Svet
Evropske unije

Bruselj, 6. december 2022
(OR. en)

15706/22

Medinstitucionalna zadeva:
2021/0136(COD)

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

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Datum:	6. december 2022
Prejemnik:	delegacije
Št. predh. dok.:	14959/22 + ADD 1 + ADD 2
Št. dok. Kom.:	9471/21
Zadeva:	Predlog uredbe Evropskega parlamenta in Sveta o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo okvira za evropsko digitalno identiteto – splošni pristop (6. december 2022)

V prilogi vam pošiljamo besedilo splošnega pristopa Sveta v zvezi z navedenim predlogom, ki ga je Svet (promet, telekomunikacije in energija) sprejel na 3917. seji 6. decembra 2022.

Splošni pristop, ki določa začasno stališče Sveta o tem predlogu, je podlaga za pripravo pogajanj z Evropskim parlamentom.

PRILOGA

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo okvira za evropsko digitalno identiteto

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[1],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

„(1) V sporočilu Komisije z dne 19. februarja 2020 z naslovom „Oblikovanje digitalne prihodnosti Evrope“[2] je napovedana revizija Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta s ciljem izboljšati njeno učinkovitost, razširiti njene koristi na zasebni sektor ter spodbujati zaupanja vredne digitalne identitete za vse Evropejce.

[1] UL C , , str. .
[2] COM(2020) 67 final.

„(2) Evropski svet je v svojih sklepih z dne 1. in 2. oktobra 2020[3] pozval Komisijo, naj predlaga razvoj okvira za varno javno elektronsko identifikacijo na ravni Unije, vključno z interoperabilnimi digitalnimi podpisi, da bi ljudje imeli nadzor nad svojo spletno identiteto in podatki ter da se omogoči dostop do javnih, zasebnih in čezmejnih digitalnih storitev.

„(3) V sporočilu Komisije z dne 9. marca 2021 z naslovom „Digitalni kompas do leta 2030: evropska pot v digitalno desetletje“[4] je določen cilj glede okvira Unije, ki naj bi do leta 2030 omogočil široko uporabo zaupanja vredne identitete pod nadzorom uporabnika, ki bi vsakemu državljanu omogočila nadzor nad lastno komunikacijo in prisotnostjo na spletu.

„(4) Bolj usklajen pristop k digitalni identifikaciji bi moral zmanjšati tveganja in znižati stroške sedanje razdrobljenosti zaradi uporabe različnih nacionalnih rešitev ter bo okrepil enotni trg z omogočanjem priročne in enotne spletne identifikacije državljanom, drugim rezidentom, kot so opredeljeni z nacionalnim pravom, in podjetjem po vsej Uniji. Evropska denarnica za digitalno identiteto bo fizičnim in pravnim osebam po vsej Uniji zagotovila harmonizirano sredstvo elektronske identifikacije, ki jim bo omogočilo avtentikacijo in izmenjavo podatkov, povezanih z njihovo identiteto. Vsem bi moral biti omogočen varen dostop do javnih in zasebnih storitev, ki temeljijo na izboljšanem ekosistemu za storitve zaupanja ter preverjenih dokazilih o identiteti in potrdilih o atributih, kot je univerzitetna diploma, ki je zakonsko priznana in sprejeta po vsej Uniji. Okvir za evropsko digitalno identiteto je namenjen uresničitvi prehoda z zanašanja samo na nacionalne rešitve digitalne identitete na zagotavljanje elektronskih potrdil o atributih, veljavnih na evropski ravni. Ponudniki elektronskega potrjevanja atributov bi morali imeti koristi od jasnih in enotnih pravil, javnim upravam pa bi moralo biti omogočeno, da se zanašajo na elektronske dokumente v določeni obliki.

---

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

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

(4a) Več držav članic je uvedlo in večinoma uporablja sredstva elektronske identifikacije, ki jih danes ponudniki storitev v Uniji sprejemajo. Poleg tega so bile izvedene naložbe v nacionalne in čezmejne rešitve na podlagi sedanje uredbe eIDAS, vključno s tehnično infrastrukturo za interoperabilnost vozlišč eIDAS. Da bi zagotovili dopolnjevanje in bi sedanji uporabniki priglašenih sredstev elektronske identifikacije hitro sprejeli evropske denarnice za digitalno identiteto ter da bi čim bolj zmanjšali učinke na obstoječe ponudnike storitev, bi bilo treba pri evropskih denarnicah za digitalno identiteto izkoristiti izkušnje z obstoječimi sredstvi elektronske identifikacije in vzpostavljeno infrastrukturo eIDAS na evropski in nacionalni ravni.

„(5) Za podpiranje konkurenčnosti evropskih podjetij bi moralo biti ponudnikom spletnih storitev omogočeno, da se zanašajo na rešitve digitalne identitete, priznane po vsej Uniji, ne glede na državo članico, v kateri so bile izdane, ter tako izkoriščajo usklajen evropski pristop k zaupanju, varnosti in interoperabilnosti. Uporabniki in ponudniki storitev bi morali imeti koristi od enake pravne veljave, kot je zagotovljena elektronskim potrdilom o atributih po vsej Uniji.

„(6) Uredba (EU) št. 2016/679[5] se uporablja za obdelavo osebnih podatkov pri izvajanju te uredbe. Zato bi morali biti v tej uredbi določeni posebni zaščitni ukrepi, ki bi ponudnikom sredstev za elektronsko identifikacijo in elektronskega potrjevanja atributov preprečevali združevanje osebnih podatkov iz drugih storitev z osebnimi podatki, povezanimi s storitvami, ki spadajo na področje uporabe te uredbe. Osebne podatke v zvezi z zagotavljanjem evropskih denarnic za digitalno identiteto bi bilo treba hraniti logično ločeno od vseh drugih podatkov, ki jih hrani izdajatelj. Ta uredba izdajateljem evropskih denarnic za digitalno identiteto ne preprečuje uporabe dodatnih tehničnih ukrepov, ki prispevajo k varstvu osebnih podatkov, kot je fizično ločevanje osebnih podatkov v zvezi z zagotavljanjem denarnic od vseh drugih podatkov, ki jih hranijo.

---

[5] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

„(7) Določiti je treba usklajene pogoje za vzpostavitev okvira za evropske denarnice za digitalno identiteto, ki bi jih izdajale države članice, ki bi morale opolnomočiti vse državljane Unije in druge rezidente, kot so opredeljeni z nacionalnim pravom, za varno izmenjavo podatkov, povezanih z njihovo identiteto, na uporabniku prijazen in priročen način pod izključnim nadzorom uporabnika. Razviti bi bilo treba tehnologije, ki bi se uporabljale za dosego teh ciljev ter bi bile namenjene doseganju najvišje ravni varnosti, zasebnosti, priročnosti za uporabnike in široke uporabnosti. Države članice bi morale zagotoviti enak dostop do digitalne identifikacije vsem svojim državljanom in rezidentom.

