely prístupu k online službám v zmysle článku 33 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2065[15], od týchto platforiem by sa malo vyžadovať, aby na základe dobrovoľnej žiadosti používateľa akceptovali používanie európskych peňaženiek digitálnej identity. Používatelia by nemali mať povinnosť používať na prístup k súkromným službám európsku peňaženku digitálnej identity a nemali by byť obmedzovaní ani by sa im nemalo brániť v prístupe k službám z dôvodu, že európsku peňaženku digitálnej identity nepoužívajú. Ak si to však používatelia želajú, veľmi veľké online platformy by ich na tento účel mali akceptovať, pričom by mali dodržiavať zásadu minimalizácie údajov a právo používateľov používať voľne zvolené pseudonymy. Vzhľadom na význam veľmi veľkých online platforiem z dôvodu ich dosahu, najmä pokiaľ ide o počet príjemcov služieb a hospodárskych transakcií, je povinnosť akceptovať európske peňaženky digitálnej identity potrebná na zvýšenie ochrany používateľov pred podvodmi a na zabezpečenie vysokej úrovne ochrany údajov.

(58) Mali by sa vypracovať kódexy správania na úrovni Únie s cieľom prispieť k širokej dostupnosti a použiteľnosti prostriedkov elektronickej identifikácie vrátane európskych peňaženiek digitálnej identity v rozsahu pôsobnosti tohto nariadenia. Tieto kódexy správania by mali uľahčiť širokú akceptáciu prostriedkov elektronickej identifikácie vrátane európskych peňaženiek digitálnej identity zo strany tých poskytovateľov služieb, ktorí nie sú považovaní za veľmi veľké platformy a ktorí na autentifikáciu používateľov využívajú služby elektronickej identifikácie tretích strán.

---

[15] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) (Ú. v. EÚ L 277, 27.10.2022, s. 1).

(59) Selektívne zverejňovanie je koncepcia, ktorá oprávňuje vlastníka údajov zverejniť len určité časti väčšieho súboru údajov, aby prijímajúci subjekt získal len také informácie, ktoré sú potrebné na poskytovanie služby, ktorú požaduje používateľ. Európska peňaženka digitálnej identity by mala technicky umožniť selektívne zverejňovanie atribútov spoliehajúcim sa stranám. Malo by byť technicky možné pre používateľa selektívne zverejniť atribúty, a to aj z viacerých odlišných elektronických osvedčení, a kombinovať a bezproblémovo ich prezentovať spoliehajúcim sa stranám. Táto funkcia by sa mala stať základným prvkom štruktúry európskych peňaženiek digitálnej identity, čím by sa zvýšilo pohodlie používateľov a ochrana osobných údajov vrátane minimalizácie údajov.

(60) Pokiaľ sa v osobitných pravidlách práva Únie alebo vnútroštátneho práva nevyžaduje identifikácia, aby sa používatelia identifikovali, nemal by sa zakazovať prístup k službám s použitím pseudonymu.

(61) Atribúty poskytnuté kvalifikovanými poskytovateľmi dôveryhodných služieb ako súčasť kvalifikovaného osvedčenia atribútov by sa mali overovať na základe autentických zdrojov buď priamo kvalifikovaným poskytovateľom dôveryhodných služieb, alebo prostredníctvom určených sprostredkovateľov uznaných na vnútroštátnej úrovni v súlade s právom Únie alebo vnútroštátnym právom na účely bezpečnej výmeny osvedčených atribútov medzi poskytovateľmi služieb totožnosti alebo 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. Malo by byť možné, aby vhodné mechanizmy zahŕňali využívanie konkrétnych sprostredkovateľov alebo technických riešení v súlade s vnútroštátnym právom, ktoré umožňujú prístup k autentickým zdrojom. Zabezpečenie dostupnosti mechanizmu, ktorý umožňuje overovanie atribútov pomocou autentických zdrojov, má za cieľ uľahčiť kvalifikovaným poskytovateľom dôveryhodných služieb, ktorí poskytujú kvalifikované elektronické osvedčenia atribútov, dodržiavanie ich povinností podľa nariadenia (EÚ) č. 910/2014. Nová príloha k uvedenému nariadeniu by mala obsahovať zoznam kategórií atribútov, v súlade s ktorými majú členské štáty 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.

(62) Bezpečná elektronická identifikácia a poskytovanie osvedčení atribútov by mali ponúknuť sektoru finančných služieb dodatočnú flexibilitu a riešenia, ktoré umožnia identifikáciu klientov a výmenu osobitných atribútov potrebných napríklad na splnenie požiadaviek náležitej starostlivosti vo vzťahu ku klientovi podľa budúceho nariadenia, ktorým sa zriadi úrad pre boj proti praniu špinavých peňazí, požiadaviek na vhodnosť vyplývajúcich z právnych predpisov v oblasti ochrany investorov, alebo ktoré podporia plnenie prísnych požiadaviek na autentifikáciu zákazníkov pri online identifikácii na účely prihlásenia sa do účtu a iniciovania transakcií v oblasti platobných služieb.

(63) Právny účinok elektronického podpisu sa nemá napadnúť z dôvodu, že je v elektronickej forme alebo že nespĺňa požiadavky kvalifikovaného elektronického podpisu. Avšak je na vnútroštátnom práve, aby stanovilo právny účinok elektronických podpisov, s výnimkou požiadaviek stanovených v tomto nariadení, podľa ktorého sa má právny účinok kvalifikovaného elektronického podpisu považovať za rovnocenný s vlastnoručným podpisom. Pri určovaní právnych účinkov elektronických podpisov by členské štáty mali zohľadniť zásadu proporcionality medzi právnou hodnotou dokumentu, ktorý sa má podpísať, a úrovňou bezpečnosti a nákladov, ktoré si vyžaduje elektronický podpis. S cieľom zvýšiť dostupnosť a používanie elektronických podpisov sa členské štáty nabádajú, aby zvážili používanie zdokonalených elektronických podpisov pri každodenných transakciách, pre ktoré poskytujú dostatočnú úroveň bezpečnosti a dôvery.

(64) S cieľom zabezpečiť konzistentnosť certifikačných postupov v celej Únii 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 verejným alebo súkromným subjektom, ktoré majú certifikované zariadenia na vyhotovenie kvalifikovaného elektronického podpisu, dočasne opätovne certifikovať takéto zariadenia na krátke obdobie certifikácie na základe výsledkov predchádzajúceho certifikačného postupu, ak takúto opätovnú certifikáciu nemožno vykonať v zákonom stanovenej lehote z iného dôvodu ako je narušenie bezpečnosti alebo bezpečnostný incident, a bez toho, aby bola dotknutá povinnosť viesť posúdenie zraniteľnosti a to bez toho, aby bol dotknutý uplatniteľný certifikačný postup.

(65) Vydávanie certifikátov na autentifikáciu webových sídiel má za cieľ poskytovať používateľom istotu s vysokou úrovňou dôvery, pokiaľ ide o totožnosť subjektu, ktorý stojí za webovým sídlom, bez ohľadu na platformu použitú na zobrazenie uvedenej identity. Tieto certifikáty by mali prispievať k budovaniu dôvery v podnikanie online, keďže používatelia by mali dôveru vo webové sídlo, ktoré bolo autentifikované. Používanie týchto certifikátov webovými sídlami by malo byť dobrovoľné. Aby sa autentifikácia webových sídiel stala prostriedkom na zvýšenie dôvery, poskytnutie lepšieho zážitku pre používateľa a podporu rastu na vnútornom trhu, týmto nariadením sa ustanovuje rámec dôvery, ktorého súčasťou sú aj minimálne povinnosti v oblasti bezpečnosti a zodpovednosti pre poskytovateľov kvalifikovaných certifikátov pre autentifikáciu webových sídiel a požiadavky na vydávanie uvedených certifikátov. Národné dôveryhodné zoznamy by mali potvrdiť kvalifikovaný status služieb autentifikácie webových sídiel a ich poskytovateľov dôveryhodných služieb vrátane ich úplného súladu s požiadavkami tohto nariadenia, pokiaľ ide o vydávanie kvalifikovaných certifikátov pre autentifikáciu webových sídiel. Uznávanie kvalifikovaných certifikátov pre autentifikáciu webových sídiel znamená, že poskytovatelia webových prehliadačov by nemali popierať pravosť týchto certifikátov výlučne na účel osvedčenia prepojenia medzi názvom domény webového sídla a fyzickou alebo právnickou osobou, ktorej sa certifikát vydáva, alebo na účely potvrdenia totožnosti tejto osoby. Poskytovatelia webových prehliadačov by mali koncovému používateľovi zobrazovať certifikované údaje o totožnosti a ostatné osvedčené atribúty používateľsky ústretovým spôsobom v prostredí prehliadača, a to technickými prostriedkami podľa vlastného výberu. Na tento účel by poskytovatelia webových prehliadačov mali zabezpečiť podporu kvalifikovaných certifikátov pre autentifikáciu webových sídiel vydaných v plnom súlade s týmto nariadením a interoperabilitu s nimi.

Povinnosť uznávania a interoperability a podpory kvalifikovaných certifikátov pre autentifikáciu webových sídiel nemá vplyv na slobodu poskytovateľov webových prehliadačov zaistiť bezpečnosť webových sídel, autentifikáciu domén a šifrovanie webovej prevádzky spôsobom a pomocou technológie, ktoré považujú za najvhodnejšie. S cieľom prispieť k online bezpečnosti koncových používateľov by poskytovatelia webových prehliadačov mali mať za výnimočných okolností možnosť prijať preventívne opatrenia, ktoré sú potrebné a primerané v reakcii na odôvodnené obavy týkajúce sa narušenia bezpečnosti alebo straty integrity identifikovaného certifikátu alebo súboru certifikátov. Ak poskytovatelia webových prehliadačov prijmú takéto preventívne opatrenia, mali by bez zbytočného odkladu informovať Komisiu, vnútroštátny orgán dohľadu, subjekt, ktorému bol certifikát vydaný, a kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydal daný certifikát alebo súbor certifikátov, o akýchkoľvek obavách týkajúcich sa takéhoto narušenia bezpečnosti alebo straty integrity, ako aj o opatreniach prijatých v súvislosti s daným certifikátom alebo súborom certifikátov. Uvedenými opatreniami by nemala byť dotknutá povinnosť poskytovateľov webových prehliadačov uznávať kvalifikované certifikáty pre autentifikáciu webových sídiel v súlade s národnými dôveryhodnými zoznamami. S cieľom väčšmi chrániť občanov Únie a osoby s pobytom v Únii a podporovať používanie kvalifikovaných certifikátov pre autentifikáciu webových sídiel by verejné orgány v členských štátoch mali zvážiť začlenenie týchto certifikátov do svojich webových sídel. Opatrenia stanovené v tomto nariadení, ktorých cieľom je zabezpečiť väčšiu súdržnosť medzi rozdielnymi prístupmi a postupmi členských štátov v oblasti postupov dohľadu, majú prispieť k zvýšeniu dôvery v bezpečnosť, kvalitu a dostupnosť kvalifikovaných certifikátov pre autentifikáciu webových sídiel.

(66) Mnohé členské štáty zaviedli vnútroštátne požiadavky na služby, ktoré poskytujú bezpečnú a dôveryhodnú elektronickú archiváciu s cieľom umožniť dlhodobé uchovávanie elektronických údajov a elektronických dokumentov, a na 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 stanovené v tomto nariadení. Právny rámec pre kvalifikované elektronické archivačné služby 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. Uvedené ustanovenia by sa mali vzťahovať na elektronické údaje a elektronické dokumenty, ktoré boli vytvorené v elektronickej forme, ako aj na dokumenty v listinnej podobe, ktoré boli naskenované a digitalizované. V prípade potreby by uvedené ustanovenia mali umožniť prenos uchovávaných elektronických údajov a elektronických dokumentov na rôznych médiách alebo v rôznych formátoch na účely predĺženia ich trvanlivosti a čitateľnosti aj po uplynutí obdobia technologickej platnosti, pričom by sa malo v čo najväčšej možnej miere zabrániť strate a pozmeňovaniu. Ak elektronické údaje a elektronické dokumenty zaslané elektronickej 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 mohla prípadne využívať aj iné kvalifikované dôveryhodné služby zriadené týmto nariadením. Na vytváranie dôkazov o uchovávaní v prípade použitia elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok by sa mali používať kvalifikované dôveryhodné služby. V rozsahu, v akom elektronické archivačné služby nie sú harmonizované týmto nariadením, by členské štáty mali mať možnosť zachovať alebo zaviesť vnútroštátne ustanovenia v súlade s právom Únie týkajúce sa týchto služieb, ako napríklad osobitné ustanovenia o službách začlenených do organizácie a používaných len pre interné archívy danej organizácie. V tomto nariadení by sa nemalo rozlišovať medzi elektronickými údajmi a elektronickými dokumentmi, ktoré boli vytvorené v elektronickej forme, a fyzickými dokumentmi, ktoré boli digitalizované.

(67) Činnosti národných archívov a ústavov pamäti národa ako organizácií, ktoré sa venujú zachovávaniu dokumentárneho dedičstva vo verejnom záujme, sú zvyčajne upravené vo vnútroštátnom práve a nemusia nevyhnutne zahŕňať poskytovanie dôveryhodných služieb v zmysle tohto nariadenia. Pokiaľ tieto inštitúcie takéto dôveryhodné služby neposkytujú, ich fungovanie týmto nariadením nie je dotknuté.

(68) Elektronické registre sú sekvenciou záznamov elektronických údajov, ktoré by mali zabezpečovať ich integritu a presnosť ich chronologického poradia. Elektronické registre by mali stanoviť chronologické poradie záznamov údajov. V spojení s inými technológiami by mali prispieť k riešeniam, ktoré majú priniesť efektívnejšie a transformačnejšie verejné služby, ako sú elektronické hlasovanie, cezhraničná spolupráca colných orgánov, cezhraničná spolupráca akademických inštitúcií a zaznamenávanie vlastníctva nehnuteľností v decentralizovaných katastroch nehnuteľností. Kvalifikované elektronické registre by mali vytvárať právny predpoklad pre jedinečné a presné sekvenčné chronologické poradie a integritu záznamov údajov v registri. Vzhľadom na ich špecifiká, ako je sekvenčné chronologické poradie záznamov údajov, by sa elektronické registre mali odlišovať od iných dôveryhodných služieb, ako sú elektronické časové pečiatky a elektronické doručovacie služby pre registrované zásielky. S cieľom zabezpečiť právnu istotu a podporiť inováciu by sa mal vytvoriť právny rámec pre celú Úniu, ktorým sa zabezpečí cezhraničné uznávanie dôveryhodných služieb na zaznamenávanie údajov v elektronických registroch. Malo by sa tým dostatočne zabrániť tomu, aby sa rovnaké digitálne aktíva kopírovali a predávali viackrát rôznym stranám. Postup vytvárania a aktualizácie elektronického registra závisí od typu použitého registra, konkrétne či ide o centralizovaný alebo distribuovaný register. Týmto nariadením by sa mala zabezpečiť technologická neutralita, čiže by sa nemala uprednostňovať ani diskriminovať žiadna technológia používaná na implementáciu novej dôveryhodnej služby pre elektronické registre. Okrem toho by Komisia mala pri príprave vykonávacích aktov, v ktorých sa špecifikujú požiadavky na kvalifikované elektronické registre, pomocou primeraných metodík zohľadniť ukazovatele udržateľnosti, pokiaľ ide o akékoľvek nepriaznivé vplyvy na klímu alebo iné nepriaznivé vplyvy súvisiace so životným prostredím.

(69) Úlohou poskytovateľov dôveryhodných služieb pre elektronické registre by malo byť zabezpečenie sekvenčného zaznamenávania údajov do registra. Týmto nariadením nie sú dotknuté žiadne zákonné povinnosti používateľov elektronických registrov podľa práva Únie alebo vnútroštátneho práva. Napríklad prípady použitia, ktoré zahŕňajú spracúvanie osobných údajov, by mali byť v súlade s nariadením (EÚ) 2016/679 a prípady použitia súvisiace s finančnými službami by mali byť v súlade s príslušnými právnymi predpismi Únie v oblasti finančných služieb.