„(8) Da bi se zanašajoče se stranke lahko zanesle na uporabo evropskih denarnic za digitalno identiteto in da bi uporabnike zaščitili pred nezakonito uporabo občutljivih podatkov, bi zanašajoče se stranke morale biti registrirane v okviru postopka priglasitve. Zahteve glede priglasitve, ki se uporabljajo za zanašajoče se stranke, bi morale v večini primerov temeljiti na tem, da se zagotovi omejena količina informacij, potrebnih za avtentikacijo zanašajoče se stranke za vstop v evropsko denarnico za digitalno identiteto. Te zahteve bi morale omogočati tudi uporabo avtomatiziranega ali preprostega postopka samoprijave, med drugim tako, da bi se države članice opirale na obstoječe registre in jih uporabljale. Hkrati lahko za kategorije občutljivih podatkov obstajajo posebne ureditve na nacionalni ravni ali ravni Unije, v okviru katerih je zanašajočim se strankam mogoče naložiti strožje zahteve glede registracije in pridobitve dovoljenja, da bi v takih primerih preprečili nezakonito uporabo podatkov o identiteti. V drugih primerih uporabe so lahko zanašajoče se stranke izvzete iz obveznosti priglasitve namere, da se bodo zanašale na evropske denarnice za digitalno identiteto, na primer kadar za uveljavljanje pravice do preverjanja posebnih atributov avtentikacija zanašajoče se stranke z elektronskimi sredstvi ni potrebna ali ni mogoča. Običajno lahko uporabnik v teh scenarijih, ki se odvijajo v živo, identificira zanašajočo se stranko iz konteksta, na primer pri komuniciranju z uradnikom za najem avtomobila ali farmacevtom. Postopek priglasitve naj bi temeljil na sektorski zakonodaji Unije ali nacionalni zakonodaji, saj je tako mogoče upoštevati različne primere uporabe, ki se lahko razlikujejo z vidika zahtev glede registracije, načina delovanja (spletno/nespletno) ali zahtev glede avtentikacije naprav, ki se lahko povežejo z evropsko denarnico za digitalno identiteto. Preverjanja uporabe evropske denarnice za digitalno identiteto s strani zanašajočih se strank ne bi bilo treba predpisati na ravni evropske denarnice za digitalno identiteto.

„(9) Vse evropske denarnice za digitalno identiteto bi morale uporabnikom omogočati čezmejno elektronsko identifikacijo ter spletno in nespletno avtentikacijo za dostopanje do različnih javnih in zasebnih storitev. Brez poseganja v pristojnosti držav članic, kar zadeva identifikacijo njihovih državljanov in rezidentov, se lahko denarnice uporabljajo tudi za izpolnjevanje institucionalnih potreb javnih uprav, mednarodnih organizacij ter institucij, organov, uradov in agencij Unije. Nespletna uporaba bi bila pomembna v številnih sektorjih, vključno z zdravstvenim, v katerem se storitve pogosto zagotavljajo prek osebne interakcije, pri e-receptih pa bi morala biti omogočena uporaba QR kod ali podobnih tehnologij za preverjanje avtentičnosti. Ker temeljijo na visoki ravni zanesljivosti, bi morale evropske denarnice za digitalno identiteto za izpolnitev zahtev iz te uredbe izkoristiti potencial rešitev za zaščito pred nedovoljenimi posegi, kot so varnostni elementi. Evropske denarnice za digitalno identiteto bi morale uporabnikom omogočati tudi ustvarjanje in uporabo kvalificiranih elektronskih podpisov in žigov, sprejetih po vsej EU. Za poenostavitev in koriščenje ugodnosti znižanja stroškov za osebe in podjetja po vsej EU, tudi z omogočanjem pooblastil za zastopanje in mandatov v elektronski obliki, bi morale države članice izdajati evropske denarnice za digitalno identiteto z uporabo skupnih standardov, da bi zagotovile nemoteno interoperabilnost in visoko raven varnosti. Samo pristojni organi držav članic lahko zagotovijo visoko stopnjo zaupanja v ugotavljanje identitete osebe, s čimer zagotovijo, da je oseba, ki izkazuje ali uveljavlja določeno identiteto, dejansko oseba, za katero se izkazuje. Zato morajo evropske denarnice za digitalno identiteto temeljiti na pravni identiteti državljanov, drugih rezidentov ali pravnih subjektov. Zaupanje v evropske denarnice za digitalno identiteto bi bilo okrepljeno z dejstvom, da morajo strani izdajateljice izvajati ustrezne tehnične in organizacijske ukrepe za zagotovitev ravni varnosti, ki je sorazmerna s tveganji, izpostavljenimi v zvezi s pravicami in svoboščinami fizičnih oseb, v skladu z Uredbo (EU) 2016/679. Izdaja, uporaba za avtentikacijo in preklic evropskih denarnic za digitalno identiteto so za fizične osebe brezplačni. Storitve, ki se zanašajo na uporabo denarnice, lahko ustvarijo stroške, npr. pri izdajanju elektronskih potrdil o atributih v denarnico.

(9a) Koristno bi bilo, da bi evropske denarnice za digitalno identiteto brezhibno vključili v ekosistem javnih in zasebnih digitalnih storitev, ki se že izvajajo na nacionalni, lokalni ali regionalni ravni, ter tako olajšali njihovo uvajanje in uporabo. Za dosego tega cilja lahko države članice določijo pravne in organizacijske ukrepe, da bi povečale prožnost za izdajatelje evropskih denarnic za digitalno identiteto in omogočile dodatne funkcije evropskih denarnic za digitalno identiteto, ki presegajo to, kar je določeno v tej uredbi, med drugim z večjo interoperabilnostjo z obstoječimi nacionalnimi sredstvi elektronske identifikacije. S tem nikakor ne bi smele ogroziti zagotavljanja osnovnih funkcij evropskih denarnic za digitalno identiteto, določenih v tej uredbi, niti prednostno promovirati obstoječih nacionalnih rešitev namesto evropskih denarnic za digitalno identiteto. Ker te dodatne funkcionalnosti presegajo to uredbo, se zanje ne uporabljajo določbe o čezmejni uporabi evropskih denarnic za digitalno identiteto iz te uredbe.