(70) Na to, aby sa zabránilo fragmentácii a prekážkam na vnútornom trhu spôsobeným rôznymi normami a technickými obmedzeniami a aby sa zabezpečil koordinovaný proces, ktorý zabráni ovplyvneniu vykonávania európskeho rámca digitálnej identity, je potrebná úzka a štruktúrovaná spolupráca medzi Komisiou, členskými štátmi, občianskou spoločnosťou, akademickou obcou a súkromným sektorom. Na dosiahnutie tohto cieľa by členské štáty a Komisia mali spolupracovať v rámci stanovenom v odporúčaní Komisie (EÚ) 2021/946[16] v záujme určenia spoločného súboru nástrojov Únie pre európsky rámec digitálnej identity. V tejto súvislosti by sa členské štáty mali dohodnúť na komplexnej technickej architektúre a referenčnom rámci, súbore spoločných noriem a technických referencií vrátane uznávaných existujúcich noriem a na súbore usmernení a opisov najlepších postupov vzťahujúcich sa aspoň na všetky funkcie a interoperabilitu európskych peňaženiek digitálnej identity vrátane elektronických podpisov a kvalifikovaných poskytovateľov dôveryhodných služieb pre elektronické osvedčenie atribútov, ako sa stanovuje v tomto nariadení. V tejto súvislosti by sa členské štáty mali dohodnúť aj na spoločných prvkoch obchodného modelu a štruktúry poplatkov za európske peňaženky digitálnej identity s cieľom uľahčiť ich využívanie, najmä zo strany MSP, v cezhraničnom kontexte. Obsah súboru nástrojov by sa mal vyvíjať a upravovať paralelne s výsledkami diskusií a procesom prijímania európskeho rámca digitálnej identity.

---

[16] Odporúčanie Komisie (EÚ) 2021/946 z 3. júna 2021 o spoločnom súbore nástrojov Únie pre koordinovaný prístup k európskemu rámcu digitálnej identity (Ú. v. EÚ L 210, 14.6.2021, s. 51).

(71) Týmto nariadením sa stanovuje harmonizovaná úroveň kvality, dôveryhodnosti a bezpečnosti kvalifikovaných dôveryhodných služieb bez ohľadu na to, kde sa operácie vykonávajú. Kvalifikovaný poskytovateľ dôveryhodných služieb by preto mal môcť vykonávať svoje operácie súvisiace s poskytovaním kvalifikovanej dôveryhodnej služby prostredníctvom externých dodávateľov v tretej krajine, ak táto tretia krajina poskytne primerané záruky a zabezpečí, že činnosti dohľadu a audity možno presadzovať tak, ako keby sa vykonávali v Únii. Ak súlad s týmto nariadením nemožno v plnej miere zabezpečiť, orgány dohľadu by mali mať možnosť prijať primerané a odôvodnené opatrenia vrátane odňatia kvalifikovaného štatútu poskytovanej dôveryhodnej službe.

(72) S cieľom zabezpečiť právnu istotu, pokiaľ ide o platnosť zdokonalených elektronických podpisov založených na kvalifikovaných certifikátoch, je nevyhnutné špecifikovať posúdenie spoliehajúcou sa stranou, ktorá vykonáva validáciu daného zdokonaleného elektronického podpisu na základe kvalifikovaných certifikátov.

(73) Poskytovatelia dôveryhodných služieb by na zaistenie bezpečnosti a spoľahlivosti svojich dôveryhodných služieb mali používať kryptografické metódy odzrkadľujúce súčasné najlepšie postupy a dôveryhodné vykonávanie týchto algoritmov.

(74) V tomto nariadení sa stanovuje povinnosť kvalifikovaných poskytovateľov dôveryhodných služieb overovať totožnosť fyzickej alebo právnickej osoby, ktorej sa vydáva kvalifikovaný certifikát alebo kvalifikované elektronické osvedčenie atribútov, na základe rôznych harmonizovaných metód v rámci Únie. S cieľom zabezpečiť, aby sa kvalifikované certifikáty a kvalifikované elektronické osvedčenia atribútov vydávali osobe, ktorej patria, a aby osvedčovali správny a jedinečný súbor údajov predstavujúcich totožnosť danej osoby, by kvalifikovaní poskytovatelia dôveryhodných služieb, ktorí vydávajú kvalifikované certifikáty alebo kvalifikované elektronické osvedčenia atribútov, mali v čase vydávania týchto certifikátov a osvedčení s úplnou istotou zabezpečiť identifikáciu danej osoby. Okrem povinného overovania totožnosti osoby, ak sa vzťahuje na vydávanie kvalifikovaných certifikátov a pri vydávaní kvalifikovaného elektronického osvedčenia atribútov, by kvalifikovaní poskytovatelia dôveryhodných služieb mali s úplnou istotou zabezpečiť aj správnosť a presnosť overených atribútov osoby, ktorej sa vydáva kvalifikovaný certifikát alebo kvalifikované elektronické osvedčenie atribútov. Uvedené povinnosti týkajúce sa výsledku a úplnej istoty pri overovaní osvedčovaných údajov by mali byť podporené vhodnými prostriedkami, okrem iného aj použitím jednej alebo v prípade potreby viacerých z osobitných metód stanovených v tomto nariadení. Tieto metódy by malo byť možné kombinovať, aby sa poskytol vhodný základ na overenie totožnosti osoby, ktorej sa vydáva kvalifikovaný certifikát alebo kvalifikované elektronické osvedčenie atribútov. Malo by byť možné, aby takáto kombinácia zahŕňala aj využívanie prostriedkov elektronickej identifikácie, ktoré spĺňajú požiadavky na úroveň záruky „významná“, v kombinácii s inými prostriedkami overovania totožnosti. Takáto elektronická identifikácia by umožnila splnenie harmonizovaných požiadaviek stanovených v tomto nariadení, pokiaľ ide o úroveň záruky „vysoká“ v rámci dodatočných harmonizovaných postupov na diaľku, ktorými sa zabezpečuje identifikácia s vysokou úrovňou spoľahlivosti. Uvedené metódy by mali umožňovať, aby kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý vydáva kvalifikované elektronické osvedčenie atribútov, overil atribúty, ktoré sa majú osvedčiť, elektronickými prostriedkami na žiadosť používateľa v súlade s právom Únie alebo vnútroštátnym právom, a to aj na základe autentických zdrojov.

(75) Aby bolo toto nariadenie v súlade so globálnym vývojom a aby sa dodržiavali najlepšie 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.

(76) Keďže ciele tohto nariadenia, a to rozvoj celoúnijného európskeho rámca digitálnej identity a rámca dôveryhodných služieb, nie je možné uspokojivo dosiahnuť na úrovni členských štátov, ale z dôvodov ich rozsahu a dôsledkov ich možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie týchto cieľov.

(77) V súlade s článkom 42 ods. 1 nariadenia (EÚ) 2018/1725 sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov.

(78) Nariadenie (EÚ) č. 910/2014 by sa preto malo zodpovedajúcim spôsobom zmeniť,

PRIJALI TOTO NARIADENIE:

Článok 1

Zmeny nariadenia (EÚ) č. 910/2014

Nariadenie (EÚ) č. 910/2014 sa mení takto:

1. Článok 1 sa nahrádza takto:

„*Článok 1*

Predmet úpravy

Cieľom tohto nariadenia je zabezpečiť riadne fungovanie vnútorného trhu a primeranú úroveň bezpečnosti prostriedkov elektronickej identifikácie a dôveryhodných služieb používaných v celej Únii s cieľom umožniť a uľahčiť fyzickým a právnickým osobám vykonávať ich právo bezpečne sa zúčastňovať na digitálnej spoločnosti a právo na prístup k online verejným a súkromným službám v celej Únii. Na tieto účely sa týmto nariadením:

a) stanovujú podmienky, za ktorých majú členské štáty uznávať prostriedky elektronickej identifikácie fyzických a právnických osôb, na ktoré sa vzťahuje oznámená schéma elektronickej identifikácie iného členského štátu, a poskytnúť a uznávať európske peňaženky digitálnej identity;

b) stanovujú pravidlá pre dôveryhodné služby, najmä elektronické transakcie;

c) zriaďuje právny rámec pre elektronické podpisy, elektronické pečate, elektronické časové pečiatky, elektronické dokumenty, elektronické doručovacie služby pre registrované zásielky, certifikačné služby pre autentifikáciu webových sídiel, elektronickú archiváciu, elektronické osvedčenie atribútov, zariadenia na vyhotovenie elektronického podpisu, zariadenia na vyhotovenie elektronickej pečate a elektronické registre.“

2. Článok 2 sa mení takto:

a) odsek 1 sa nahrádza takto:

„1. Toto nariadenie sa vzťahuje na schémy elektronickej identifikácie oznámené členskými štátmi, európske peňaženky digitálnej identity poskytované členskými štátmi a na poskytovateľov dôveryhodných služieb usadených v Únii.“;

b) odsek 3 sa nahrádza takto:

„3. Toto nariadenie nemá vplyv na právo Únie ani na vnútroštátne právo súvisiace s uzatváraním a platnosťou zmlúv, iné právne či procesné záväzky týkajúce sa formy alebo sektorovo špecifické požiadavky týkajúce sa formy.

4. Týmto nariadením nie je dotknuté nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679*.

---

* 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).“

3. Článok 3 sa mení takto:

a) body 1 až 5 nahrádzajú 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 inú fyzickú alebo právnickú osobu;

2. „prostriedok elektronickej identifikácie“ je hmotná a/alebo nehmotná jednotka, ktorá obsahuje osobné identifikačné údaje a ktorá sa používa na autentifikáciu v rámci online služby, alebo v príslušnom prípade offline služby;

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

4. „schéma elektronickej identifikácie“ je systém na elektronickú identifikáciu, v rámci ktorého sa fyzickým alebo právnickým osobám alebo fyzickým osobám zastupujúcim iné fyzické alebo právnické osoby vydávajú prostriedky elektronickej identifikácie ;

5. „autentifikácia“ je elektronický proces, ktorý umožňuje potvrdenie elektronickej identifikácie fyzickej alebo právnickej osoby alebo potvrdenie pôvodu a integrity údajov v elektronickej forme;“;

b) vkladá sa tento bod:

„5a. „používateľ“ je fyzická alebo právnická osoba alebo fyzická osoba zastupujúca inú fyzickú alebo právnickú osobu, ktorá využíva dôveryhodné služby alebo prostriedky elektronickej identifikácie poskytované v súlade s týmto nariadením;“**;**

c) bod 6 sa nahrádza takto:

„6. „spoliehajúca sa strana“ je fyzická alebo právnická osoba, ktorá sa spolieha na elektronickú identifikáciu, európske peňaženky digitálnej identity, iné prostriedky elektronickej identifikácie alebo na dôveryhodnú službu;“;

d) bod 16 sa nahrádza takto:

„16. „dôveryhodná služba“ je elektronická služba, ktorá sa spravidla poskytuje za protihodnotu a spočíva v ktorejkoľvek z týchto činností:

a) vydávanie certifikátov pre elektronické podpisy, certifikátov pre elektronické pečate, certifikátov pre autentifikáciu webových sídiel alebo certifikátov na poskytovanie iných dôveryhodných služieb;

b) validácia certifikátov pre elektronické podpisy, certifikátov pre elektronické pečate, certifikátov pre autentifikáciu webových sídiel alebo certifikátov na poskytovanie iných dôveryhodných služieb;

c) vyhotovovanie elektronických podpisov alebo elektronických pečatí;

d) validácia elektronických podpisov alebo elektronických pečatí;

e) uchovávanie elektronických podpisov, elektronických pečatí, certifikátov pre elektronické podpisy alebo certifikátov pre elektronické pečate;

f) správa zariadení na vyhotovenie elektronického podpisu na diaľku alebo zariadení na vyhotovenie elektronickej pečate na diaľku;

g) vydávanie elektronických osvedčení atribútov;

h) validácia elektronického osvedčenia atribútov;

i) vyhotovovanie elektronických časových pečiatok;

j) validácia elektronických časových pečiatok;

k) poskytovanie elektronickej doručovacej služby pre registrované zásielky;

l) validácia údajov prenášaných prostredníctvom elektronických doručovacích služieb pre registrované zásielky a súvisiacich dôkazov;

m) elektronická archivácia elektronických údajov a elektronických dokumentov;

n) zaznamenávanie elektronických údajov v elektronickom registri;“;

e) bod 18 sa nahrádza takto:

„18. „orgán posudzovania zhody“ je orgán posudzovania zhody v zmysle vymedzenia v článku 2 bode 13 nariadenia (ES) č. 765/2008, ktorý je v súlade s uvedeným nariadením akreditovaný ako orgán príslušný na posudzovanie zhody kvalifikovaného poskytovateľa dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytuje, alebo príslušný na certifikáciu európskych peňaženiek digitálnej identity alebo prostriedkov elektronickej identifikácie;“;

f) bod 21 sa nahrádza takto:

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

g) vkladajú sa tieto body:

„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; “;

h) bod 38 sa nahrádza takto:

„38. „certifikát pre autentifikáciu webového sídla“ je elektronické osvedčenie, ktoré umožňuje autentifikáciu webového sídla a spája webové sídlo s fyzickou alebo právnickou osobou, ktorej bol certifikát vydaný;“;

i) bod 41 sa nahrádza takto:

„41. „validácia“ je proces overenia a potvrdenia, že údaje v elektronickej forme sú platné v súlade s týmto nariadením;“;

j) dopĺňajú sa tieto body :

„42. „európska peňaženka digitálnej identity“ je prostriedok elektronickej identifikácie, ktorý používateľovi umožňuje bezpečne uchovávať, spravovať a validovať údaje o totožnosti osoby a elektronické osvedčenia atribútov na účely ich poskytnutia spoliehajúcim sa stranám a iným používateľom európskych peňaženiek digitálnej identity, ako aj podpisovať prostredníctvom kvalifikovaných elektronických podpisov alebo pečatiť prostredníctvom kvalifikovaných elektronických pečatí;

43. „atribút“ je črta, 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;

46. „elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene“ je elektronické osvedčenie atribútov, ktoré vydal subjekt verejného sektora zodpovedný za autentický zdroj alebo subjekt verejného sektora, ktorý členský štát určil na vydávanie takýchto osvedčení atribútov v mene subjektov verejného sektora zodpovedných za autentické zdroje v súlade s článkom 45f a s prílohou VII;

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

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

49. „kvalifikovaná elektronická archivačná služba“ je elektronická archivačná služba, ktorú poskytuje kvalifikovaný poskytovateľ dôveryhodných služieb a ktorá spĺňa požiadavky stanovené v článku 45j;

50. „značka dôvery EÚ pre peňaženku digitálnej identity“ je overiteľné, jednoduché a rozpoznateľné označenie, ktorým sa jasne oznamuje, že európska peňaženka digitálnej identity bola poskytnutá v súlade s týmto nariadením;

51. „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 vlastní len používateľ, alebo inherencia, niečo, čím používateľ je, a ktoré sú nezávislé v tom zmysle, že narušením jedného faktora sa neskompromituje spoľahlivosť ostatných faktorov, a je navrhnutá tak, aby sa ňou chránila dôvernosť autentifikačných údajov;

52. „elektronický register“ je postupnosť záznamov elektronických údajov, ktorá zabezpečuje integritu týchto záznamov a presnosť chronologického poradia týchto záznamov;

53. „kvalifikovaný elektronický register“ je elektronický register, ktorý poskytuje kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v článku 45l;

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

55. „párovanie totožnosti“ je proces, pri ktorom sa osobné identifikačné údaje alebo elektronické identifikačné prostriedky párujú alebo spájajú s existujúcim účtom patriacim rovnakej osobe ;

56. „záznam údajov“ sú elektronické údaje zaznamenané so súvisiacimi metaúdajmi, ktoré podporujú spracovanie údajov;

57. „offline režim“ je, pokiaľ ide o používanie európskych peňaženiek digitálnej identity, interakcia medzi používateľom a treťou stranou na fyzickom mieste s využitím technológií tesnej blízkosti, pričom na účely interakcie sa od európskej peňaženky digitálnej identity nevyžaduje prístup k diaľkovým systémom prostredníctvom elektronických komunikačných sietí.“

4. Článok 5 sa nahrádza takto:

„*Článok 5*
Pseudonymy v elektronickej transakcii

Používanie pseudonymov zvolených používateľom sa nezakazuje, pričom tým nie sú dotknuté osobitné pravidlá práva Únie alebo vnútroštátneho práva, podľa ktorých sa od používateľov vyžaduje, aby sa identifikovali, ani právny účinok pseudonymov podľa vnútroštátneho práva. “

5. V kapitole II sa vkladá tento oddiel:

„ODDIEL 1
EURÓPSKA PEŇAŽENKA DIGITÁLNEJ IDENTITY

Článok 5a
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 a zároveň mali plnú kontrolu nad svojimi údajmi, každý členský štát poskytne aspoň jednu európsku peňaženku digitálnej identity do 24 mesiacov odo dňa nadobudnutia účinnosti vykonávacích aktov uvedených v odseku 23 tohto článku a v článku 5c ods. 6.