„(10) Da bi dosegli visoko raven varstva podatkov, varnosti in zanesljivosti, bi bilo treba s to uredbo vzpostaviti harmoniziran okvir, ki bi podrobno določal skupne specifikacije in zahteve, ki bi veljale za evropske denarnice za digitalno identiteto. Skladnost evropskih denarnic za digitalno identiteto s takimi zahtevami bi morali potrditi akreditirani organi za ugotavljanje skladnosti, ki jih imenujejo države članice. Certificiranje bi moralo temeljiti predvsem na ustreznih evropskih certifikacijskih shemah za kibernetsko varnost, vzpostavljenih v skladu z Uredbo (EU) 2019/881[6], ali njihovih delih, kolikor te sheme zajemajo zahteve glede kibernetske varnosti, ki se uporabljajo za evropske denarnice za digitalno identiteto. Opiranje na evropske certifikacijske sheme za kibernetsko varnost bi moralo pripomoči k usklajeni ravni zaupanja v varnost evropskih denarnic za digitalno identiteto, ne glede na to, kje v Uniji se izdajo. Certificiranje kibernetske varnosti evropskih denarnic za digitalno identiteto bi moralo temeljiti na vlogi nacionalnih certifikacijskih organov za kibernetsko varnost pri nadzoru in spremljanju skladnosti certifikatov, ki jih izdajo organi za ugotavljanje skladnosti v okviru svojih pristojnosti, z ustreznimi evropskimi shemami za kibernetsko varnost. Podobno bi moralo certificiranje po potrebi temeljiti na standardih in tehničnih specifikacijah iz Uredbe (EU) 2019/881. Take specifikacije se lahko uporabljajo kot najsodobnejši dokumenti, kot je določeno v ustreznih certifikacijskih shemah za kibernetsko varnost v skladu z Uredbo (EU) 2019/881. Kadar nobena ustrezna evropska certifikacijska shema za kibernetsko varnost, vzpostavljena v skladu z Uredbo (EU) 2019/881, ne zajema certificiranja ustreznih storitev ali postopkov, ki prispevajo k varnosti denarnice, bi bilo treba vzpostaviti ustrezne sheme v skladu z naslovom III Uredbe (EU) 2019/881. Vzpostaviti bi bilo treba skupno in harmonizirano shemo za certificiranje evropskih denarnic za digitalno identiteto, da bi ocenili njihovo skladnost s skupnimi specifikacijami in zahtevami iz te uredbe, z izjemo tistih, ki so povezane s kibernetsko varnostjo in varstvom podatkov, zlasti pa s tistimi, ki zajemajo funkcionalne in operativne vidike. V zvezi s tem certificiranjem bi bilo treba za zagotovitev visoke ravni zaupanja in preglednosti vzpostaviti mehanizme in postopke za spodbujanje vzajemnega učenja in sodelovanja med državami članicami pri spremljanju in preverjanju certifikacijskih organov ter potrdil in poročil o certificiranju, ki jih izdajo. Tak mehanizem vzajemnega učenja ne bi smel posegati v Uredbo (ES) 2016/679 in Uredbo (EU) 2019/881. Certificiranje denarnice v skladu z Uredbo (ES) 2016/679 je prostovoljno orodje, ki se lahko med drugim uporablja za dokazovanje skladnosti z zahtevami iz Uredbe (ES) 2016/679, saj se te uporabljajo za evropske denarnice za digitalno identiteto in zagotavljanje teh denarnic evropskim državljanom.

[6] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

(10a) Vstop državljanov in prebivalcev v evropsko denarnico za digitalno identiteto bi bilo treba olajšati z uporabo sredstev elektronske identifikacije, izdanih z „visoko“ ravnjo zanesljivosti. Sredstva elektronske identifikacije, izdana s „srednjo“ ravnjo zanesljivosti, bi se smela uporabljati le v primeru, da usklajene tehnične in operativne specifikacije, pri katerih se uporabljajo sredstva elektronske identifikacije, izdana z „srednjo“ ravnjo zanesljivosti, v kombinaciji z drugimi dodatnimi sredstvi za preverjanje identitete omogočajo izpolnjevanje zahtev glede „visoke “ravni zanesljivosti iz te uredbe. Taka dodatna sredstva ali ukrepi bi morali biti zanesljivi in enostavni za uporabnike ter bi lahko temeljili na možnosti uporabe postopkov vstopa na daljavo, kvalificiranih potrdil, podprtih s kvalificiranimi podpisi, kvalificiranega elektronskega potrdila o atributih ali kombinacije navedenega. Da bi zagotovili zadostno uporabo evropskih denarnic za digitalno identiteto, bi bilo treba v izvedbenih aktih določiti harmonizirane tehnične in operativne specifikacije za vstop uporabnikov z uporabo sredstev elektronske identifikacije, vključno s tistimi, ki se izdajo na „srednji“ ravni zanesljivosti.

(10b) Cilj te uredbe je zagotoviti popolnoma mobilno, varno in uporabniku prijazno evropsko denarnico za digitalno identiteto. Kot prehodni ukrep se lahko za evropske denarnice za digitalno identiteto, dokler ne bodo na voljo certificirane rešitve, zaščitene pred nedovoljenimi posegi, na primer varnostni elementi v napravah uporabnikov, uporabljajo certificirani zunanji varnostni elementi za zaščito kriptografskega materiala in drugih občutljivih podatkov ali priglašene nacionalne rešitve z „visoko“ ravnjo zanesljivosti, da se dokaže skladnost z ustreznimi zahtevami iz Uredbe v zvezi z ravnjo zanesljivosti denarnice. Uporaba navedenega prehodnega ukrepa bi morala biti omejena na primere, za katere je zahtevana „visoka“ raven zanesljivosti, kot sta vstop uporabnika v denarnico in avtentikacija za storitve, za katere je zahtevana „visoka“ raven zanesljivosti. Pri avtentikaciji za storitve, za katere je zahtevana „srednja“ stopnja zanesljivosti, uporaba navedenega predhodnega ukrepa za evropsko denarnico za digitalno identiteto ne bi bila obvezna. Ta uredba ne bi smela posegati v nacionalne pogoje za izdajo in uporabo certificiranega zunanjega varnostnega elementa, če ta prehodni ukrep temelji na njem.

„(11) Evropske denarnice za digitalno identiteto bi morale zagotoviti najvišjo raven varovanja in varnosti osebnih podatkov, ki se uporabljajo za avtentikacijo, ne glede na to, ali se taki podatki shranjujejo lokalno ali v rešitvah v oblaku, ob upoštevanju različnih ravni tveganja. Obdelava biometričnih podatkov kot dejavnika avtentikacije v okviru močne avtentikacije uporabnika je eden od načinov identifikacije, ki zagotavlja visoko stopnjo zaupanja, zlasti če se uporablja v kombinaciji z drugimi elementi avtentikacije. Ker so biometrični podatki enolična značilnost osebe, je njihova obdelava dovoljena le v skladu z izjemami iz člena 9(2) Uredbe (EU) 2016/679 in so zanjo potrebni ustrezni zaščitni ukrepi, sorazmerni s tveganjem, ki ga taka obdelava lahko vključuje za pravice in svoboščine fizičnih oseb.

(11a) Delovanje evropskih denarnic za digitalno identiteto bi moralo biti pregledno in omogočati preverljivo obdelavo osebnih podatkov. V ta namen se priporoča, da države članice razkrijejo izvorno kodo komponent programske opreme evropskih denarnic za digitalno identiteto, ki so povezane z obdelavo osebnih podatkov in podatkov pravnih oseb. Razkritje take izvorne kode omogoča družbi, med drugim uporabnikom in programerjem, da razumejo delovanje evropskih denarnic. To bi lahko tudi povečalo zaupanje uporabnikov v ekosistem denarnic in prispevalo k varnosti denarnic, saj bi lahko vsakdo prijavil šibke točke in napake v kodi. To spodbuja dobavitelje, da dobavijo in vzdržujejo zelo varen izdelek. Poleg tega se priporoča, da države članice po potrebi dajo izvorno kodo na voljo v okviru odprtokodne licence. Odprtokodna licenca družbi, med drugim uporabnikom in programerjem, omogoča spreminjanje in ponovno uporabo izvorne kode.

„(12) Za zagotovitev, da je evropski okvir za digitalno identiteto odprt za inovacije in tehnološki razvoj ter kos izzivom prihodnosti, bi bilo treba države članice spodbujati k skupni vzpostavitvi peskovnikov za preizkušanje inovativnih rešitev v nadzorovanem in varnem okolju, zlasti za izboljšanje funkcionalnosti, varstva osebnih podatkov, varnosti in interoperabilnosti rešitev, ter k obveščanju o prihodnjih posodobitvah tehničnih referenc in pravnih zahtev. To okolje bi moralo spodbujati vključevanje malih in srednjih podjetij, zagonskih podjetij ter posameznih inovatorjev in raziskovalcev.

„(13) Uredba (EU) št. 2019/1157[7] krepi varnost osebnih izkaznic z izboljšanimi varnostnimi značilnostmi do avgusta 2021. Države članice bi morale preučiti možnost njihove priglasitve v okviru shem elektronske identifikacije za razširitev čezmejne razpoložljivosti sredstev elektronske identifikacije.

„(14) Postopek priglasitve sheme elektronske identifikacije bi bilo treba poenostaviti in pospešiti za spodbujanje dostopa do uporabnih, zaupanja vrednih, varnih in inovativnih rešitev avtentikacije in identifikacije ter, če je ustrezno, za spodbujanje zasebnih ponudnikov identitete, naj organom države članice ponujajo sheme elektronske identifikacije za priglasitev kot nacionalne sheme elektronske identifikacije v skladu z Uredbo (EU) št. 910/2014.

„(15) Racionalizacija sedanjih postopkov priglasitve in medsebojnih strokovnih pregledov bo preprečila raznolike pristope k ocenjevanju različnih priglašenih shem elektronske identifikacije in olajšala krepitev zaupanja med državami članicami. Novi, poenostavljeni mehanizmi bi morali spodbujati sodelovanje držav članic na področju varnosti in interoperabilnosti njihovih priglašenih shem elektronske identifikacije.

„(16) Države članice bi morale imeti koristi od novih, prožnih orodij za zagotavljanje izpolnjevanja zahtev iz te uredbe in ustreznih izvedbenih aktov. Ta uredba bi morala državam članicam omogočati uporabo poročil in ocen, ki jih izvedejo akreditirani organi za ugotavljanje skladnosti, kot je predvideno v okviru certifikacijskih shem, ki se vzpostavijo na ravni Unije na podlagi Uredbe (EU) 2019/881, v podporo njihovim zahtevam po uskladitvi shem ali njihovih delov z zahtevami uredbe eIDAS glede interoperabilnosti in varnosti priglašenih shem elektronske identifikacije.

---

[7] Uredba (EU) 2019/1157 Evropskega parlamenta in Sveta z dne 20. junija 2019 o okrepitvi varnosti osebnih izkaznic državljanov Unije in dokumentov za prebivanje, izdanih državljanom Unije in njihovim družinskim članom, ki uresničujejo svojo pravico do prostega gibanja (UL L 188, 12.7.2019, str. 67).

(17a) Uporaba enoličnih in stalnih identifikatorjev, ki jih izdajo države članice ali ki jih ustvari evropska denarnica za digitalno identiteto, je skupaj z uporabo identifikacijskih podatkov osebe nujna za zagotovitev, da se lahko preveri identiteta uporabnika, predvsem v javnem sektorju in kadar to predpisuje nacionalno pravo ali pravo Unije. S to uredbo bi bilo treba zagotoviti, da se lahko z evropsko denarnico za digitalno identiteto da na voljo mehanizem, ki omogoča usklajevanje evidenc, med drugim z uporabo kvalificiranih elektronskih potrdil o atributih, ter vključitev enoličnih in stalnih identifikatorjev v naboru identifikacijskih podatkov osebe. Enolični in stalni identifikator je lahko sestavljen iz enega ali več identifikacijskih podatkov, ki so lahko značilni za posamezen sektor, pod pogojem da ta identifikator enolično identificira uporabnika po vsej Uniji. Evropska denarnica za digitalno identiteto bi morala zagotavljati tudi mehanizem, ki omogoča uporabo identifikatorjev, značilnih za zanašajočo se stranko, v primerih, ko nacionalno pravo ali pravo Unije predpisuje uporabo enoličnega in stalnega identifikatorja. V vseh primerih bi moral mehanizem, namenjen lažjemu usklajevanju evidenc ter uporabi enoličnih in stalnih identifikatorjev, zagotavljati zaščito uporabnika pred zlorabo osebnih podatkov v skladu s to uredbo in veljavnim pravom Unije, zlasti Uredbo (EU) 2016/679, med drugim pred tveganjem oblikovanja profilov in sledenja, povezanih z uporabo evropske denarnice za digitalno identiteto.

(17aa) Nujno je treba upoštevati potrebe uporabnikov in tako spodbuditi povpraševanje po evropskih denarnicah za digitalno identiteto. Na voljo bi morali biti smiselni primeri uporabe in spletne storitve, ki bi temeljile na evropskih denarnicah za digitalno identiteto. Zaradi večje praktičnosti za uporabnike in da bi zagotovili čezmejno razpoložljivost takih storitev, je treba sprejeti ukrepe, ki bi omogočili, da bi v vseh državah članicah na podoben način pristopili k zasnovi, razvoju in uvajanju spletnih storitev. Nezavezujoče smernice o tem, kako snovati, razvijati in uvajati spletne storitve, ki temeljijo na evropskih denarnicah za digitalno identiteto, bi lahko pripomogle k doseganju tega cilja. Te smernice bi bilo treba pripraviti ob ustreznem upoštevanju okvira Unije za interoperabilnost. Pri njihovem sprejemanju bi morale imeti glavno vlogo države članice.

„(18) V skladu z Direktivo (EU) 2019/882[8] bi morala biti invalidom omogočena uporaba evropskih denarnic za digitalno identiteto, storitev zaupanja in proizvodov za končne uporabnike, ki se uporabljajo pri zagotavljanju zadevnih storitev, pod enakimi pogoji, kot veljajo za druge uporabnike.

„(19) Ta uredba ne bi smela zajemati vidikov, povezanih s sklepanjem in veljavnostjo pogodb ali drugih pravnih obveznosti, če nacionalno pravo ali pravo Unije določa zahteve glede obličnosti. Poleg tega ne bi smela vplivati na nacionalne zahteve glede obličnosti, ki se nanašajo na javne registre, zlasti poslovne registre in zemljiške knjige.