2. Európske peňaženky digitálnej identity sa poskytnú jedným alebo viacerými z týchto spôsobov:

   a) priamo zo strany členského štátu;

   b) na základe poverenia členského štátu;

   c) nezávisle od členského štátu, ktorý však príslušný postup uznáva.

3. Zdrojový kód komponentov aplikačného softvéru európskych peňaženiek digitálnej identity má licenciu s otvoreným zdrojovým kódom. Členské štáty môžu ustanoviť, že zdrojový kód špecifických komponentov iných ako tie, ktoré sú nainštalované na zariadeniach používateľov, sa z riadne opodstatnených dôvodov nezverejní.

4. Európske peňaženky digitálnej identity umožňujú používateľovi používateľsky ústretovým, transparentným a vysledovateľným spôsobom:

a) pod výlučnou kontrolou používateľa bezpečne požadovať, získavať, vyberať, kombinovať, uchovávať, vymazávať, zdieľať a predkladať osobné identifikačné údaje, v príslušných prípadoch v kombinácii s elektronickými osvedčeniami atribútov, s cieľom autentifikovať sa spoliehajúcim sa stranám online a v príslušných prípadoch v offline režime, aby mohol mať prístup k verejným a súkromným službám, pričom sa zabezpečí možnosť selektívneho sprístupňovania údajov;

b) vytvárať pseudonymy a uchovávať ich zašifrované a lokálne v európskej peňaženke digitálnej identity;

c) bezpečne autentifikovať európsku peňaženku digitálnej identity inej osoby a prijímať a zdieľať údaje o totožnosti osoby a elektronické osvedčenia atribútov zabezpečeným spôsobom medzi dvoma európskymi peňaženkami digitálnej identity;

d) prístup k logu všetkých transakcií vykonaných prostredníctvom európskej peňaženky digitálnej identity prostredníctvom spoločného prehľadu, ktorý používateľovi umožní:

i) zobraziť aktuálny zoznam spoliehajúcich sa strán, s ktorými používateľ nadviazal spojenie, a v príslušnom prípade všetky vymenené údaje;

ii) jednoducho požiadať, aby spoliehajúca sa strana vymazala osobné údaje podľa článku 17 nariadenia (EÚ) 2016/679;

iii) v prípade prijatia údajne nezákonnej alebo podozrivej žiadosti o údaje jednoduchým spôsobom nahlásiť spoliehajúcu sa stranu príslušnému vnútroštátnemu orgánu pre ochranu údajov;

e) podpisovať pomocou kvalifikovaných elektronických podpisov alebo pečatiť pomocou kvalifikovaných elektronických pečatí;

f) sťahovať, pokiaľ je to technicky možné, používateľské údaje, elektronické osvedčenie atribútov a konfigurácie;

g) uplatňovať práva používateľa na prenosnosť údajov.

5. Európske peňaženky digitálnej identity najmä:

a) podporujú spoločné protokoly a rozhrania:

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

ii) pre spoliehajúce sa strany, aby mohli požadovať a validovať osobné identifikačné údaje a elektronické osvedčenia atribútov;

iii) na zdieľanie osobných identifikačných údajov, elektronického osvedčenia atribútov alebo selektívne sprístupnených súvisiacich údajov online a v príslušnom prípade v offline režime so spoliehajúcimi sa stranami a ich predkladanie spoliehajúcim sa stranám;

iv) pre používateľa s cieľom umožniť interakciu s európskou peňaženkou digitálnej identity a zobraziť značku dôvery EÚ pre peňaženku digitálnej identity;

v) na bezpečné pridanie používateľa použitím prostriedku elektronickej identifikácie v súlade s článkom 5a ods. 24;

vi) na interakciu medzi európskymi peňaženkami digitálnej identity dvoch osôb na účely bezpečného prijímania, validácie a zdieľania údajov o totožnosti osoby a elektronických osvedčení atribútov;

vii) na autentifikáciu a identifikáciu spoliehajúcich sa strán zavedením autentifikačných mechanizmov v súlade s článkom 5b;

viii) na overenie pravosti a platnosti európskych peňaženiek digitálnej identity spoliehajúcimi sa stranami;

ix) na požiadanie spoliehajúcej sa strany o vymazanie osobných údajov podľa článku 17 nariadenia (EÚ) 2016/679;

x) na nahlásenie spoliehajúcej sa strany príslušnému vnútroštátnemu orgánu pre ochranu údajov v prípade prijatia údajne nezákonnej alebo podozrivej žiadosti o údaje;

xi) na vyhotovenie kvalifikovaných elektronických podpisov alebo elektronických pečatí prostredníctvom zariadení na vyhotovenie kvalifikovaného elektronického podpisu alebo elektronickej pečate;

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

c) zabezpečujú, aby spoliehajúce sa strany mohli byť autentifikované a identifikované zavedením autentifikačných mechanizmov v súlade s článkom 5b;

d) spĺňajú požiadavky stanovené v článku 8, pokiaľ ide o úroveň zabezpečenia „vysoká“, najmä vo vzťahu k požiadavkám na preukazovanie a overovanie totožnosti a správu a autentifikáciu prostriedkov elektronickej identifikácie;

e) v prípade elektronického osvedčenia atribútov so zahrnutými pravidlami sprístupňovania informácií zavádzajú vhodný mechanizmus na informovanie používateľa, že spoliehajúca sa strana alebo používateľ európskej peňaženky digitálnej identity požaduje, aby elektronické osvedčenie atribútov malo povolenie na prístup k takémuto osvedčeniu;

f) zabezpečujú, aby osobné identifikačné údaje, ktoré sú dostupné zo schémy elektronickej identifikácie, v rámci ktorej sa poskytuje európska peňaženka digitálnej identity, jedinečne reprezentovali fyzickú osobu, právnickú osobu alebo fyzickú osobu zastupujúcu fyzickú alebo právnickú osobu a aby boli spojené s danou európskou peňaženkou digitálnej identity;

g) dávajú štandardne všetkým fyzickým osobám možnosť bezplatne sa podpisovať prostredníctvom kvalifikovaných elektronických podpisov.

Bez ohľadu na písmeno g) prvého pododseku môžu členské štáty stanoviť primerané opatrenia na zabezpečenie toho, aby sa bezplatné používanie kvalifikovaných elektronických podpisov fyzickými osobami obmedzilo na neprofesionálne účely.

6. Členský štát bezodkladne informuje používateľov o každom narušení bezpečnosti, ktoré by mohlo úplne alebo čiastočne skompromitovať ich európsku peňaženku digitálnej identity alebo jej obsah, najmä ak bola platnosť ich európskej peňaženky digitálnej identity pozastavená alebo zrušená podľa článku 5e.

7. Bez toho, aby bol dotknutý článok 5f, môžu členské štáty v súlade s vnútroštátnym právom stanoviť dodatočné funkcie európskych peňaženiek digitálnej identity vrátane interoperability s existujúcimi vnútroštátnymi prostriedkami elektronickej identifikácie. Tieto dodatočné funkcie musia byť v súlade s týmto článkom.

8. Členské štáty poskytnú mechanizmy validácie bezplatne s cieľom:

   a) zabezpečiť, aby bolo možné overiť pravosť a platnosť európskych peňaženiek digitálnej identity;

   b) umožniť používateľom overiť pravosť a platnosť totožnosti spoliehajúcich sa strán zaregistrovaných v súlade s článkom 5b.

9. Členské štáty zabezpečia, aby sa platnosť európskej peňaženky digitálnej identity mohla zrušiť za týchto okolností:

   a) na výslovnú žiadosť používateľa;

   b) ak bola skompromitovaná bezpečnosť európskej peňaženky digitálnej identity;

   c) po smrti používateľa alebo ukončení činnosti právnickej osoby.

10. Poskytovatelia európskych peňaženiek digitálnej identity zabezpečia, aby používatelia mohli ľahko požiadať o technickú podporu a oznamovať technické problémy alebo akékoľvek iné incidenty, ktoré majú negatívny vplyv na používanie európskych peňaženiek digitálnej identity.

11. Európske peňaženky digitálnej identity sa poskytujú v rámci schémy elektronickej identifikácie s úrovňou zabezpečenia „vysoká“.

12. Európske peňaženky digitálnej identity zaisťujú bezpečnosť už v štádiu návrhu.

13. Európske peňaženky digitálnej identity sa pre všetky fyzické osoby vydávajú, používajú a zneplatňujú bezplatne.

14. Používatelia majú plnú kontrolu nad používaním svojej európskej peňaženky digitálnej identity a údajmi v nej. Pokiaľ používateľ výslovne nepožiada inak, poskytovateľ európskej peňaženky digitálnej identity nezískava informácie o používaní európskej peňaženky digitálnej identity, ktoré nie sú potrebné na poskytovanie služieb európskej peňaženky digitálnej identity, ani nekombinuje osobné identifikačné údaje ani žiadne iné osobné údaje uchovávané alebo súvisiace s používaním európskej peňaženky digitálnej identity s osobnými údajmi zo žiadnych iných služieb, ktoré ponúka alebo ktoré ponúkajú tretie strany, ktoré nie sú potrebné na poskytovanie služieb európskej peňaženky digitálnej identity. Osobné údaje týkajúce sa poskytovania európskej peňaženky digitálnej identity sa uchovávajú logicky oddelené od akýchkoľvek iných údajov v držbe poskytovateľa európskej peňaženky digitálnej identity. Ak európsku peňaženku digitálnej identity poskytujú súkromné subjekty v súlade s odsekom 2 písm. b) a c) tohto článku, ustanovenia článku 45h ods. 3 sa uplatňujú *mutatis mutandis*.

15. Používanie európskych peňaženiek digitálnej identity je dobrovoľné. Fyzickým alebo právnickým osobám, ktoré nepoužívajú európske peňaženky digitálnej identity, sa nesmie nijako obmedziť ani znevýhodniť prístup k verejným a súkromným službám, trhu práce a slobode podnikania. Prístup k verejným a súkromným službám musí byť aj naďalej možný prostredníctvom iných existujúcich prostriedkov identifikácie a autentifikácie.

16. Technický rámec európskej peňaženky digitálnej identity:

    a) neumožňuje poskytovateľom elektronických osvedčení atribútov ani akejkoľvek inej strane po vydaní osvedčenia atribútov získavať údaje, ktoré umožňujú sledovať transakcie alebo správanie používateľov, prepájať ich alebo vytvárať medzi nimi vzťahy, alebo inak získavať informácie o transakciách či správaní používateľov, pokiaľ to používateľ výslovne nepovolí;

    b) umožňuje techniky ochrany súkromia, ktoré zabezpečujú neprepojiteľnosť, ak si osvedčenie atribútov nevyžaduje identifikáciu používateľa.

17. Každé spracúvanie osobných údajov vykonávané členskými štátmi alebo v ich mene orgánmi alebo stranami zodpovednými za poskytovanie európskych peňaženiek digitálnej identity ako prostriedkov elektronickej identifikácie sa vykonáva v súlade s náležitými a účinnými opatreniami na ochranu údajov. Musí sa preukázať súlad takéhoto spracúvania s nariadením (EÚ) 2016/679. Členské štáty môžu zaviesť vnútroštátne ustanovenia na ďalšie spresnenie uplatňovania takýchto opatrení.

18. Členské štáty bez zbytočného odkladu oznámia Komisii informácie o:

a) orgáne zodpovednom za zostavenie a vedenie zoznamu registrovaných spoliehajúcich sa strán, ktoré využívajú európske peňaženky digitálnej identity v súlade s článkom 5b ods. 5, a umiestnenie tohto zoznamu;

b) orgánoch zodpovedných za poskytovanie európskych peňaženiek digitálnej identity v súlade s článkom 5a ods. 1;

c) orgánoch zodpovedných za zabezpečenie toho, aby osobné identifikačné údaje boli spojené s európskou peňaženkou digitálnej identity v súlade s článkom 5a ods. 5 písm. f);

d) mechanizme umožňujúcom validáciu osobných identifikačných údajov uvedených v článku 5a ods. 5 písm. f) a totožnosti spoliehajúcich sa strán;

e) mechanizme overovania pravosti a platnosti európskych peňaženiek digitálnej identity.

Komisia zverejní informácie oznámené podľa prvého pododseku prostredníctvom zabezpečeného kanála v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

19. Bez toho, aby bol dotknutý odsek 22 tohto článku, sa článok 11 uplatňuje na európsku peňaženku digitálnej identity *mutatis mutandis*.

20. Článok 24 ods. 2 písm. b) a d) až h) sa uplatňujú na poskytovateľov európskych peňaženiek digitálnej identity *mutatis mutandis*.

21. Európske peňaženky digitálnej identity sa sprístupňujú na používanie osobám so zdravotným postihnutím na rovnakom základe ako ostatným používateľom v súlade so smernicou Európskeho parlamentu a Rady (EÚ) 2019/882[*].

22. Na účely poskytovania európskych peňaženiek digitálnej identity sa na európske peňaženky digitálnej identity a schémy elektronickej identifikácie, v rámci ktorých sa poskytujú, nevzťahujú požiadavky stanovené v článkoch 7, 9, 10, 12 a 12a.

23. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre požiadavky uvedené v odsekoch 4, 5, 8 a 18 tohto článku týkajúce sa implementácie európskej peňaženky digitálnej identity. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

24. Komisia prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy s cieľom uľahčiť pridávanie používateľov do európskej peňaženky digitálnej identity buď prostriedkami elektronickej identifikácie, ktoré zodpovedajú úrovni záruky „vysoká“, alebo prostriedkami elektronickej identifikácie, ktoré zodpovedajú úrovni záruky „významná“ v spojení s dodatočnými postupmi ich pridávania, ktoré spolu spĺňajú požiadavky úrovne záruky „vysoká“. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 5b

Spoliehajúce sa strany v prípade európskych peňaženiek digitálnej identity

1. Ak má spoliehajúca sa strana v úmysle využívať európske peňaženky digitálnej identity na poskytovanie verejných alebo súkromných služieb prostredníctvom digitálnej interakcie, zaregistruje sa v členskom štáte, v ktorom je usadená .

2. Proces registrácie musí byť nákladovo efektívny a primeraný riziku. Spoliehajúca sa strana poskytne aspoň:

   a) informácie potrebné na autentifikáciu európskych peňaženiek digitálnej identity, ktoré zahŕňajú prinajmenšom:

      i) členský štát, v ktorom je spoliehajúca sa strana usadená; a

      ii) názov spoliehajúcej sa strany a v príslušných prípadoch jej registračné číslo uvedené v úradnom registri spolu s identifikačnými údajmi daného úradného registra;

b) kontaktné údaje spoliehajúcej sa strany;

c) zamýšľané použitie európskych peňaženiek digitálnej identity vrátane určenia údajov, ktoré bude spoliehajúca sa strana požadovať od používateľov.

3. Spoliehajúce sa strany nesmú od používateľov požadovať poskytnutie iných údajov, než sú údaje určené podľa odseku 2 písm. c).

4. Odsekmi 1 a 2 nie je dotknuté právo Únie ani vnútroštátne právo uplatniteľné na poskytovanie konkrétnych služieb.

5. Členské štáty sprístupnia informácie uvedené v odseku 2 verejnosti online v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

6. Spoliehajúce sa strany zaregistrované v súlade s týmto článkom bezodkladne informujú členské štáty o akýchkoľvek zmenách informácií poskytnutých počas registrácie podľa odseku 2.

7. Členské štáty ustanovia spoločný mechanizmus umožňujúci identifikáciu a autentifikáciu spoliehajúcich sa strán, ako sa uvádza v článku 5a ods. 5 písm. c).

8. Ak majú spoliehajúce sa strany v úmysle používať európske peňaženky digitálnej identity, identifikujú sa používateľovi.

9. Spoliehajúce sa strany sú zodpovedné za vykonanie postupu autentifikácie a validácie osobných identifikačných údajov a elektronického osvedčenia atribútov požadovaných od európskych peňaženiek digitálnej identity. Spoliehajúce sa strany nesmú odmietnuť použitie pseudonymov, ak sa podľa práva Únie alebo vnútroštátneho práva identifikácia používateľa nevyžaduje.

10. Sprostredkovatelia konajúci v mene spoliehajúcich sa strán sa považujú za spoliehajúce sa strany a neuchovávajú údaje o obsahu transakcie.

11. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] stanoví technické špecifikácie a postupy týkajúce sa požiadaviek uvedených v odsekoch 2, 5 a 6 až 9 tohto článku prostredníctvom vykonávacích aktov o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 5a ods. 23. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 5c

Certifikácia európskych peňaženiek digitálnej identity

1. Súlad európskych peňaženiek digitálnej identity a schémy elektronickej identifikácie, v rámci ktorej sa poskytujú, s požiadavkami stanovenými v článku 5a ods. 4, 5 a 8, požiadavkou logického oddelenia stanovenou v článku 5a ods. 14 a v príslušnom prípade s normami a technickými špecifikáciami uvedenými v článku 5a ods. 24 certifikujú orgány posudzovania zhody určené členskými štátmi.

2. Certifikácia súladu európskych peňaženiek digitálnej identity s požiadavkami uvedenými v odseku 1 tohto článku alebo ich časťami, ktoré sú relevantné pre kybernetickú bezpečnosť, sa vykonáva v súlade s európskymi schémami certifikácie kybernetickej bezpečnosti prijatými podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881** a uvedenými vo vykonávacích aktoch uvedených v odseku 6 tohto článku.

3. Pokiaľ ide o požiadavky uvedené v odseku 1 tohto článku, ktoré nie sú relevantné pre kybernetickú bezpečnosť, a o požiadavky uvedené v odseku 1 tohto článku, ktoré sú relevantné pre kybernetickú bezpečnosť, v rozsahu v akom schémy certifikácie kybernetickej bezpečnosti uvedené v odseku 2 tohto článku na uvedené požiadavky kybernetickej bezpečnosti nevzťahujú alebo sa na ne vzťahujú len čiastočne, členské štáty tiež pre tieto požiadavky zriadia vnútroštátne schémy certifikácie v súlade s požiadavkami stanovenými vo vykonávacích aktoch uvedených v odseku 6 tohto článku. Členské štáty zašlú svoje návrhy vnútroštátnych schém certifikácie skupine pre európsku spoluprácu v oblasti digitálnej identity zriadenej podľa článku 46e ods. 1 (ďalej len „skupina pre spoluprácu“). Skupina pre spoluprácu môže vydať stanoviská a odporúčania.

4. Certifikácia podľa odseku 1 platí najviac päť rokov za predpokladu, že každé dva roky sa vykoná posúdenie zraniteľnosti. Ak sa zistí zraniteľnosť a neodstráni sa včas, certifikácia sa zruší.

5. Súlad s požiadavkami stanovenými v článku 5a tohto nariadenia a súvisiacimi s operáciami spracúvania osobných údajov sa môže certifikovať podľa nariadenia (EÚ) 2016/679.

6. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy certifikácie európskych peňaženiek digitálnej identity uvedenej v odsekoch 1, 2 a 3 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

7. Členské štáty oznámia Komisii názvy a adresy orgánov posudzovania zhody uvedených v odseku 1. Komisia sprístupní tieto informácie všetkým členským štátom.

8. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 47, ktorými stanoví osobitné kritériá, ktoré majú spĺňať určené orgány posudzovania zhody uvedené v odseku 1 tohto článku.

Článok 5d

Uverejnenie zoznamu certifikovaných európskych peňaženiek digitálnej identity

1. Členské štáty bez zbytočného odkladu informujú Komisiu a skupinu pre spoluprácu zriadenú podľa článku 46e ods. 1 o európskych peňaženkách digitálnej identity, ktoré boli poskytnuté podľa článku 5a a certifikované orgánmi posudzovania zhody uvedenými v článku 5c ods. 1. V prípade zrušenia certifikácie o tom bez zbytočného odkladu informujú Komisiu a skupinu pre spoluprácu zriadenú podľa článku 46e ods. 1, pričom uvedú dôvody zrušenia.

2. Bez toho, aby bol dotknutý článok 5a ods. 18, informácie poskytnuté členskými štátmi a uvedené v odseku 1 tohto článku zahŕňajú aspoň:

   a) certifikát a správu o posúdení certifikácie certifikovanej európskej peňaženky digitálnej identity;

   b) opis schémy elektronickej identifikácie, v rámci ktorej sa poskytuje európska peňaženka digitálnej identity;

   c) uplatniteľný režim dohľadu a informácie o režime zodpovednosti, pokiaľ ide o stranu poskytujúcu európsku peňaženku digitálnej identity;

   d) orgán alebo orgány zodpovedné za schému elektronickej identifikácie;

   e) opatrenia na pozastavenie alebo zrušenie schémy elektronickej identifikácie alebo autentifikácie alebo dotknutých skompromitovaných častí.

3. Na základe informácií získaných podľa odseku 1 Komisia vypracuje, uverejní v *Úradnom vestníku Európskej úni*e a vedie v strojovo čitateľnej forme zoznam certifikovaných európskych peňaženiek digitálnej identity.

4. Členský štát môže Komisii predložiť žiadosť o odstránenie európskej peňaženky digitálnej identity a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, zo zoznamu uvedeného v odseku 3.

5. Ak sa informácie poskytnuté podľa odseku 1 zmenia, členský štát poskytne Komisii aktualizované informácie.

6. Komisia aktualizuje zoznam uvedený v odseku 3 tak, že v *Úradnom vestníku Európskej úni*e uverejní zodpovedajúce zmeny zoznamu do jedného mesiaca od doručenia žiadosti podľa odseku 4 alebo aktualizovaných informácií podľa odseku 5.

7. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] stanoví formáty a postupy uplatniteľné na účely odsekov 1, 4 a 5 tohto článku prostredníctvom vykonávacích aktov o implementácii európskych peňaženiek digitálnej identity, ako sa uvádza v článku 5a ods. 23. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 5e

Narušenie bezpečnosti európskych peňaženiek digitálnej identity

1. Ak sú európske peňaženky digitálnej identity poskytnuté podľa článku 5a, mechanizmy validácie uvedené v článku 5a ods. 8 alebo schéma elektronickej identifikácie, v rámci ktorej sa poskytujú európske peňaženky digitálnej identity, predmetom narušenia bezpečnosti alebo čiastočnej kompromitácie spôsobom, ktorý má dosah na ich spoľahlivosť alebo spoľahlivosť iných európskych peňaženiek digitálnej identity, členský štát, ktorý európske peňaženky digitálnej identity poskytol, ich poskytovanie a používanie bez zbytočného odkladu pozastaví.

   Ak je to odôvodnené závažnosťou narušenia bezpečnosti alebo kompromitácie uvedených v prvom pododseku, členský štát bez zbytočného odkladu európske peňaženky digitálnej identity stiahne.

Členský štát zodpovedajúcim spôsobom informuje dotknutých používateľov, jednotné kontaktné miesta určené podľa článku 46c ods. 1, spoliehajúce sa strany a Komisiu.

2. Ak sa narušenie bezpečnosti alebo kompromitácia uvedené v odseku 1 prvom pododseku tohto článku nenapraví do troch mesiacov od pozastavenia, členský štát, ktorý poskytol európske peňaženky digitálnej identity, ich stiahne a zruší ich platnosť. Členský štát o stiahnutí zodpovedajúcim spôsobom informuje dotknutých používateľov, jednotné kontaktné miesta určené podľa článku 46c ods. 1, spoliehajúce sa strany a Komisiu.

3. Ak dôjde k náprave narušenia bezpečnosti alebo kompromitácie uvedených v odseku 1 prvom pododseku tohto článku, poskytujúci členský štát obnoví poskytovanie a používanie európskych peňaženiek digitálnej identity a bez zbytočného odkladu informuje dotknutých používateľov a spoliehajúce sa strany, jednotné kontaktné miesta určené podľa článku 46c ods. 1 a Komisiu.

4. Komisia bez zbytočného odkladu uverejní zodpovedajúce zmeny zoznamu uvedeného v článku 5d v *Úradnom vestníku Európskej úni*e.

5. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre opatrenia uvedené v odsekoch 1, 2 a 3 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 5f

Cezhraničné využívanie európskych peňaženiek digitálnej identity

1. Ak členské štáty vyžadujú na prístup k online službe, ktorú poskytuje subjekt verejného sektora, elektronickú identifikáciu a autentifikáciu, akceptujú aj európske peňaženky digitálnej identity, ktoré sa poskytujú v súlade s týmto nariadením.

2. Ak sa od súkromných spoliehajúcich sa strán, ktoré poskytujú služby, s výnimkou mikropodnikov a malých podnikov v zmysle vymedzenia v článku 2 prílohy k odporúčaniu Komisie 2003/361/ES[***], vyžaduje podľa práva Únie alebo vnútroštátneho práva, aby na online identifikáciu používali silnú autentifikáciu používateľa, alebo ak sa silná autentifikácia používateľa na online identifikáciu vyžaduje na základe zmluvnej povinnosti, a to aj v oblasti dopravy, energetiky, bankovníctva, finančných služieb, sociálneho zabezpečenia, zdravotníctva, pitnej vody, poštových služieb, digitálnej infraštruktúry, vzdelávania alebo telekomunikácií, tieto súkromné spoliehajúce sa strany najneskôr do 36 mesiacov odo dňa nadobudnutia účinnosti vykonávacích aktov uvedených v článku 5a ods. 23 a článku 5c ods. 6 a len na základe dobrovoľnej žiadosti používateľa akceptujú aj európske peňaženky digitálnej identity, ktoré sa poskytujú v súlade s týmto nariadením.

3. Ak poskytovatelia veľmi veľkých online platforiem uvedených v článku 33 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2065[****] vyžadujú autentifikáciu používateľov na prístup k online službám, akceptujú a uľahčujú aj používanie európskych peňaženiek digitálnej identity, ktoré sa poskytujú v súlade s týmto nariadením na účely autentifikácie používateľov len na základe dobrovoľnej žiadosti používateľa a za použitia minimálnych údajov potrebných pre konkrétnu online službu, pre ktorú sa autentifikácia požaduje.

4. Komisia v spolupráci s členskými štátmi uľahčí vypracovanie kódexov správania v úzkej spolupráci so všetkými príslušnými zainteresovanými stranami vrátane občianskej spoločnosti s cieľom prispieť k širokej dostupnosti a použiteľnosti európskych peňaženiek digitálnej identity v rozsahu pôsobnosti tohto nariadenia a nabádať poskytovateľov služieb, aby vypracovanie kódexov správania dokončili.

5. Komisia do 24 mesiacov od zavedenia európskych peňaženiek digitálnej identity posúdi dopyt po európskych peňaženkách digitálnej identity, a ich dostupnosť a použiteľnosť, pričom zohľadní kritériá, ako je rozšírenie medzi používateľmi, cezhraničná prítomnosť poskytovateľov služieb, technologický vývoj, vývoj modelov používania a dopyt spotrebiteľov.

---

* 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).

** 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).

*** Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení mikropodnikov, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003, s. 36).

**** Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) (Ú. v. EÚ L 277, 27.10.2022, s. 1).“

6. Pred článok 6 sa vkladá tento nadpis:

„ODDIEL 2
SCHÉMY ELEKTRONICKEJ IDENTIFIKÁCIE“

7. V článku 7 sa písmeno g) nahrádza takto:

„g) najmenej šesť mesiacov pred oznámením podľa článku 9 ods. 1 poskytne oznamujúci členský štát ostatným členským štátom na účely článku 12 ods. 5 opis uvedenej schémy v súlade s dojednaniami o postupe stanovenými vo vykonávacích aktoch prijatých podľa článku 12 ods. 6;“

8. V článku 8 ods. 3 sa prvý pododsek nahrádza takto:

„3. S výhradou odseku 2 a s ohľadom na príslušné medzinárodné normy Komisia do 18. septembra 2015 prostredníctvom vykonávacích aktov stanoví minimálne technické špecifikácie, normy a postupy, na ktoré sa odkazuje pri špecifikácii úrovní záruky prostriedkov elektronickej identifikácie „nízka“, „významná“ a „vysoká“.“

9. V článku 9 sa odseky 2 a 3 nahrádzajú takto:

„2. Komisia bez zbytočného odkladu uverejní v *Úradnom vestníku Európskej únie* zoznam schém elektronickej identifikácie, ktoré boli oznámené podľa odseku 1, spolu so základnými informáciami o týchto schémach.

3. Komisia uverejní zmeny zoznamu uvedeného v odseku 2 v *Úradnom vestníku Európskej únie* do jedného mesiaca od doručenia daného oznámenia.“

10. V článku 10 sa názov nahrádza takto:

„Narušenie bezpečnosti schém elektronickej identifikácie“

11. Vkladá sa tento článok :

„*Článok 11a*
Cezhraničné párovanie totožnosti

1. Keď členské štáty konajú ako spoliehajúce sa strany pre cezhraničné služby, zabezpečia jednoznačné párovanie totožnosti fyzických osôb pomocou oznámených prostriedkov elektronickej identifikácie alebo európskych peňaženiek digitálnej identity.

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

3. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vytvorí zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre požiadavky uvedené v odseku 1 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

12. Článok 12 sa mení takto:

a) názov sa nahrádza takto:

„Interoperabilita“;

b) odsek 3 sa mení takto:

i) písmeno c) sa nahrádza takto:

„c) uľahčuje uplatňovanie ochrany súkromia a bezpečnosti už v štádiu návrhu;“;

ii) písmeno d) sa vypúšťa;

c) v odseku 4 sa písmeno d) nahrádza takto:

„d) odkaz na minimálny súbor osobných identifikačných údajov potrebných na jedinečnú reprezentáciu fyzickej alebo právnickej osoby alebo fyzickej osoby zastupujúcej inú fyzickú alebo právnickú osobu, ktorý je k dispozícii zo schém elektronickej identifikácie;“;

d) odseky 5 a 6 sa nahrádzajú takto:

„5. Členské štáty vykonávajú vzájomné preskúmania schém elektronickej identifikácie, ktoré patria do rozsahu pôsobnosti tohto nariadenia a ktoré sa majú oznamovať podľa článku 9 ods. 1 písm. a).

6. Komisia do 18. marca 2025 prostredníctvom vykonávacích aktov stanoví potrebné dojednania o postupe pre vzájomné preskúmania uvedené v odseku 5 tohto článku s cieľom posilniť vysokú úroveň dôvery a bezpečnosti primeranú stupňu rizika. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“;

e) odsek 7 sa vypúšťa;

f) odsek 8 sa nahrádza takto:

„8. Na účely stanovenia jednotných podmienok vykonávania požiadavky podľa odseku 1 tohto článku prijme Komisia do 18. septembra 2025 v súlade s kritériami stanovenými v odseku 3 tohto článku a s prihliadnutím na výsledky spolupráce medzi členskými štátmi vykonávacie akty týkajúce sa rámca interoperability, ako sa stanovuje v odseku 4 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

13. V kapitole II sa vkladajú tieto články:

„*Článok 12a*

Certifikácia schém elektronickej identifikácie

1. Zhodu schém elektronickej identifikácie, ktoré sa majú oznamovať, s požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení vrátane zhody s požiadavkami relevantnými z hľadiska kybernetickej bezpečnosti stanovenými v článku 8 ods. 2, pokiaľ ide o úrovne záruky schém elektronickej identifikácie, certifikujú orgány posudzovania zhody určené členskými štátmi.

2. Certifikácia podľa odseku 1 tohto článku sa vykonáva v rámci príslušnej schémy certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 alebo jeho častí, pokiaľ sa certifikát kybernetickej bezpečnosti alebo jeho časti vzťahujú na uvedené požiadavky kybernetickej bezpečnosti.

3. Certifikácia podľa odseku 1 platí najviac päť rokov za predpokladu, že každé dva roky sa vykoná posúdenie zraniteľnosti. Ak sa zistí zraniteľnosť a neodstráni sa do troch mesiacov od jej zistenia, certifikácia sa zruší.

4. Bez ohľadu na odsek 2 môžu členské štáty požiadať v súlade s uvedeným odsekom oznamujúci členský štát o dodatočné informácie o schémach certifikácie elektronickej identifikácie alebo ich častiach.

5. Vzájomné preskúmanie schém elektronickej identifikácie uvedené v článku 12 ods. 5 sa nevzťahuje na schémy elektronickej identifikácie alebo časti takýchto schém certifikovaných v súlade s odsekom 1 tohto článku. Pokiaľ ide o úrovne zabezpečenia schém elektronickej identifikácie, členské štáty môžu používať certifikát alebo vyhlásenie zhody s inými ako kybernetickobezpečnostnými požiadavkami stanovenými v článku 8 ods. 2, ktoré bolo vydané v súlade s príslušnou schémou certifikácie alebo časťami takýchto schém.

6. Členské štáty oznámia Komisii názvy a adresy orgánov posudzovania zhody uvedených v odseku 1. Komisia sprístupní tieto informácie všetkým členským štátom.