„(20) Zagotavljanje in uporaba storitev zaupanja postajata vse pomembnejša za mednarodno trgovino in sodelovanje. Mednarodni partnerji EU vzpostavljajo okvire zaupanja, ki temeljijo na Uredbi (EU) št. 910/2014. Zato lahko izvedbena zakonodaja za olajšanje priznavanja takih storitev in njihovih ponudnikov določa pogoje, pod katerimi bi se okviri zaupanja tretjih držav lahko šteli za enakovredne okviru zaupanja za kvalificirane storitve zaupanja in ponudnike iz te uredbe, kot dopolnitev možnosti vzajemnega priznavanja storitev zaupanja in ponudnikov s sedežem v Uniji in v tretjih državah v skladu s členom 218 Pogodbe. Pri določanju pogojev, pod katerimi bi se okviri zaupanja tretjih držav lahko šteli za enakovredne okviru zaupanja za kvalificirane storitve zaupanja in ponudnike iz te uredbe, sta bistvena elementa za krepitev zaupanja tudi zagotavljanje skladnosti z ustreznimi določbami Direktive XXXX/XXXX (direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji) in Uredbe (EU) 2016/679 ter uporaba zanesljivih seznamov.

[8] Direktiva (EU) 2019/882 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o zahtevah glede dostopnosti za proizvode in storitve (UL L 151, 7.6.2019, str. 70).

„(21) Ta uredba bi morala temeljiti na aktih Unije, ki zagotavljajo odprte in pravične trge v digitalnem sektorju. Njena podlaga je zlasti Uredba (EU) 2022/1925, ki uvaja pravila za ponudnike jedrnih platformnih storitev, ki so imenovani za vratarje, in, med drugim, prepoveduje vratarjem, da od poslovnih uporabnikov zahtevajo, naj uporabljajo ali ponujajo storitev identifikacije, ki jo zagotavlja vratar, ali zagotavljajo interoperabilnost z njo, v okviru storitev, ki jih ponujajo poslovni uporabniki, ki uporabljajo jedrne platformne storitve zadevnega vratarja. Člen 6(7) Uredbe 2022/1925 določa, da vratar poslovnim uporabnikom in ponudnikom pomožnih storitev omogoča dostop do istih funkcij operacijskega sistema, strojne opreme ali programske opreme, ki so na voljo vratarju ali jih vratar uporablja pri zagotavljanju morebitnih pomožnih storitev, ter interoperabilnost z njimi. V skladu s členom 2(15) akta o digitalnih trgih so storitve identifikacije vrsta pomožnih storitev. Poslovnim uporabnikom in ponudnikom pomožnih storitev bi morala biti zato omogočena dostop do strojne opreme ali funkcij programske opreme, kot so varnostni elementi v pametnih telefonih, in interoperabilnost z njimi prek evropskih denarnic za digitalno identiteto ali priglašenih sredstev elektronske identifikacije držav članic.

„(22) Za racionalizacijo obveznosti v zvezi s kibernetsko varnostjo, naloženih ponudnikom storitev, ter za omogočanje tem ponudnikom in njihovim ustreznim pristojnim organom, da izkoristijo pravni okvir, vzpostavljen z Direktivo XXXX/XXXX (direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji), morajo ponudniki storitev zaupanja sprejeti ustrezne tehnične in organizacijske ukrepe v skladu z Direktivo XXXX/XXXX (direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji), kot so ukrepi za obravnavanje sistemskih napak, človeških napak, zlonamernih dejanj ali naravnih pojavov, za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih zadevni ponudniki uporabljajo pri zagotavljanju svojih storitev, ter za priglasitev pomembnih incidentov v skladu z Direktivo XXXX/XXXX (direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji). Kar zadeva poročanje o incidentih, bi morali ponudniki storitev zaupanja priglasiti vse incidente, ki pomembno vplivajo na zagotavljanje njihovih storitev, vključno s takimi, ki so posledica kraje ali izgube naprav, poškodb omrežnega kabla ali incidentov, ki so se zgodili v okviru identifikacije oseb. Za zahteve glede obvladovanja tveganj za kibernetsko varnost in obveznosti poročanja iz Direktive XXXXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] bi se moralo šteti, da dopolnjujejo zahteve, naložene ponudnikom storitev zaupanja v skladu s to uredbo. Če je to ustrezno, bi morali pristojni organi, imenovani v skladu z Direktivo XXXXXX [direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji], še naprej uporabljati uveljavljene nacionalne prakse ali smernice v zvezi z izvajanjem zahtev glede varnosti in poročanja ter nadzor nad izpolnjevanjem takih zahtev v skladu z Uredbo (EU) št. 910/2014. Nobena zahteva v skladu s to uredbo ne vpliva na obveznost glede obveščanja o kršitvah varstva osebnih podatkov v skladu z Uredbo (EU) 2016/679.

„(23) Zagotoviti je treba ustrezno pozornost zagotavljanju učinkovitega sodelovanja med organi iz direktive o kibernetski varnosti in uredbe o eIDAS. Kadar se nadzorni organ iz te uredbe razlikuje od pristojnih organov, imenovanih v skladu z Direktivo XXXX/XXXX [direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji], bi morali zadevni organi pravočasno tesno sodelovati z izmenjavo ustreznih informacij, da bi se zagotovila učinkovit nadzor in izpolnjevanje zahtev iz te uredbe in Direktive XXXX/XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji]. Nadzorni organi iz te uredbe bi morali imeti pravico od pristojnega organa iz Direktive [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] zahtevati, naj predloži ustrezne informacije, potrebne za dodelitev kvalificiranega statusa in izvajanje nadzornih ukrepov za preverjanje, ali ponudniki storitev zaupanja izpolnjujejo ustrezne zahteve iz direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, ali zahtevati, naj odpravi neskladnost.

„(24) Zagotoviti je treba, da pravni okvir olajšuje čezmejno priznavanje med obstoječimi nacionalnimi pravnimi sistemi, povezanimi s storitvami elektronske priporočene dostave. Ta okvir bi lahko ustvaril tudi nove tržne priložnosti za ponudnike storitev zaupanja iz Unije, ki bi lahko ponujali nove vse-evropske storitve elektronske priporočene dostave. Da bi zagotovili, da bodo z uporabo kvalificirane storitve elektronske priporočene dostave podatki dostavljeni pravemu naslovniku, bi morala kvalificirana storitev elektronske priporočene dostave povsem zanesljivo zagotavljati identifikacijo naslovnika, medtem ko bi pri identifikaciji pošiljatelja zadostovala visoka stopnja zaupanja. Države članice bi morale ponudnike kvalificiranih storitev elektronske priporočene dostave spodbujati k interoperabilnosti njihovih storitev s kvalificiranimi storitvami elektronske priporočene dostave, ki jih zagotavljajo drugi ponudniki kvalificiranih storitev zaupanja, da bi se olajšal prenos podatkov med dvema ali več ponudniki kvalificiranih storitev zaupanja in spodbujale poštene prakse na notranjem trgu.

„(25) V večini primerov si državljani in drugi rezidenti ne morejo varno in z visoko ravnjo varstva podatkov digitalno čezmejno izmenjevati informacij, povezanih z njihovo identiteto, kot so naslovi, starost in poklicne kvalifikacije, vozniška in druga dovoljenja ter podatki o plačilih.