Článok 12b

Prístup k hardvérovým a softvérovým funkciám

Ak sú poskytovatelia európskych peňaženiek digitálnej identity a vydavatelia oznámených prostriedkov elektronickej identifikácie, ktorí konajú v rámci obchodnej alebo profesionálnej činnosti a využívajú základné platformové služby vymedzené v článku 2 bode 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/1925* na účely alebo v priebehu poskytovania služieb európskej peňaženky digitálnej identity a prostriedkov elektronickej identifikácie koncovým používateľom, komerčnými používateľmi v zmysle vymedzenia v článku 2 bodu 21 uvedeného nariadenia, strážcovia prístupu im najmä umožnia skutočnú interoperabilitu s rovnakým operačným systémom a hardvérovými alebo softvérovými funkciami a prístup k nim na účely interoperability. Takáto skutočná interoperabilita a prístup sa umožní bezplatne a bez ohľadu na to, či sú hardvérové alebo softvérové funkcie súčasťou operačného systému, ktoré má daný strážca prístupu k dispozícii alebo ktoré tento strážca prístupu používa pri poskytovaní takýchto služieb v zmysle článku 6 ods. 7 nariadenia (EÚ) 2022/1925. Týmto článkom nie je dotknutý článok 5a ods. 14 tohto nariadenia.

---

* Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/1925 zo 14. septembra 2022 o súťaži schopných a spravodlivých trhoch digitálneho sektora a o zmene smerníc (EÚ) 2019/1937 a (EÚ) 2020/1828 (akt o digitálnych trhoch) (Ú. v. EÚ L 265, 12.10.2022, s. 1).“

14. V článku 13 sa odsek 1 nahrádza takto:

„1. Bez ohľadu na odsek 2 tohto článku a bez toho, aby bolo dotknuté nariadenie (EÚ) 2016/679, poskytovatelia dôveryhodných služieb zodpovedajú za škodu spôsobenú úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe v dôsledku nesplnenia povinností podľa tohto nariadenia. Každá fyzická alebo právnická osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia poskytovateľom dôveryhodných služieb, má právo požadovať náhradu škody v súlade s právom Únie a vnútroštátnym právom.

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.“

15. Články 14, 15 a 16 sa nahrádzajú takto:

„*Článok 14*
Medzinárodné aspekty

1. Dôveryhodné služby poskytované poskytovateľmi dôveryhodných služieb usadenými v tretej krajine alebo medzinárodnou organizáciou sa uznávajú za právne rovnocenné s kvalifikovanými dôveryhodnými službami poskytovanými kvalifikovanými poskytovateľmi dôveryhodných služieb usadenými v Únii, ak sú dôveryhodné služby pôvodom z tretej krajiny alebo z medzinárodnej organizácie uznané prostredníctvom vykonávacích aktov alebo dohody uzavretej medzi Úniou a treťou krajinou alebo medzinárodnou organizáciou podľa článku 218 ZFEÚ.

   Vykonávacie akty uvedené v prvom pododseku sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

2. Vykonávacími aktmi a dohodou uvedenými v odseku 1 sa zabezpečí, aby poskytovatelia dôveryhodných služieb v dotknutej tretej krajine alebo medzinárodné organizácie a dôveryhodné služby, ktoré poskytujú, spĺňali požiadavky uplatniteľné na kvalifikovaných poskytovateľov dôveryhodných služieb usadených v Únii a na kvalifikované dôveryhodné služby, ktoré poskytujú. Tretie krajiny a medzinárodná organizácia predovšetkým vypracujú, vedú a uverejňujú dôveryhodný zoznam uznaných poskytovateľov dôveryhodných služieb.

3. Dohodou uvedenou v odseku 1 sa zabezpečí, aby kvalifikované dôveryhodné služby poskytované kvalifikovanými poskytovateľmi dôveryhodných služieb usadenými v Únii boli uznané za právne rovnocenné s dôveryhodnými službami poskytovanými poskytovateľmi dôveryhodných služieb v tretej krajine alebo medzinárodnou organizáciou, s ktorou je dohoda uzavretá.

Článok 15

Prístupnosť pre osoby so zdravotným postihnutím a s osobitnými potrebami

Poskytovanie prostriedkov elektronickej identifikácie, dôveryhodných služieb a produktov pre koncových používateľov, ktoré sa používajú pri poskytovaní týchto služieb, sa uskutočňuje v jasnom a zrozumiteľnom jazyku v súlade s Dohovorom Organizácie Spojených národov o právach osôb so zdravotným postihnutím a s požiadavkami na prístupnosť v smernici (EÚ) 2019/882, z čoho budú mať prospech aj osoby s funkčnými obmedzeniami, ako sú starší ľudia, a osoby s obmedzeným prístupom k digitálnym technológiám.

Článok 16

Sankcie

1. Bez toho, aby bol dotknutý článok 31 smernice Európskeho parlamentu a Rady (EÚ) 2022/2555[*], členské štáty stanovia pravidlá týkajúce sa sankcií uplatniteľných v prípade porušenia tohto nariadenia. Uvedené sankcie musia byť účinné, primerané a odrádzajúce.

2. Členské štáty zabezpečia, aby sa za porušenie tohto nariadenia kvalifikovanými a nekvalifikovanými poskytovateľmi dôveryhodných služieb ukladali správne pokuty v maximálnej výške aspoň:

   a) 5 000 000 EUR, ak je poskytovateľom dôveryhodných služieb fyzická osoba; alebo

   b) ak je poskytovateľom dôveryhodných služieb právnická osoba, 5 000 000 EUR alebo 1 % celkového celosvetového ročného obratu podniku, ku ktorému poskytovateľ dôveryhodných služieb patril vo finančnom roku predchádzajúcom roku, v ktorom došlo k porušeniu, podľa toho, ktorá suma je vyššia.

3. V závislosti od právneho systému členských štátov sa pravidlá o správnych pokutách môžu uplatňovať tak, že pokutu iniciuje príslušný orgán dohľadu a ukladajú ju príslušné vnútroštátne súdy. Uplatňovaním takýchto pravidiel v uvedených členských štátoch sa zabezpečí, aby tieto právne prostriedky nápravy boli účinné a mali rovnocenný účinok ako správne pokuty uložené priamo dozornými orgánmi.

---

* Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).“

16. V kapitole III, oddiele 2 sa názov nahrádza takto:

„Nekvalifikované dôveryhodné služby“

17. Články 17 a 18 sa vypúšťajú.

18. V kapitole III oddiele 2 sa vkladá tento článok:

„*Článok 19a*
Požiadavky na nekvalifikovaných poskytovateľov dôveryhodných služieb

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

a) mať vhodné politiky a prijímať zodpovedajúce opatrenia na riadenie právnych, obchodných, prevádzkových a iných priamych alebo nepriamych rizík poskytovania nekvalifikovanej dôveryhodnej služby, ktoré bez ohľadu na článok 21 smernice (EÚ) 2022/2555 zahŕňajú aspoň opatrenia týkajúce sa:

i) postupov registrácie a pridávania používateľov dôveryhodnej služby;

ii) procesných alebo administratívnych kontrol potrebných na poskytovanie dôveryhodných služieb;

iii) riadenia a implementácie dôveryhodných služieb;

b) oznámiť orgánu dohľadu, identifikovateľným dotknutým jednotlivcom, verejnosti, ak je to vo verejnom záujme, a v príslušnom prípade iným relevantným príslušným orgánom všetky narušenia bezpečnosti alebo narušenia poskytovania služby alebo vykonávania opatrení uvedených v písmene a) bode i), ii) alebo iii), ktoré majú významný vplyv na poskytovanú dôveryhodnú službu alebo na osobné údaje v nej uchovávané, a to bez zbytočného odkladu a v každom prípade najneskôr do 24 hodín po tom, ako sa o akýchkoľvek narušeniach bezpečnosti alebo ďalších narušeniach dozvedel.

2. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre odsek 1 písm. a) tohto článku. Ak sú tieto normy, špecifikácie a postupy splnené, predpokladá sa, že sa dosiahol súlad s požiadavkami stanovenými v tomto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

19. 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. Auditom sa potvrdí, že kvalifikovaní poskytovatelia dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky stanovené v tomto nariadení a v článku 21 smernice (EÚ) 2022/2555. Kvalifikovaní poskytovatelia dôveryhodných služieb predložia výslednú správu o posúdení zhody orgánu dohľadu do troch pracovných dní od jej doručenia.“;

b) vkladajú sa tieto odseky:

„1a. Kvalifikovaní poskytovatelia dôveryhodných služieb informujú orgán dohľadu najneskôr jeden mesiac pred každým plánovaným auditom a umožnia orgánu dohľadu, aby sa na požiadanie zúčastnil ako pozorovateľ.

1b. Členské štáty bez zbytočného odkladu oznámia Komisii názvy, adresy a akreditačné údaje orgánov posudzovania zhody uvedených v odseku 1 a všetky ich následné zmeny. Komisia sprístupní tieto informácie všetkým členským štátom.“;

c) odseky 2, 3 a 4 sa nahrádzajú takto:

„2. Bez toho, aby bol dotknutý odsek 1, orgán dohľadu môže kedykoľvek vykonať audit alebo požiadať orgán posudzovania zhody, aby vykonal posúdenie zhody kvalifikovaných poskytovateľov dôveryhodných služieb na náklady týchto poskytovateľov dôveryhodných služieb s cieľom potvrdiť, že títo poskytovatelia a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky stanovené v tomto nariadení. Ak sa zdá, že boli porušené predpisy týkajúce sa ochrany osobných údajov, orgán dohľadu bez zbytočného odkladu informuje príslušné dozorné orgány zriadené podľa článku 51 nariadenia (EÚ) 2016/679 .

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

Ak tento poskytovateľ nápravu nezabezpečí, v relevantných prípadoch v lehote stanovenej orgánom dohľadu, orgán dohľadu, ak je to odôvodnené najmä rozsahom, trvaním a dôsledkami neplnenia požiadavky, odníme kvalifikovaný štatút tohto poskytovateľa alebo dotknutej služby, ktorú poskytuje .

3a. Ak príslušné orgány určené alebo zriadené podľa článku 8 ods. 1 smernice (EÚ) 2022/2555 informujú orgán dohľadu o tom, že kvalifikovaný poskytovateľ dôveryhodných služieb nespĺňa niektorú z požiadaviek stanovených v článku 21 uvedenej smernice, orgán dohľadu, ak je to odôvodnené najmä rozsahom, trvaním a dôsledkami takéhoto neplnenia požiadavky, odníme kvalifikovaný štatút tohto poskytovateľa alebo dotknutej služby, ktorú poskytuje.

3b. Ak dozorné orgány zriadené podľa článku 51 nariadenia (EÚ) 2016/679 informujú orgán dohľadu o tom, že kvalifikovaný poskytovateľ dôveryhodných služieb nespĺňa niektorú z požiadaviek stanovených v uvedenom nariadení, orgán dohľadu, ak je to odôvodnené najmä rozsahom, trvaním a dôsledkami takéhoto neplnenia požiadavky, odníme kvalifikovaný štatút tohto poskytovateľa alebo dotknutej služby, ktorú poskytuje.

3c. Orgán dohľadu informuje kvalifikovaného poskytovateľa dôveryhodných služieb o odňatí jeho kvalifikovaného štatútu alebo kvalifikovaného štatútu dotknutej služby. Na účely aktualizácie dôveryhodných zoznamov uvedených v článku 22 ods. 1 tohto nariadenia orgán dohľadu informuje orgán, o ktorom sa informovalo podľa odseku 3 uvedeného článku, a príslušný orgán určený alebo zriadený podľa článku 8 ods. 1 smernice (EÚ) 2022/2555.

4. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre :

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

b) požiadavky na audit pre orgány posudzovania zhody na vykonávanie posudzovania zhody vrátane zloženého posudzovania kvalifikovaných poskytovateľov dôveryhodných služieb podľa odseku 1 ;

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

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

20. Článok 21 sa mení takto:

a) odseky 1 a 2 sa nahrádzajú takto:

„1. Ak majú poskytovatelia dôveryhodných služieb v úmysle začať poskytovať kvalifikovanú dôveryhodnú službu, svoj zámer oznámia orgánu dohľadu spolu so správou o posúdení zhody vydanou orgánom posudzovania zhody, v ktorej sa potvrdzuje splnenie požiadaviek stanovených v tomto nariadení a v článku 21 smernice (EÚ) 2022/2555.

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 spĺňa požiadavky stanovené v článku 21 smernice (EÚ) 2022/2555, orgán dohľadu požiada príslušné orgány určené alebo zriadené podľa článku 8 ods. 1 uvedenej smernice, aby v tejto súvislosti vykonali opatrenia dohľadu a poskytli informácie o výsledku bez zbytočného odkladu a v každom prípade do dvoch mesiacov od doručenia uvedenej žiadosti. Ak sa overenie neukončí do dvoch mesiacov od oznámenia, tieto príslušné orgány o tom informujú orgán dohľadu, pričom uvedú dôvody omeškania a lehotu, v ktorej sa má overenie 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 od oznámenia v súlade s odsekom 1 tohto článku.

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

b) odsek 4 sa nahrádza takto:

„4. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov stanoví formáty a postupy oznamovania a overovania na účely odsekov 1 a 2 tohto článku . Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

21. 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 v príslušnom prípade všetky osobitné atribúty fyzickej alebo právnickej osoby, ktorej sa má vydať kvalifikovaný certifikát alebo kvalifikované elektronické osvedčenie atribútov.

1a. Overenie totožnosti uvedené v odseku 1 vykoná vhodnými prostriedkami kvalifikovaný poskytovateľ dôveryhodných služieb, a to buď priamo alebo prostredníctvom tretej strany, a to na základe jednej z týchto metód alebo v prípade potreby ich kombinácie v súlade s vykonávacími aktmi uvedenými v odseku 1c:

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

b) prostredníctvom certifikátu kvalifikovaného elektronického podpisu alebo kvalifikovanej elektronickej pečate vydaného v súlade s písmenom a), c) alebo d);

c) použitím iných metód identifikácie , ktorými sa zabezpečuje identifikácia osoby s vysokou úrovňou spoľahlivosti, ktorých zhodu potvrdí orgán posudzovania zhody;

d) fyzickou prítomnosťou fyzickej osoby alebo splnomocneného zástupcu právnickej osoby prostredníctvom vhodných dôkazov a postupov v súlade s vnútroštátnym právom.

1b. Overenie atribútov uvedené v odseku 1 vykoná vhodnými prostriedkami kvalifikovaný poskytovateľ dôveryhodných služieb, a to buď priamo alebo prostredníctvom tretej strany, a to na základe jednej z týchto metód alebo v prípade potreby ich kombinácie v súlade s vykonávacími aktmi uvedenými v odseku 1c:

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

b) prostredníctvom certifikátu kvalifikovaného elektronického podpisu alebo kvalifikovanej elektronickej pečate vydaného v súlade s odsekom 1a písm. a), c) alebo d);

c) prostredníctvom kvalifikovaného elektronického osvedčenia atribútov;

d) použitím iných metód, ktorými sa zabezpečuje overenie atribútov s vysokou úrovňou spoľahlivosti, ktorých zhodu potvrdí orgán posudzovania zhody;

e) prostredníctvom fyzickej prítomnosti fyzickej osoby alebo splnomocneného zástupcu právnickej osoby, prostredníctvom vhodných dôkazov a postupov v súlade s vnútroštátnym právom.

1c. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy na overovanie totožnosti a atribútov v súlade s odsekmi 1, 1a a 1b tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2. “;

b) odsek 2 sa mení takto:

i) písmeno a) sa nahrádza 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 ukončiť tieto činnosti;“;

ii) písmená d) a e) sa nahrádzajú takto:

„d) pred uzavretím zmluvného vzťahu jasne, v plnom rozsahu a ľahko dostupným spôsobom vo verejne prístupnom priestore a individuálne informuje každú osobu, ktorá chce využívať kvalifikovanú dôveryhodnú službu, o presných podmienkach jej používania vrátane všetkých obmedzení jej používania;

e) používa dôveryhodné systémy a produkty, ktoré sú chránené proti pozmeneniu, a zaisťuje technickú bezpečnosť a spoľahlivosť procesov, ktoré sa nimi podporujú, a to aj použitím vhodných kryptografických techník;“;

iii) vkladajú sa tieto písmená:

„fa) má bez ohľadu na článok 21 smernice (EÚ) 2022/2555 vhodné politiky a prijíma zodpovedajúce opatrenia na riadenie právnych, obchodných, prevádzkových a iných priamych alebo nepriamych rizík poskytovania kvalifikovanej dôveryhodnej služby vrátane aspoň opatrení týkajúcich sa:

i) postupov registrácie a pridávania používateľov služby;

ii) procesných alebo administratívnych kontrol;

iii) riadenia a implementácie služieb;

fb) bez zbytočného odkladu a v každom prípade do 24 hodín od incidentu oznámi orgánu dohľadu, identifikovateľným dotknutým jednotlivcom, v príslušnom prípade iným relevantným príslušným orgánom a na žiadosť orgánu dohľadu aj verejnosti, ak je to vo verejnom záujme, všetky narušenia bezpečnosti alebo narušenia poskytovania služby alebo vykonávania opatrení uvedených v písmene fa) bodoch i), ii) alebo iii), ktoré majú významný vplyv na poskytovanú dôveryhodnú službu alebo na osobné údaje, ktoré sa v rámci nej uchovávajú;“;

iv) písmená g), h) a i) 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 po ukončení činností kvalifikovaného poskytovateľa dôveryhodných služieb potrebné, 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;

i) má aktualizovaný plán ukončenia činnosti s cieľom zabezpečiť kontinuitu služby v súlade s ustanoveniami, ktoré overuje orgán dohľadu podľa článku 46b ods. 4 písm. i);“;

v) písmeno j) sa vypúšťa;

vi) dopĺňa sa tento pododsek:

„Orgán dohľadu môže okrem informácií oznámených podľa prvého pododseku písm. a) požadovať informácie alebo výsledok posudzovania zhody a môže udelenie povolenia na vykonanie zamýšľaných zmien kvalifikovaných dôveryhodných služieb môže podmieniť. Ak sa overenie neukončí do troch mesiacov od oznámenia, orgán dohľadu o tom informuje poskytovateľa dôveryhodných služieb, pričom uvedie dôvody omeškania a lehotu, v ktorej sa má overenie ukončiť.“;

c) odsek 5 sa nahrádza takto:

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

4b. Komisia je splnomocnená prijímať v súlade s článkom 47 delegované akty, ktorými sa stanovujú dodatočné opatrenia uvedené v odseku 2 písm. fa) tohto článku.

5. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre požiadavky uvedené v odseku 2 tohto článku. Ak sú tieto normy, špecifikácie a postupy splnené, predpokladá sa, že sa dosiahol súlad s požiadavkami stanovenými v tomto odseku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

22. V kapitole III oddiele 3 sa vkladá tento článok:

„*Článok 24a*

Uznávanie kvalifikovaných dôveryhodných služieb

1. Kvalifikované elektronické podpisy založené na kvalifikovanom certifikáte vydané v jednom členskom štáte a kvalifikované elektronické pečate založené na kvalifikovanom certifikáte vyhotovené v jednom členskom štáte sa uznávajú ako kvalifikované elektronické podpisy a kvalifikované elektronické pečate vo všetkých ostatných členských štátoch.

2. Zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a zariadenia na vyhotovenie kvalifikovanej elektronickej pečate certifikované v jednom členskom štáte sa uznávajú ako zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a zariadenia na vyhotovenie kvalifikovanej elektronickej pečate vo všetkých ostatných členských štátoch.

3. Kvalifikovaný certifikát pre elektronické podpisy, kvalifikovaný certifikát pre elektronické pečate, kvalifikovaná dôveryhodná služba na správu zariadení na vyhotovenie kvalifikovaných elektronických podpisov na diaľku a kvalifikovaná dôveryhodná služba na správu zariadení na vyhotovenie kvalifikovaných elektronických pečatí na diaľku poskytované v jednom členskom štáte sa uznávajú ako kvalifikovaný certifikát pre elektronické podpisy, kvalifikovaný certifikát pre elektronické pečate, kvalifikovaná dôveryhodná služba na správu zariadení na vyhotovenie kvalifikovaných elektronických podpisov na diaľku a kvalifikovaná dôveryhodná služba na správu zariadení na vyhotovenie kvalifikovaných elektronických pečatí na diaľku vo všetkých ostatných členských štátoch.

4. Kvalifikovaná služba validácie kvalifikovaných elektronických podpisov a kvalifikovaná služba validácie kvalifikovaných elektronických pečatí poskytovaná v jednom členskom štáte sa uznáva ako kvalifikovaná služba validácie kvalifikovaných elektronických podpisov a kvalifikovaná služba validácie kvalifikovaných elektronických pečatí vo všetkých ostatných členských štátoch.

5. Kvalifikovaná služba uchovávania kvalifikovaných elektronických podpisov a kvalifikovaná služba uchovávania kvalifikovaných elektronických pečatí poskytovaná v jednom členskom štáte sa uznáva ako kvalifikovaná služba uchovávania kvalifikovaných elektronických podpisov a kvalifikovaná služba uchovávania kvalifikovaných elektronických pečatí vo všetkých ostatných členských štátoch.

6. Kvalifikovaná elektronická časová pečiatka poskytnutá v jednom členskom štáte sa uznáva ako kvalifikovaná elektronická časová pečiatka vo všetkých ostatných členských štátoch.

7. Kvalifikovaný certifikát pre autentifikáciu webového sídla vydaný v jednom členskom štáte sa uznáva ako kvalifikovaný certifikát pre autentifikáciu webového sídla vo všetkých ostatných členských štátoch.

8. Kvalifikovaná elektronická doručovacia služba pre registrované zásielky v jednom členskom štáte sa uznáva ako kvalifikovaná elektronická doručovacia služba pre registrované zásielky vo všetkých ostatných členských štátoch.

9. Kvalifikované elektronické osvedčenie atribútov vydané v jednom členskom štáte sa uznáva ako kvalifikované elektronické osvedčenie atribútov vo všetkých ostatných členských štátoch.

10. Kvalifikovaná elektronická archivačná služba poskytovaná v jednom členskom štáte sa uznáva ako kvalifikovaná elektronická archivačná služba vo všetkých ostatných členských štátoch.

11. Kvalifikovaný elektronický register poskytovaný v jednom členskom štáte sa uznáva ako kvalifikovaný elektronický register vo všetkých ostatných členských štátoch.“

23. V článku 25 sa vypúšťa odsek 3.

24. Článok 26 sa mení takto:

a) jediný odsek sa stáva odsekom 1;

b) dopĺňa sa tento odsek:

„2. Komisia do … [24 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] posúdi, či je potrebné prijať vykonávacie akty na vypracovanie zoznamu referenčných noriem a v prípade potreby stanovenie špecifikácií a postupov pre zdokonalené elektronické podpisy. Na základe tohto posúdenia môže Komisia prijať takéto vykonávacie akty. Ak zdokonalený elektronický podpis spĺňa normy, špecifikácie a postupy, predpokladá sa, že je v súlade s požiadavkami na zdokonalené elektronické podpisy. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

25. V článku 27 sa vypúšťa odsek 4.

26. V článku 28 sa odsek 6 nahrádza takto:

„6. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre kvalifikované certifikáty pre elektronický podpis. Ak kvalifikovaný certifikát pre elektronický podpis spĺňa uvedené normy, špecifikácie a postupy, 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 vkladá tento odsek:

„1a. Vytváranie alebo správu údajov na vyhotovenie elektronického podpisu alebo duplikáciu takýchto údajov na vyhotovenie podpisu na účely zálohovania vykonáva len kvalifikovaný poskytovateľ dôveryhodných služieb poskytujúci kvalifikovanú dôveryhodnú službu na správu zariadenia na vyhotovenie kvalifikovaného elektronického podpisu na diaľku len v mene podpisovateľa a na jeho žiadosť.“

28. Vkladá sa tento článok :

„*Článok 29a*
Požiadavky na kvalifikovanú službu správy zariadení na vyhotovenie kvalifikovaného elektronického podpisu na diaľku

1. Správu zariadení na vyhotovenie kvalifikovaného elektronického podpisu na diaľku ako kvalifikovanú službu vykonáva len kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý:

   a) generuje alebo spravuje údaje na vyhotovenie elektronického podpisu v mene podpisovateľa;

   b) bez ohľadu na bod 1 písm. d) prílohy II duplikuje údaje na vyhotovenie elektronického podpisu len na účely zálohovania za predpokladu, že sú splnené tieto požiadavky:

      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 potrebné na zabezpečenie kontinuity služby;

   c) spĺňa všetky požiadavky uvedené v certifikačnej správe konkrétneho zariadenia na vyhotovenie kvalifikovaného elektronického podpisu na diaľku vydanej podľa článku 30.

2. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy na účely odseku 1 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

29. V článku 30 sa vkladá tento odsek:

„3a. Platnosť certifikácie uvedenej v odseku 1 nepresiahne päť rokov za predpokladu, že posúdenia zraniteľnosti sa vykonávajú každé dva roky. Ak sa zistia zraniteľnosti a neodstránia sa, certifikácia sa zruší.“

30. V článku 31 sa odsek 3 nahrádza takto:

„3. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov stanoví formáty a postupy uplatniteľné na účely odseku 1 tohto článku. 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 normy, špecifikácie a postupy uvedené v odseku 3, predpokladá sa, že je v súlade s požiadavkami stanovenými v prvom pododseku tohto odseku. “;

b) odsek 3 sa nahrádza takto:

„3. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre validáciu kvalifikovaných elektronických podpisov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

32. Vkladá sa tento článok:

„*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) validačné údaje podpisu zodpovedajú údajom poskytnutým spoliehajúcej sa strane;

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

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

f) nebola skompromitovaná integrita podpísaných údajov;

g) v čase podpísania boli dodržané požiadavky stanovené v článku 26.

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. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre validáciu zdokonalených elektronických podpisov založených na kvalifikovaných certifikátoch. Ak validácia zdokonaleného elektronického podpisu založeného na kvalifikovaných certifikátoch spĺňa uvedené normy, špecifikácie a postupy, predpokladá sa, že je v súlade s požiadavkami stanovenými v odseku 1 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

33. V článku 33 sa odsek 2 nahrádza takto:

„2. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre kvalifikovanú službu validácie uvedenú v odseku 1 tohto článku. Ak kvalifikovaná službu validácie pre kvalifikované elektronické podpisy spĺňa uvedené normy, špecifikácie a postupy, predpokladá sa, že je v súlade s požiadavkami stanovenými v odseku 1 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

34. Článok 34 sa mení takto:

a) vkladá sa tento odsek:

„1a. Ak opatrenia týkajúce sa kvalifikovanej služby uchovávania kvalifikovaných elektronických podpisov spĺňajú normy, špecifikácie a postupy uvedené v odseku 2, predpokladá sa, že sú v súlade s požiadavkami stanovenými v odseku 1.“;

b) odsek 2 sa nahrádza takto:

„2. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre kvalifikovanú službu uchovávania kvalifikovaných elektronických podpisov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2. “

35. V článku 35 sa vypúšťa odsek 3.

36. Článok 36 sa mení takto:

a) jediný odsek sa stáva odsekom 1;

b) dopĺňa sa tento odsek:

„2. Komisia do … [24 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] posúdi, či je potrebné prijať vykonávacie akty na vypracovanie zoznamu referenčných noriem a v prípade potreby stanovenie špecifikácií a postupov pre zdokonalené elektronické pečate. Na základe tohto posúdenia môže Komisia prijať takéto vykonávacie akty. Ak zdokonalená elektronická pečať spĺňa uvedené normy, špecifikácie a postupy, predpokladá sa, že je v súlade s požiadavkami na zdokonalené elektronické pečate. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

37. V článku 37 sa vypúšťa odsek 4.

38. V článku 38 sa odsek 6 nahrádza takto:

„6. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre kvalifikované certifikáty pre elektronické pečate. Ak kvalifikovaný certifikát pre elektronickú pečať spĺňa uvedené normy, špecifikácie a postupy, predpokladá sa, že je v súlade s požiadavkami stanovenými v prílohe III. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

39. Vkladá sa tento článok :

„*Článok 39a*
Požiadavky na kvalifikovanú službu správy zariadení na vyhotovenie kvalifikovanej elektronickej pečate na diaľku

Článok 29a sa uplatňuje *mutatis mutandis* na kvalifikovanú službu správy zariadení na vyhotovenie kvalifikovanej elektronickej pečate na diaľku.“

40. V kapitole III, oddiele 5 sa vkladá tento článok:

„*Článok 40a*
Požiadavky na validáciu zdokonalených elektronických pečatí založených na kvalifikovaných certifikátoch

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

41. V článku 41 sa vypúšťa odsek 3.

42. Článok 42 sa mení takto:

a) vkladá sa tento odsek:

„1a. Ak spojenie dátumu a času s údajmi a presnosť zdroju času spĺňajú normy, špecifikácie a postupy uvedené v odseku 2, predpokladá sa, že požiadavky stanovené v odseku 1 sú splnené.“;

b) odsek 2 sa nahrádza takto:

„2. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre spájanie dátumu a času s údajmi a pre stanovovanie presnosti zdrojov času. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2. “

43. Článok 44 sa mení takto:

a) vkladá sa tento odsek:

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

b) odsek 2 sa nahrádza takto:

„2. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy 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:

„2a. 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 byť v súlade s požiadavkami stanovenými v odseku 1 a takýto súlad musí potvrdiť orgán posudzovania zhody.

2b. Komisia môže prostredníctvom vykonávacích aktov vypracovať zoznam referenčných noriem a v prípade potreby stanoviť špecifikácie a postupy pre rámec interoperability uvedený v odseku 2a tohto článku. Technické špecifikácie a obsah noriem musia byť nákladovo efektívne a primerané. Vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

44. Článok 45 sa nahrádza takto:

„*Článok 45*

Požiadavky na kvalifikované certifikáty pre autentifikáciu webových sídiel

1. Kvalifikované certifikáty pre autentifikáciu webových sídiel musia spĺňať požiadavky stanovené v prílohe IV. Hodnotenie súladu s týmito požiadavkami sa vykonáva v súlade s normami, špecifikáciami a postupmi uvedenými v odseku 2 tohto článku.

1a. Kvalifikované certifikáty pre autentifikáciu webových sídiel vydané v súlade s odsekom 1 tohto článku musia byť uznávané poskytovateľmi webových prehliadačov. Poskytovatelia webových prehliadačov zabezpečia, aby sa údaje o totožnosti osvedčené v certifikáte a ďalšie osvedčené atribúty zobrazovali používateľsky ústretovým spôsobom. Poskytovatelia webových prehliadačov zabezpečia podporu kvalifikovaných certifikátov pre autentifikáciu webových sídiel uvedených v odseku 1 tohto článku a interoperabilitu s nimi s výnimkou mikropodnikov alebo malých podnikov v zmysle vymedzenia v článku 2 prílohy k odporúčaniu 2003/361/ES počas prvých piatich rokov pôsobenia ako poskytovatelia služieb prehliadania webu.

1b. Kvalifikované certifikáty pre autentifikáciu webových sídiel nepodliehajú žiadnym povinným požiadavkám okrem požiadaviek stanovených v odseku 1.

2. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre kvalifikované certifikáty pre autentifikáciu webových sídiel uvedené v odseku 1 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

45. Vkladá sa tento článok:

„*Článok 45a*
Preventívne opatrenia v oblasti kybernetickej bezpečnosti

1. Poskytovatelia webových prehliadačov neprijmú žiadne opatrenia, ktoré by boli v rozpore s ich povinnosťami stanovenými v článku 45, najmä s požiadavkami na uznávanie kvalifikovaných certifikátov pre autentifikáciu webových sídiel a na zobrazenie poskytnutých údajov o totožnosti používateľsky ústretovým spôsobom.

2. Odchylne od odseku 1 a len v prípade opodstatnených obáv súvisiacich s narušením bezpečnosti alebo stratou integrity identifikovaného certifikátu alebo súboru certifikátov môžu poskytovatelia webových prehliadačov v súvislosti s daným certifikátom alebo súborom certifikátov prijať preventívne opatrenia.

3. Ak poskytovateľ webového prehliadača prijme preventívne opatrenia podľa odseku 2, poskytovateľ webového prehliadača bez zbytočného odkladu písomne oznámi svoje obavy spolu s opisom opatrení prijatých na zmiernenie týchto obáv Komisii, príslušnému orgánu dohľadu, subjektu, ktorému bol certifikát vydaný, a kvalifikovanému poskytovateľovi dôveryhodných služieb, ktorý tento certifikát alebo súbor certifikátov vydal. Po doručení takéhoto oznámenia vydá príslušný orgán dohľadu dotknutému poskytovateľovi webového prehliadača potvrdenie o doručení.