„(26) Omogočiti bi bilo treba izdajanje zaupanja vrednih digitalnih atributov in ravnanje z njimi ter prispevanje k zmanjšanju upravnega bremena z opolnomočenjem državljanov in drugih rezidentov za njihovo uporabo pri zasebnih in javnih transakcijah. Državljanom in drugim rezidentom bi bilo treba na primer omogočiti, da dokažejo lastništvo veljavnega vozniškega dovoljenja, ki ga je izdal organ v eni državi članici, ter da ga lahko preverijo in se nanj zanesejo ustrezni organi v drugi državi članici, da se lahko zanašajo na socialnovarnostne poverilnice ali prihodnje digitalne potovalne dokumente v čezmejnem okviru.

„(27) Vsakemu subjektu, ki zbira, ustvarja in izdaja potrjene atribute, kot so diplome, spričevala, rojstni listi, bi moralo biti omogočeno, da postane ponudnik elektronskih potrdil o atributih. Zanašajoče se stranke bi morale uporabljati elektronska potrdila o atributih kot enakovredna potrdilom v papirni obliki. Zato se elektronskim potrdilom o atributih ne bi smelo odvzeti pravnega učinka na podlagi tega, da gre za elektronsko obliko ali ker ne izpolnjujejo zahtev glede kvalificiranih elektronskih potrdil o atributih. V ta namen bi bilo treba določiti splošne zahteve za zagotovitev, da imajo kvalificirana elektronska potrdila o atributih enak pravni učinek kot zakonito izdana potrdila v papirni obliki. Vendar bi se morale take zahteve uporabljati brez poseganja v pravo Unije ali nacionalno pravo, v katerem so opredeljene dodatne zahteve za posamezne sektorje glede obličnosti s temeljnimi pravnimi učinki in zlasti čezmejnim priznavanjem kvalificiranih elektronskih potrdil o atributih, kjer je to primerno.

„(28) Široka razpoložljivost in uporabnost evropskih denarnic za digitalno identiteto zahtevata njihovo sprejemanje s strani ponudnikov zasebnih storitev. Zasebne zanašajoče se stranke, ki zagotavljajo storitve na področjih prometa, energetike, bančništva, finančnih storitev, socialnega varstva, zdravja, pitne vode, poštnih storitev, digitalne infrastrukture, izobraževanja ali telekomunikacij, bi morale sprejeti uporabo evropskih denarnic za digitalno identiteto za zagotavljanje storitev, za katere nacionalno pravo ali pravo Unije ali pogodbena obveznost zahteva močno avtentikacijo uporabnikov. Da bi spodbudili uporabo in sprejemanje evropske denarnice za digitalno identiteto, bi bilo treba upoštevati splošno sprejete sektorske standarde in specifikacije. Kadar zelo velike spletne platforme, kot so opredeljene v členu 25(1) Uredbe [referenčne uredbe, tj. akta o digitalnih storitvah], od uporabnikov zahtevajo avtentikacijo za dostop do spletnih storitev, bi morale sprejeti uporabo evropskih denarnic za digitalno identiteto na podlagi prostovoljne zahteve uporabnika. Uporabniki ne bi smeli biti obvezani uporabljati denarnice za dostop do zasebnih storitev, vendar če to želijo, bi morale velike spletne platforme sprejeti evropsko denarnico za digitalno identiteto za ta namen, ob upoštevanju načela podatkovne minimizacije. Glede na pomen zelo velikih spletnih platform je zaradi njihovega dosega, zlasti kot so navedli številni prejemniki storitve in kot se je izkazalo pri številnih gospodarskih transakcijah, to potrebno za povečanje zaščite uporabnikov pred goljufijami in zagotovitev visoke ravni varstva podatkov. Oblikovati bi bilo treba samoregulativne kodekse ravnanja na ravni Unije (v nadaljnjem besedilu: kodeksi ravnanja), da bi prispevali k široki razpoložljivosti in uporabnosti sredstev elektronske identifikacije, vključno z evropskimi denarnicami za digitalno identiteto v okviru področja uporabe te uredbe. Kodeksi ravnanja bi morali olajšati široko sprejemanje sredstev elektronske identifikacije, vključno z evropskimi denarnicami za digitalno identiteto, tudi pri tistih ponudnikih storitev, ki se ne štejejo za zelo velike spletne platforme in za avtentikacijo uporabnikov uporabljajo storitve elektronske identifikacije tretjih oseb. Pripraviti bi jih bilo treba v 12 mesecih po sprejetju te uredbe. Komisija bi morala oceniti učinkovitost teh določb za razpoložljivost in uporabnost evropskih denarnic za digitalno identiteto za uporabnike v 24 mesecih po njihovi uvedbi.

„(29) Selektivno razkrivanje je koncept, ki lastniku podatkov omogoča, da razkrije le nekatere dele večjega nabora podatkov, da bi lahko prejemnik pridobil le potrebne informacije; uporabnik torej zanašajoči se stranki razkrije samo podatke, ki so potrebni za zagotavljanje storitve, ki jo zahteva uporabnik. Evropska denarnica za digitalno identiteto bi morala tehnično omogočati selektivno razkrivanje atributov zanašajočim se strankam. Taki selektivno razkriti atributi bi se lahko – tudi tedaj, ko bi izvirali iz več ločenih elektronskih potrdil – naknadno združili in predložili zanašajočim se strankam. To bi moralo postati značilnost osnovne zasnove, s čimer bi se povečala uporabnost in izboljšalo varstvo osebnih podatkov, vključno s podatkovno minimizacijo.

„(30) Atributi, ki jih zagotovijo ponudniki kvalificiranih storitev zaupanja v okviru kvalificiranih potrdil o atributih, bi se morali preverjati glede na verodostojne vire bodisi neposredno s strani ponudnika kvalificiranih storitev zaupanja bodisi prek posrednikov, priznanih na nacionalni ravni v skladu z nacionalnim pravom ali pravom Unije za varno izmenjavo potrjenih atributov med ponudniki storitev identifikacije ali potrjevanja atributov in zanašajočimi se strankami. Države članice bi morale na nacionalni ravni vzpostaviti ustrezne mehanizme, da bi lahko ponudniki kvalificiranih storitev zaupanja, ki izdajajo kvalificirana elektronska potrdila o atributih, na podlagi privolitve osebe, ki ji je potrdilo izdano, preverili avtentičnost atributov, ki se opirajo na verodostojne vire. Med ustrezne mehanizme lahko spada tudi uporaba posebnih posrednikov ali tehničnih rešitev v skladu z nacionalno zakonodajo, ki omogočajo dostop do verodostojnih virov. Z zagotavljanjem razpoložljivosti mehanizma, ki bo omogočal preverjanje atributov glede na verodostojne vire, bi ponudnikom kvalificiranih storitev zaupanja, ki izdajajo kvalificirana elektronska potrdila o atributih, olajšali izpolnjevanje njihovih obveznosti iz te uredbe. V Prilogi VI je naveden seznam kategorij atributov, glede katerih bi države članice morale zagotoviti, da se sprejmejo ukrepi, s katerimi lahko kvalificirani ponudniki, ki izdajajo elektronska potrdila o atributih, z elektronskimi sredstvi na zahtevo uporabnika preverijo njihovo avtentičnost na podlagi ustreznega verodostojnega vira. Države članice bi se morale dogovoriti, kateri posebni atributi spadajo v te kategorije.