4. Príslušný orgán dohľadu vyšetrí záležitosti uvedené v oznámení v súlade s článkom 46b ods. 4 písm. k). Ak výsledok tohto vyšetrovania nevedie k odňatiu kvalifikovaného štatútu certifikátu, orgán dohľadu o tom informuje poskytovateľa webového prehliadača a požiada ho, aby preventívne opatrenia uvedené v odseku 2 tohto článku ukončil.“

46. V kapitole III sa dopĺňajú tieto oddiely:

„ODDIEL 9
ELEKTRONICKÉ OSVEDČENIE ATRIBÚTOV

Článok 45b
Právne účinky elektronického osvedčenia atribútov

1. Právny účinok elektronického osvedčenia atribútov alebo jeho prípustnosť ako dôkaz v súdnom konaní sa nesmie zamietnuť 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 majú rovnaký právny účinok ako zákonne vydané osvedčenia v listinnej podobe.

3. Osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj v jednom členskom štáte alebo v jeho mene sa uznáva ako osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene vo všetkých členských štátoch.

Článok 45c

Elektronické osvedčenie 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 autentifikácie 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 45d

Požiadavky na kvalifikované elektronické osvedčenie atribútov

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

2. Hodnotenie súladu s požiadavkami stanovenými v prílohe V sa vykonáva v súlade s normami, špecifikáciami a postupmi uvedenými v odseku 5 tohto článku.

3. Kvalifikované elektronické osvedčenia atribútov nesmú podliehať žiadnym povinným požiadavkám nad rámec požiadaviek stanovených v prílohe V.

4. Ak sa po počiatočnom vydaní kvalifikované elektronické osvedčenie atribútov zruší, stráca svoju platnosť okamihom jeho zrušenia a jeho štatút sa za žiadnych okolností nesmie zmeniť na pôvodný.

5. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre kvalifikované elektronické osvedčenia atribútov. Uvedené vykonávacie akty musia byť v súlade s vykonávacími aktmi uvedenými v článku 5a ods. 23 o implementácii európskej peňaženky digitálnej identity. Prijmú sa v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 45e

Overovanie atribútov na základe autentických zdrojov

1. Členské štáty do 24 mesiacov odo dňa nadobudnutia účinnosti vykonávacích aktov uvedených v článku 5a ods. 23 a článku 5c ods. 6 zabezpečia, aby sa aspoň v prípade atribútov uvedených v prílohe VI vždy, keď sa tieto atribúty spoliehajú na autentické zdroje vo verejnom sektore, prijali opatrenia, ktoré kvalifikovaným poskytovateľom dôveryhodných služieb elektronických osvedčení atribútov umožnia overiť tieto atribúty elektronickými prostriedkami na žiadosť používateľa v súlade s právom Únie alebo vnútroštátnym právom.

2. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] s prihliadnutím na príslušné medzinárodné normy prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre katalóg atribútov, ako aj systémy osvedčovania atribútov a postupy overovania kvalifikovaných elektronických osvedčení atribútov na účely odseku 1 tohto článku. Uvedené vykonávacie akty musia byť v súlade s vykonávacími aktmi uvedenými v článku 5a ods. 23 o implementácii európskej peňaženky digitálnej identity. Prijmú sa v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 45f

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 46 a identifikovaného ako vydavateľ uvedený v prílohe VII bode b) a obsahujúci osobitný súbor certifikovaných atribútov vo forme vhodnej na automatizované spracovanie:

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

      ii) ktorý obsahuje súbor údajov jednoznačne reprezentujúcich autentický zdroj uvedený v bode i), a

      iii) ktorý odkazuje na právo Únie alebo vnútroštátne právo uvedené v bode i).

2. Členský štát, v ktorom sú zriadené subjekty verejného sektora uvedené v článku 3 bode 46, zabezpečí, aby subjekty verejného sektora, ktoré vydávajú elektronické osvedčenia atribútov, mali úroveň spoľahlivosti a dôveryhodnosti, ktorá je rovnocenná úrovni kvalifikovaných poskytovateľov dôveryhodných služieb v súlade s článkom 24.

3. Členské štáty oznámia subjekty verejného sektora uvedené v článku 3 bode 46 Komisii. 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 kanála zverejní zoznam subjektov verejného sektora uvedený v článku 3 bode 46 v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

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

5. 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, ak spĺňa normy, špecifikácie a postupy uvedené v odseku 6.

6. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre elektronické osvedčenie atribútov vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene. Uvedené vykonávacie akty musia byť v súlade s vykonávacími aktmi uvedenými v článku 5a ods. 23 o implementácii európskej peňaženky digitálnej identity. Prijmú sa v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

7. Komisia do … [šesť mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy na účely odseku 3 tohto článku. Uvedené vykonávacie akty musia byť v súlade s vykonávacími aktmi uvedenými v článku 5a ods. 23 o implementácii európskej peňaženky digitálnej identity. Prijmú sa v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

8. Subjekty verejného sektora uvedené v článku 3 bode 46, ktoré vydávajú elektronické osvedčenie atribútov, poskytujú rozhranie s európskymi peňaženkami digitálnej identity, ktoré sa poskytujú v súlade s článkom 5a.

Článok 45g

Vydávanie elektronického osvedčenia atribútov pre európske peňaženky digitálnej identity

1. Poskytovatelia elektronických osvedčení atribútov poskytnú používateľom európskej peňaženky digitálnej identity možnosť požiadať o elektronické osvedčenie atribútov, získať, uchovávať a spravovať ho bez ohľadu na členský štát, v ktorom sa európska peňaženka digitálnej identity poskytuje.

2. Poskytovatelia kvalifikovaných elektronických osvedčení atribútov poskytujú rozhranie s európskymi peňaženkami digitálnej identity, ktoré sa poskytujú v súlade s článkom 5a.

Článok 45h

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 oni sami alebo ich obchodní partneri.

2. Osobné údaje týkajúce sa poskytovania služieb elektronického osvedčovania atribútov sa uchovávajú logicky oddelene od ostatných údajov v držbe poskytovateľa elektronického osvedčenia atribútov.

3. Poskytovatelia služieb kvalifikovaného elektronického osvedčovania atribútov poskytujú takéto kvalifikované dôveryhodné služby spôsobom, ktorý je funkčne oddelený od iných služieb, ktoré poskytujú.

ODDIEL 10
ELEKTRONICKÉ ARCHIVAČNÉ SLUŽBY

Článok 45i
Právny účinok elektronických archivačných služieb

1. Právny účinok elektronických údajov a elektronických dokumentov uchovávaných prostredníctvom elektronickej archivačnej služby alebo ich prípustnosť ako dôkaz v súdnom konaní sa nesmie zamietnuť výlučne z dôvodu, že majú elektronickú formu alebo že sa neuchovávajú prostredníctvom kvalifikovanej elektronickej archivačnej služby.

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

Článok 45j
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 zabezpečiť trvácnosť a čitateľnosť elektronických údajov a elektronických dokumentov nad rámec obdobia technologickej platnosti a aspoň počas celého zákonného alebo zmluvného obdobia uchovávania pri zachovaní ich integrity a presnosti ich pôvodu;

c) zabezpečujú, aby sa tieto elektronické údaje a tieto elektronické dokumenty 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 prijať automatizovaným spôsobom správu, ktorou sa potvrdí, že na elektronické údaje a elektronické dokumenty získané z kvalifikovaného elektronického archívu sa vzťahuje domnienka integrity údajov od začiatku obdobia uchovávania až do okamihu získania.

Správa uvedená v prvom pododseku písm. d) sa poskytuje spoľahlivým a účinným spôsobom a obsahuje kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať poskytovateľa kvalifikovanej elektronickej archivačnej služby.

2. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre kvalifikované elektronické archivačné služby. Ak kvalifikovaná elektronická archivačná služba spĺňa tieto normy, špecifikácie a postupy, predpokladá sa, že je v súlade 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 45k
Právne účinky elektronických registrov

1. Právny účinok elektronického registra alebo jeho prípustnosť ako dôkaz v súdnom konaní sa nesmie zamietnuť výlučne z 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.

Článok 45l
Požiadavky na kvalifikované elektronické registre

1. Kvalifikované elektronické registre musia spĺňať tieto požiadavky:

   a) sú vytvorené a spravované jedným alebo viacerými kvalifikovanými poskytovateľmi 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, čím sa zabezpečí ich integrita v priebehu času.

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

3. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov vypracuje zoznam referenčných noriem a v prípade potreby stanoví špecifikácie a postupy pre požiadavky ustanovené v odseku 1 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

47. Vkladá sa táto kapitola:

„KAPITOLA IVa
RÁMEC RIADENIA

Článok 46a
Dohľad nad rámcom európskej peňaženky digitálnej identity

1. Členské štáty určia na svojom území jeden alebo viac orgánov dohľadu.

Orgánom dohľadu určeným podľa prvého pododseku sa udelia právomoci a primerané zdroje potrebné na to, aby si mohli účinne, efektívne a nezávisle plniť svoje úlohy.

2. Členské štáty oznámia Komisii názvy a adresy svojich orgánov dohľadu určených podľa odseku 1 a všetky ich následné zmeny. Komisia zoznam oznámených orgánov dohľadu uverejní.

3. Poslaním orgánov dohľadu určených podľa odseku 1 je:

   a) vykonávať dohľad nad poskytovateľmi európskych peňaženiek digitálnej identity usadenými v určujúcom členskom štáte a prostredníctvom činností dohľadu ex ante a ex post zabezpečiť, aby títo poskytovatelia a európske peňaženky digitálnej identity, ktoré poskytujú, spĺňali požiadavky stanovené v tomto nariadení;

   b) v prípade potreby prijať opatrenia v súvislosti s poskytovateľmi európskych peňaženiek digitálnej identity usadenými na území určujúceho členského štátu prostredníctvom činností dohľadu ex post, ak sú informovaní o tom, že poskytovatelia alebo európske peňaženky digitálnej identity, ktoré poskytujú, porušujú toto nariadenie.

4. Medzi úlohy orgánov dohľadu určených podľa odseku 1 patria najmä tieto:

   a) spolupracovať s inými orgánmi dohľadu a poskytovať im pomoc v súlade s článkami 46c a 46e;

   b) žiadať o informácie potrebné na monitorovanie súladu s týmto nariadením;

c) informovať relevantné príslušné orgány dotknutých členských štátov určené alebo zriadené podľa článku 8 ods. 1 smernice (EÚ) 2022/2555 o každom významnom narušení bezpečnosti alebo strate integrity, o ktorých sa dozvedia pri plnení svojich úloh, a v prípade závažného narušenia bezpečnosti alebo straty integrity, ktoré sa týkajú iných členských štátov, informovať jednotné kontaktné miesto dotknutého členského štátu určené alebo zriadené podľa článku 8 ods. 3 smernice (EÚ) 2022/2555 a jednotné kontaktné miesta v ostatných dotknutých členských štátoch určené podľa článku 46c ods. 1 tohto nariadenia, ako aj informovať verejnosť alebo požiadať poskytovateľov európskej peňaženky digitálnej identity, aby tak urobili, ak orgán dohľadu rozhodne, že zverejnenie narušenia bezpečnosti alebo straty integrity by bolo vo verejnom záujme*;*

d) vykonávať kontroly na mieste a dohľad na diaľku;

e) požadovať, aby poskytovatelia európskych peňaženiek digitálnej identity napravili akékoľvek nesplnenie požiadaviek stanovených v tomto nariadení;

f) pozastaviť alebo zrušiť registráciu a začlenenie spoliehajúcich sa strán do mechanizmu uvedeného v článku 5b ods. 7 v prípade nezákonného alebo podvodného používania európskej peňaženky digitálnej identity;

g) spolupracovať s príslušnými dozornými orgánmi zriadenými podľa článku 51 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 porušenie ochrany osobných údajov.

5. Ak orgán dohľadu určený podľa odseku 1 vyžaduje, aby poskytovateľ európskej peňaženky digitálnej identity napravil podľa odseku 4 písm. e) akékoľvek nesplnenie požiadaviek podľa tohto nariadenia, a tento poskytovateľ nekoná zodpovedajúcim spôsobom a v relevantnom prípade v lehote stanovenej uvedeným orgánom dohľadu, orgán dohľadu určený podľa odseku 1 môže, najmä s prihliadnutím na rozsah, trvanie a dôsledky tohto neplnenia, nariadiť poskytovateľovi, aby pozastavil alebo ukončil poskytovanie európskej peňaženky digitálnej identity. Orgán dohľadu o rozhodnutí požadovať pozastavenie alebo ukončenie poskytovania európskej peňaženky digitálnej identity bez zbytočného odkladu informuje orgány dohľadu ostatných členských štátov, Komisiu, spoliehajúce sa strany a používateľov európskej peňaženky digitálnej identity.

6. Každý rok do 31. marca predloží každý orgán dohľadu určený podľa odseku 1 Komisii správu o svojich hlavných činnostiach počas predchádzajúceho kalendárneho roka. Komisia sprístupní uvedené výročné správy Európskemu parlamentu a Rade.

7. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov stanoví formáty a postupy v súvislosti so správou uvedenou v odseku 6 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 46b

Dohľad nad dôveryhodnými službami

1. Členské štáty určia orgán dohľadu zriadený na svojom území alebo určia po vzájomnej dohode s iným členským štátom orgán dohľadu na území tohto iného členského štátu. Tento orgán dohľadu je zodpovedný za úlohy dohľadu v určujúcom členskom štáte, pokiaľ ide o dôveryhodné služby.

   Orgánom dohľadu určeným podľa prvého pododseku sa udelia potrebné právomoci a primerané zdroje na to, aby si mohli plniť svoje úlohy.

2. Členské štáty oznámia Komisii názvy a adresy svojich orgánov dohľadu určených podľa odseku 1 a všetky ich následné zmeny. Komisia zoznam oznámených orgánov dohľadu uverejní.

3. Poslaním orgánov dohľadu určených podľa odseku 1 je:

   a) dohliadať na kvalifikovaných poskytovateľov dôveryhodných služieb usadených na území určujúceho členského štátu a zabezpečiť prostredníctvom činností dohľadu ex ante a ex post, aby títo kvalifikovaní poskytovatelia dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňali požiadavky stanovené v tomto nariadení;

   b) v prípade potreby prijať opatrenia v súvislosti s nekvalifikovanými poskytovateľmi dôveryhodných služieb usadenými na území určujúceho členského štátu prostredníctvom činností dohľadu ex post, ak sú informovaní o tom, že títo nekvalifikovaní poskytovatelia dôveryhodných služieb alebo dôveryhodné služby, ktoré poskytujú, údajne nespĺňajú požiadavky stanovené v tomto nariadení.

4. Medzi úlohy orgánu dohľadu určeného podľa odseku 1 patria najmä tieto:

a) informovať relevantné príslušné orgány dotknutých členských štátov určené alebo zriadené podľa článku 8 ods. 1 smernice (EÚ) 2022/2555 o každom významnom narušení bezpečnosti alebo strate integrity, o ktorých sa dozvedel pri plnení svojich úloh, a v prípade závažného narušenia bezpečnosti alebo straty integrity, ktoré sa týka iných členských štátov, informovať jednotné kontaktné miesto dotknutého členského štátu určené alebo zriadené podľa článku 8 ods. 3 smernice (EÚ) 2022/2555 a jednotné kontaktné miesta v ostatných dotknutých členských štátoch určené podľa článku 46c ods. 1 tohto nariadenia, ako aj informovať verejnosť alebo požiadať poskytovateľa dôveryhodných služieb, aby tak urobil, ak orgán dohľadu rozhodne, že zverejnenie narušenia bezpečnosti alebo straty integrity by bolo vo verejnom záujme*;*

b) spolupracovať s inými orgánmi dohľadu a poskytovať im pomoc v súlade s článkami 46c a 46e;

c) analyzovať správy o posúdení zhody uvedené v článku 20 ods. 1 a článku 21 ods. 1;

d) podávať Komisii správy o svojich hlavných činnostiach v súlade s odsekom 6 tohto článku;

e) vykonávať audity alebo požiadať orgán posudzovania zhody, aby vykonal posúdenie zhody kvalifikovaných poskytovateľov dôveryhodných služieb v súlade s článkom 20 ods. 2;

f) spolupracovať s príslušnými dozornými orgánmi zriadenými podľa článku 51 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 porušenie ochrany osobných údajov;

g) udeľovať poskytovateľom dôveryhodných služieb a službám, ktoré poskytujú, kvalifikovaný štatút a tento štatút odňať v súlade s článkami 20 a 21;

h) informovať orgán zodpovedný za národný dôveryhodný zoznam uvedený v článku 22 ods. 3 o svojich rozhodnutiach o udelení alebo odňatí kvalifikovaného štatútu, pokiaľ tento orgán nie je súčasne aj orgánom dohľadu určeným podľa odseku 1 tohto článku;

i) overovať existenciu a správne uplatňovanie ustanovení o plánoch ukončenia činnosti, ak kvalifikovaný poskytovateľ dôveryhodných služieb ukončí svoju činnosť, vrátane spôsobu, akým sa informácie udržiavajú prístupné v súlade s článkom 24 ods. 2 písm. h);

j) požadovať, aby poskytovatelia dôveryhodných služieb napravili akékoľvek nesplnenie požiadaviek stanovených v tomto nariadení;

k) vyšetrovať tvrdenia poskytovateľov webových prehliadačov podľa článku 45a a v prípade potreby prijať opatrenia.

5. Členské štáty môžu požadovať, aby orgán dohľadu určený podľa odseku 1 zriadil, udržiaval a aktualizoval dôveryhodnú infraštruktúru v súlade s vnútroštátnym právom.

6. Každý rok do 31. marca predloží každý orgán dohľadu určený podľa odseku 1 Komisii správu o svojich hlavných činnostiach počas predchádzajúceho kalendárneho roka. Komisia sprístupní uvedené výročné správy Európskemu parlamentu a Rade.

7. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prijme usmernenia o vykonávaní úloh uvedených v odseku 4 tohto článku orgánmi dohľadu určenými podľa odseku 1 tohto článku a prostredníctvom vykonávacích aktov stanoví formáty a postupy v súvislosti so správou uvedenou v odseku 6 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.

Článok 46c

Jednotné kontaktné miesta

1. Každý členský štát určí jednotné kontaktné miesto pre dôveryhodné služby, európske peňaženky digitálnej identity a oznámené schémy elektronickej identifikácie.

2. Každé jednotné kontaktné miesto vykonáva styčnú funkciu s cieľom uľahčiť cezhraničnú spoluprácu medzi orgánmi dohľadu nad poskytovateľmi dôveryhodných služieb a medzi orgánmi dohľadu nad poskytovateľmi európskych peňaženiek digitálnej identity a v príslušnom prípade s Komisiou a Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) a s inými príslušnými orgánmi v rámci svojho členského štátu.

3. Každý členský štát zverejní a bez zbytočného odkladu oznámi Komisii názvy a adresy jednotného kontaktného miesta určeného podľa odseku 1 a všetky ich následné zmeny.

4. Komisia uverejní zoznam jednotných kontaktných miest oznámených podľa odseku 3.

Článok 46d
Vzájomná pomoc

1. S cieľom uľahčiť dohľad nad povinnosťami podľa tohto nariadenia a ich presadzovanie môžu orgány dohľadu určené podľa článku 46a ods. 1 a článku 46b ods. 1 požiadať, a to aj prostredníctvom skupiny pre spoluprácu zriadenej podľa článku 46e ods. 1, o vzájomnú pomoc orgány dohľadu iného členského štátu, v ktorom je poskytovateľ európskej peňaženky digitálnej identity alebo poskytovateľ dôveryhodných služieb usadený alebo v ktorom sa nachádzajú jeho siete a informačné systémy, alebo v ktorom sa poskytujú jeho služby.

2. Vzájomná pomoc zahŕňa aspoň to, že:

a) orgán dohľadu, ktorý uplatňuje opatrenia dohľadu a presadzovania v jednom členskom štáte, informuje orgán dohľadu z iného dotknutého členského štátu a konzultuje s ním;

b) orgán dohľadu môže požiadať orgán dohľadu iného dotknutého členského štátu, aby prijal opatrenia dohľadu alebo presadzovania, čo zahŕňa napríklad žiadosti o vykonanie kontrol súvisiacich so správami o posúdení zhody, ako sa uvádza v článkoch 20 a 21, pokiaľ ide o poskytovanie dôveryhodných služieb;

c) orgány dohľadu môžu vo vhodných prípadoch vykonávať spoločné vyšetrovania s orgánmi dohľadu iných členských štátov.

Dojednania a postupy pre spoločné činnosti podľa prvého pododseku dohodnú a stanovia dotknuté členské štáty v súlade so svojím vnútroštátnym právom.

3. Orgán dohľadu, ktorému je adresovaná žiadosť o pomoc, môže túto žiadosť zamietnuť z ktoréhokoľvek z týchto dôvodov:

a) požadovaná pomoc nie je primeraná činnostiam dohľadu orgánu dohľadu vykonávaným v súlade s článkami 46a a 46b;

b) orgán dohľadu nie je príslušný poskytnúť požadovanú pomoc;

c) poskytnutie požadovanej pomoci by bolo v rozpore s týmto nariadením.

4. Do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] a potom každé dva roky skupina pre spoluprácu zriadená podľa článku 46e ods. 1 vydá usmernenia o organizačných aspektoch a postupoch vzájomnej pomoci uvedenej v odsekoch 1 a 2 tohto článku.

Článok 46e

Skupina pre európsku spoluprácu v oblasti digitálnej identity

1. S cieľom podporiť a uľahčiť cezhraničnú spoluprácu a výmenu informácií členských štátov v oblasti dôveryhodných služieb, európskych peňaženiek digitálnej identity a oznámených schém elektronickej identifikácie Komisia zriadi skupinu pre európsku spoluprácu v oblasti digitálnej identity (ďalej len „skupina pre spoluprácu“).

2. Skupina pre spoluprácu sa skladá zo zástupcov vymenovaných členskými štátmi a Komisiou. Skupine pre spoluprácu predsedá Komisia. Komisia zabezpečuje sekretariát skupiny pre spoluprácu.

3. Na zasadnutia skupiny pre spoluprácu a na účasť na jej práci sa môžu na ad hoc báze prizývať ako pozorovatelia zástupcovia príslušných zainteresovaných strán.

4. Agentúra ENISA sa prizýva na účasť na práci skupiny pre spoluprácu ako pozorovateľ pri výmene názorov, najlepších postupov a informácií o relevantných aspektoch kybernetickej bezpečnosti, ako je oznamovanie narušení bezpečnosti, a keď sa rieši používanie certifikátov alebo noriem kybernetickej bezpečnosti.

5. Skupina pre spoluprácu plní tieto úlohy:

   a) vymieňať si rady a spolupracovať s Komisiou na nových politických iniciatívach v oblasti peňaženiek digitálnej identity, prostriedkov elektronickej identifikácie a dôveryhodných služieb;

   b) podľa potreby radiť Komisii pri včasnej príprave návrhov vykonávacích a delegovaných aktov, ktoré sa majú prijať podľa tohto nariadenia;

   c) v záujme podpory orgánov dohľadu pri vykonávaní ustanovení tohto nariadenia:

      i) vymieňať si najlepšie postupy a informácie v súvislosti s vykonávaním ustanovení tohto nariadenia;

      ii) posudzovať relevantný vývoj v odvetviach súvisiacich s peňaženkou digitálnej identity, elektronickou identifikáciou a dôveryhodnými službami;

      iii) organizovať spoločné stretnutia s príslušnými zainteresovanými stranami z celej Únie s cieľom prediskutovať činnosti skupiny pre spoluprácu a zhromažďovať informácie o nových výzvach v tejto oblasti politiky;

iv) s podporou agentúry ENISA si vymieňať názory, najlepšie postupy a informácie o relevantných kybernetickobezpečnostných aspektoch európskych peňaženiek digitálnej identity, schém elektronickej identifikácie a dôveryhodných služieb;

v) vymieňať si najlepšie postupy v súvislosti s tvorbou a vykonávaním politík týkajúcich sa oznamovania narušení bezpečnosti a spoločných opatrení uvedených v článkoch 5e a 10;

vi) organizovať spoločné stretnutia so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zriadenou podľa článku 14 ods. 1 smernice (EÚ) 2022/2555 s cieľom vymieňať si v súvislosti s dôveryhodnými službami a elektronickou identifikáciou relevantné informácie o kybernetických hrozbách, incidentoch, zraniteľnosti, iniciatívach na zvyšovanie informovanosti, odbornej príprave, cvičeniach a zručnostiach, budovaní kapacít, kapacite v oblasti noriem a technických špecifikácií, ako aj o normách a technických špecifikáciách;

vii) na žiadosť orgánu dohľadu rokovať o konkrétnych žiadostiach o vzájomnú pomoc, ako sa uvádza v článku 46d;

viii) uľahčovať výmenu informácií medzi orgánmi dohľadu poskytovaním usmernení o organizačných aspektoch a postupoch vzájomnej pomoci uvedenej v článku 46d;

d) organizovať vzájomné preskúmania schém elektronickej identifikácie oznamovaných podľa tohto nariadenia.

6. Členské štáty zabezpečia účinnú a efektívnu spoluprácu svojich určených zástupcov v skupine pre spoluprácu.

7. Komisia do … [12 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] prostredníctvom vykonávacích aktov stanoví potrebné procesné dojednania na uľahčenie spolupráce medzi členskými štátmi uvedenej v odseku 5 písm. d) tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 48 ods. 2.“

48. Článok 47 sa mení takto:

a) odseky 2 a 3 sa nahrádzajú takto:

„2. Právomoc prijímať delegované akty uvedené v článku 5c ods. 7, článku 24 ods. 6 a článku 30 ods. 4 sa Komisii udeľuje na dobu neurčitú od 17. septembra 2014.

3. Delegovanie právomoci uvedené v článku 5c ods. 7, článku 24 ods. 6 a článku 30 ods. 4 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej úni*e alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.“;

b) odsek 5 sa nahrádza takto:

„5. Delegovaný akt prijatý podľa článku 5c ods. 7, článku 24 ods. 6 alebo článku 30 ods. 4 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.“

49. V kapitole VI sa vkladá tento článok :

„*Článok 48a*
Požiadavky na podávanie správ

1. Členské štáty zabezpečujú zber štatistických údajov v súvislosti s fungovaním európskych peňaženiek digitálnej identity a kvalifikovaných dôveryhodných služieb, ktoré sa poskytujú na ich území.

2. Štatistické údaje získané v súlade s odsekom 1 zahŕňajú:

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) počet sťažností používateľov a incidentov v oblasti ochrany spotrebiteľa alebo ochrany údajov v súvislosti so spoliehajúcimi sa stranami a kvalifikovanými dôveryhodnými službami;

d) súhrnnú správu vrátane údajov o incidentoch, ktoré bránia používaniu európskej peňaženky digitálnej identity ;

e) zhrnutie významných bezpečnostných incidentov, porušení ochrany údajov a dotknutých používateľov európskych peňaženiek digitálnej identity alebo kvalifikovaných dôveryhodných služieb.

3. Štatistické údaje uvedené v odseku 2 sa zverejnia v otvorenom a bežne používanom strojovo čitateľnom formáte.

4. Členské štáty každoročne do 31. marca predložia Komisii správu o štatistických údajoch získaných v súlade s odsekom 2.“

50. Článok 49 sa nahrádza takto:

„*Článok 49*
Preskúmanie

1. Komisia preskúma uplatňovanie tohto nariadenia a do … [24 mesiacov odo dňa nadobudnutia účinnosti pozmeňujúceho nariadenia] o ňom podá Európskemu parlamentu a Rade správu. Komisia v tejto správe zhodnotí najmä to, či je vhodné upraviť rozsah pôsobnosti tohto nariadenia alebo jeho osobitné ustanovenia, okrem iného najmä ustanovenia uvedené v článku 5c ods. 5, pričom zohľadní skúsenosti získané pri uplatňovaní tohto nariadenia, ako aj technologický, trhový a právny vývoj. V prípade potreby sa k uvedenej správe pripojí návrh na zmenu tohto nariadenia.

2. Správa uvedená v odseku 1 obsahuje posúdenie dostupnosti, bezpečnosti a použiteľnosti oznámených prostriedkov elektronickej identifikácie a európskych peňaženiek digitálnej identity, ktoré patria do rozsahu pôsobnosti tohto nariadenia, a posúdi sa v nej, či sa od všetkých súkromných poskytovateľov online služieb, ktorí na účely autentifikácie používateľov využívajú služby elektronickej identifikácie tretích strán, má vyžadovať, aby akceptovali používanie oznámených prostriedkov elektronickej identifikácie a európskej peňaženky digitálnej identity.

3. Komisia do … [šesť rokov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] a potom každé štyri roky predloží Európskemu parlamentu a Rade správu o pokroku dosiahnutom pri plnení cieľov tohto nariadenia.“

51. 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 odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] .

2. Kvalifikované certifikáty vydané fyzickým osobám podľa smernice 1999/93/ES sa naďalej považujú za kvalifikované certifikáty pre elektronický podpis podľa tohto nariadenia do … [24 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia] .

3. Správa zariadení na vyhotovenie kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate na diaľku kvalifikovanými poskytovateľmi dôveryhodných služieb, ktorí nie sú 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 môže vykonávať bez toho, aby bolo potrebné získať kvalifikovaný štatút na poskytovanie týchto služieb správy, a to do … [24 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia].

4. Kvalifikovaní poskytovatelia dôveryhodných služieb, ktorým bol udelený kvalifikovaný štatút podľa tohto nariadenia pred … [dátum nadobudnutia účinnosti tohto pozmeňujúceho nariadenia], predložia orgánu dohľadu správu o posúdení zhody preukazujúcu súlad s článkom 24 ods. 1, 1a a 1b čo najskôr, avšak v každom prípade do … [24 mesiacov odo dňa nadobudnutia účinnosti tohto pozmeňujúceho nariadenia].“

52. Prílohy I až IV sa menia v súlade s prílohami I až IV k tomuto nariadeniu.

53. Dopĺňajú sa nové prílohy V, VI a VII, ktoré sa uvádzajú v prílohách V, VI a VII k tomuto nariadeniu.

Článok 2

Nadobudnutie účinnosti

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 …,

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda/predsedníčka*

PRÍLOHA I

V prílohe I k nariadeniu (EÚ) č. 910/2014 sa písmeno i) nahrádza takto:

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

PRÍLOHA II

V prílohe II k nariadeniu (EÚ) č. 910/2014 sa body 3 a 4 vypúšťajú.

PRÍLOHA III

V prílohe III k nariadeniu (EÚ) č. 910/2014 sa písmeno i) nahrádza takto:

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

PRÍLOHA IV

Príloha IV k nariadeniu (EÚ) č. 910/2014 sa mení takto:

1. Písmeno c) sa nahrádza takto:

„c) v prípade fyzických osôb: aspoň meno osoby, ktorej sa certifikát vydal, alebo pseudonym; ak sa používa pseudonym, táto skutočnosť sa musí jednoznačne uviesť;

ca) v prípade právnických osôb: jedinečný súbor údajov jednoznačne reprezentujúcich právnickú osobu, ktorej sa certifikát vydáva, aspoň s názvom právnickej osoby, ktorej sa certifikát vydáva, a v príslušných prípadoch s registračným číslom uvedeným v úradných záznamoch;“

2. Písmeno j) sa 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

„PRÍLOHA V

POŽIADAVKY NA KVALIFIKOVANÉ ELEKTRONICKÉ OSVEDČENIE ATRIBÚTOV

Kvalifikované elektronické osvedčenie atribútov obsahuje:

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

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

   i) v prípade právnickej osoby: meno a v príslušnom prípade registračné číslo tak, ako sa uvádza v úradných záznamoch,

   ii) v prípade fyzickej osoby: meno osoby;

c) súbor údajov jednoznačne reprezentujúcich subjekt, na ktorý sa osvedčené atribúty vzťahujú; ak sa používa pseudonym, táto skutočnosť sa musí jednoznačne uviesť;

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 kvalifikovaného poskytovateľa dôveryhodných služieb, a v príslušných prípadoch uvedenie systému osvedčení, ktorého je osvedčenie atribútov súčasťou;

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

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 kvalifikovaného osvedčenia.“.

PRÍLOHA VI

„PRÍLOHA VI

MINIMÁLNY ZOZNAM ATRIBÚTOV

Podľa článku 45e členské štáty zabezpečia, aby sa prijali opatrenia, ktoré kvalifikovaným poskytovateľom dôveryhodných služieb 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 právom Únie alebo vnútroštátnym právom 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 licencie;

8. odborná kvalifikácia, tituly a licencie;

9. splnomocnenia a mandáty zastupovať fyzické alebo právnické osoby;

10. verejné povolenia a licencie;

11. v prípade právnických osôb finančné a podnikové údaje.“.

PRÍLOHA VII

„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 v príslušnom prípade jeho registračné číslo, ako sa uvádza v úradných záznamoch;

c) súbor údajov jednoznačne reprezentujúcich subjekt, na ktorý sa osvedčené atribúty vzťahujú; ak sa používa pseudonym, táto skutočnosť sa musí jednoznačne uviesť;

d) osvedčený atribút alebo atribúty, v príslušnom prípade 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 príslušnom prípade 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.“.