„(31) Varna elektronska identifikacija in potrjevanje atributov bi prinesla dodatno prožnost in rešitve za sektor finančnih storitev, ki bi omogočale identifikacijo strank in izmenjavo posebnih atributov, potrebnih za izpolnitev, na primer, zahtev glede skrbnega preverjanja strank iz uredbe o preprečevanju pranja denarja [sklic se doda po sprejetju predloga] ali zahtev glede primernosti, ki izhajajo iz zakonodaje o varstvu vlagateljev, ali podpirale izpolnjevanje zahtev glede močne avtentikacije strank za spletno identifikacijo zaradi prijave v račun in začetek transakcij na področju plačilnih storitev.

(31a) Da bi zagotovila skladnost praks certificiranja po vsej EU, bi morala Komisija izdati smernice o certificiranju in ponovnem certificiranju naprav za ustvarjanje kvalificiranega elektronskega podpisa in naprav za ustvarjanje kvalificiranega elektronskega žiga, tudi glede njihove veljavnosti in časovnih omejitev. Ta uredba državam članicam ne preprečuje, da javnim ali zasebnim organom, ki so certificirali naprave za ustvarjanje kvalificiranega elektronskega podpisa, dovolijo, da začasno podaljšajo veljavnost certificiranja, kadar iste naprave ni bilo mogoče ponovno certificirati v zakonsko določenem časovnem okviru iz razloga, ki ni kršitev ali varnostni incident, ter brez poseganja v veljavno prakso certificiranja.

„(32) Storitve za avtentikacijo spletišč uporabnikom z visoko ravnijo zanesljivosti zagotavljajo, da za spletiščem stoji pristen in legitimen subjekt, in to ne glede na platformo, ki je uporabljena za njegov prikaz. Te storitve prispevajo h krepitvi zaupanja v poslovanje prek spleta in zmanjševanju števila goljufij na spletu. Uporaba storitev za avtentikacijo spletišč bi morala biti prostovoljna. Da bi avtentikacija spletišč postala sredstvo za krepitev zaupanja in zagotavljanje boljše izkušnje uporabnikov ter spodbujanje rasti na notranjem trgu, bi se morale s to uredbo določiti minimalne obveznosti glede varnosti in odgovornosti za ponudnike storitev za avtentikacijo spletišč in njihove storitve. V ta namen bi morali ponudniki spletnih brskalnikov zagotavljati podporo in interoperabilnost s kvalificiranimi potrdili za avtentikacijo spletišč v skladu z Uredbo (EU) št. 910/2014. Priznati bi morali kvalificirana potrdila za avtentikacijo spletišč in končnemu uporabniku omogočiti, da se mu v okolju brskalnika prikažejo certificirani podatki o identiteti na podlagi specifikacij, določenih v skladu s to uredbo. Priznavanje kvalificiranega potrdila za avtentikacijo spletišč kot kvalificiranega potrdila, ki ga izda ponudnik kvalificiranih storitev zaupanja, bi moralo omogočiti, da se podatki o identiteti, vključeni v certifikat, avtenticirajo in preverijo v skladu s to uredbo. To ne bi smelo vplivati na možnost ponudnikov spletnih brskalnikov za odpravljanje večjih neskladnosti, povezanih s kršitvijo varnosti in izgubo celovitosti posameznih potrdil, da bi tako pripomogli k spletni varnosti končnih uporabnikov. Da bi še bolje zaščitili državljane in še spodbudili njihovo uporabo, bi morali javni organi v državah članicah razmisliti o vključitvi kvalificiranih potrdil za avtentikacijo spletišč na svoja spletišča.

„(33) Številne države članice so uvedle nacionalne zahteve za storitve, ki zagotavljajo varno in zaupanja vredno digitalno arhiviranje za omogočanje dolgoročne hrambe elektronskih podatkov in povezanih storitev zaupanja. Zaradi zagotavljanja pravne varnosti, zaupanja in usklajenosti med državami članicami bi bilo treba vzpostaviti pravni okvir za kvalificirane storitve elektronskega arhiviranja, ki bi temeljil na okviru drugih storitev zaupanja iz te uredbe. S tem okvirom bi ponudniki in uporabniki storitev zaupanja imeli na voljo učinkovit nabor orodij, ki bi vključeval funkcionalne zahteve za storitev elektronskega arhiviranja in jasne pravne učinke pri uporabi kvalificirane storitve elektronskega arhiviranja. Te določbe bi se morale uporabljati za elektronsko ustvarjene dokumente in dokumente v papirni obliki, ki so bili skenirani in digitalizirani. Te določbe bi morale po potrebi omogočati prenos shranjenih elektronskih podatkov na različne medije ali formate, da bi bili še naprej trajni in čitljivi tudi po izteku obdobja tehnološke veljavnosti ter bi čim bolj zmanjšali izgubo in spremembo podatkov. Kadar elektronski podatki, ki se digitalno arhivirajo, vsebujejo enega ali več kvalificiranih elektronskih podpisov ali kvalificiranih elektronskih žigov, bi se morali pri arhiviranju uporabljati postopki in tehnologije, s katerimi se njihova zanesljivost podaljša za obdobje hrambe takih podatkov, po možnosti z uporabo drugih kvalificiranih elektronskih storitev zaupanja, vzpostavljenih s to uredbo. Da bi se pri uporabi elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov ustvarili dokazi o hrambi, bi bilo treba uporabljati kvalificirane elektronske storitve zaupanja. Kolikor s to uredbo storitve elektronskega arhiviranja niso usklajene, lahko države članice v skladu s pravom Unije glede teh storitev ohranijo ali uvedejo nacionalne določbe, na primer posebne določbe, ki dovoljujejo nekatera odstopanja za storitve, ki so integrirane v neko organizacijo in se uporabljajo izključno za „notranje arhive“ te organizacije. V tej uredbi naj se ne bi razlikovalo med elektronsko ustvarjenimi in fizičnimi dokumenti, ki so bili digitalizirani.

(33a) Nacionalni arhivi in spominske ustanove so kot organizacije, katerih naloga je ohranjanje dokumentarne dediščine v javnem interesu, običajno pooblaščene za izvajanje svojih dejavnosti na podlagi nacionalne zakonodaje in niso nujno ponudniki storitev zaupanja v smislu te uredbe. Če te institucije takih storitev ne ponujajo, ta uredba ne posega v njihovo delovanje.

„(34) Elektronska evidenca je zaporedje elektronskih podatkovnih zapisov, ki zagotavlja njihovo celovitost in točnost njihovega kronološkega vrstnega reda. Namen elektronskih evidenc je vzpostaviti kronološko zaporedje podatkovnih zapisov, da se digitalna sredstva ne bi kopirala in prodajala več prejemnikom. Elektronske evidence se lahko na primer uporabljajo za digitalne zapise o lastništvu v svetovni trgovini, financiranje dobavne verige, pri digitalizaciji pravic intelektualne lastnine ali blagu, kot je električna energija. Skupaj z drugimi tehnologijami lahko prispevajo k rešitvam za učinkovitejše in transformativne javne storitve, kot so e-glasovanje, čezmejno sodelovanje carinskih organov, čezmejno sodelovanje akademskih ustanov ali evidentiranje lastništva nepremičnin v decentraliziranih zemljiških knjigah. Kvalificirane elektronske evidence ustvarjajo pravno domnevo o enoličnosti in točnosti kronološkega zaporedja in celovitosti podatkovnih zapisov v evidenci. Zaradi posebnih atributov elektronskih evidenc, tj. kronološkega zaporedja podatkovnih zapisov, se elektronske evidence razlikujejo od drugih storitev zaupanja, kot so elektronski časovni žigi in storitve elektronske priporočene dostave. Niti časovno žigosanje digitalnih dokumentov niti njihov prenos prek storitev elektronske priporočene dostave namreč brez dodatnih tehničnih ali organizacijskih ukrepov ne bi mogla zadostno preprečiti kopiranja istega digitalnega sredstva in njegove večkratne prodaje različnim strankam. Postopek ustvarjanja in posodabljanja elektronske evidence je odvisen od vrste uporabljene evidence (centralizirana ali distribuirana).

„(35) Za preprečitev razdrobljenosti notranjega trga bi bilo treba vzpostaviti vseevropski pravni okvir, ki bo omogočal čezmejno priznavanje storitev zaupanja za beleženje podatkov v kvalificiranih elektronskih evidencah. Ponudniki storitev zaupanja za elektronske evidence bi morali imeti nalogo, da določijo zaporedje beleženja podatkov v evidenci. Ta uredba ne posega v morebitne pravne obveznosti, ki jih morajo izpolnjevati uporabniki elektronskih evidenc v skladu s pravom Unije in nacionalnim pravom. Denimo, primeri uporabe, ki vključujejo obdelavo osebnih podatkov, bi morali biti skladni z Uredbo (EU) 2016/679. Primeri uporabe, ki vključujejo kriptosredstva, bi morali biti skladni z vsemi veljavnimi finančnimi pravili, med drugim tudi z direktivo o trgih finančnih instrumentov[9], direktivo o plačilnih storitvah[10], direktivo o elektronskem denarju[11] ter morebitno prihodnjo zakonodajo o trgih kriptosredstev in pravili o preprečevanju pranja denarja, ki bi jih bilo mogoče vključiti v uredbo o prenosu sredstev[12], ter bi se z njimi od ponudnikov storitev v zvezi s kriptosredstvi lahko zahtevalo, da preverjajo identiteto uporabnikov elektronskih evidenc, da bi izpolnili mednarodne standarde za preprečevanje pranja denarja.

---

9 Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES (UL L 173, 12.6.2014, str. 349–496).

10 Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES (UL L 337, 23.12.2015, str. 35–127).

11 Direktiva 2009/110/ES Evropskega parlamenta in Sveta z dne 16. septembra 2009 o začetku opravljanja in opravljanju dejavnosti ter nadzoru skrbnega in varnega poslovanja institucij za izdajo elektronskega denarja ter o spremembah direktiv 2005/60/ES in 2006/48/ES in razveljavitvi Direktive 2000/46/ES (UL L 267, 10.10.2009, str. 7–17).

12 Glej predlog Komisije z dne 20. julija 2021 za prenovitev Uredbe (EU) 2015/847 Evropskega parlamenta in Sveta z dne 20. maja 2015 o informacijah, ki spremljajo prenose sredstev, COM(2021) 422 final.

„(36) Da bi se izognili razdrobljenosti in oviram zaradi različnih standardov in tehničnih omejitev ter zagotovili usklajen postopek, s katerim bi preprečili ogrožanje izvajanja prihodnjega evropskega okvira za digitalno identiteto, je potreben postopek tesnega in strukturiranega sodelovanja med Komisijo, državami članicami in zasebnim sektorjem. Za dosego tega cilja bi morale države članice sodelovati v okviru, opredeljenem v Priporočilu Komisije XXX/XXXX [Nabor orodij za usklajen pristop k evropskemu okviru za digitalno identiteto][13], za opredelitev nabora orodij za evropski okvir za digitalno identiteto. Nabor orodij bi moral vključevati celovito tehnično arhitekturo, referenčni okvir, sklop skupnih standardov in tehnične reference ter sklop smernic in opisov najboljših praks, ki bi zajemali vsaj vse vidike funkcionalnosti in interoperabilnosti evropskih denarnic za digitalno identiteto, vključno z elektronskimi podpisi, ter kvalificirane storitve zaupanja za potrjevanje atributov, kot je določeno v tej uredbi. V tem okviru bi morale države članice tudi skleniti sporazum o skupnih elementih poslovnega modela in strukturi pristojbin za evropske denarnice za digitalno identiteto, da bi olajšale njihovo uvedbo, zlasti s strani malih in srednjih podjetij, v čezmejnem okviru. Vsebina nabora orodij bi se morala razvijati vzporedno z rezultati razprave in postopkom sprejetja evropskega okvira za digitalno identiteto.

(36a) Države članice bi morale določiti pravila o kaznih za kršitve, kot so neposredne ali posredne prakse, ki povzročajo zmedo glede tega, katere storitve zaupanje so nekvalificirane ali kvalificirane, ali zlorabo znaka zaupanja EU s strani nekvalificiranih ponudnikov storitev zaupanja. Znak zaupanja EU se ne bi smel uporabljati pod pogoji, ki neposredno ali posredno vzbujajo prepričanje, da so kakršne koli nekvalificirane storitve zaupanja, ki jih nudi ta ponudnik storitev, kvalificirane.

[13] [Vstaviti sklic po sprejetju].

(36b) Ta uredba bi morala zagotoviti usklajeno raven kakovosti, zaupanja in varnosti kvalificiranih storitev zaupanja, ne glede na kraj izvajanja dejavnosti. Zato bi bilo treba ponudniku kvalificiranih storitev zaupanja omogočiti, da svoje dejavnosti, povezane z zagotavljanjem kvalificiranih storitev zaupanja, odda v zunanje izvajanje zunaj Unije, če bi jamčil, da se lahko nadzorne dejavnosti in revizije izvajajo, kot če bi se te dejavnosti izvajale v Uniji. Če skladnosti z Uredbo ni mogoče v celoti zagotoviti, bi morali imeti nadzorni organi možnost, da sprejmejo sorazmerne in utemeljene ukrepe, vključno z odvzemom kvalificiranega statusa storitve zaupanja, ki se zagotavlja.

(36c) Da bi zagotovili pravno varnost glede veljavnosti naprednih elektronskih podpisov, ki temeljijo na kvalificiranih potrdilih, je bistveno določiti komponente naprednega elektronskega podpisa, ki temelji na kvalificiranih potrdilih, ki bi jih morala oceniti zanašajoča se stranka, ki potrjuje veljavnost zadevnega podpisa.

(36d) Ponudniki storitev zaupanja bi morali uporabljati kriptografske algoritme, ki odražajo trenutne dobre prakse in zaupanja vredno izvajanje teh algoritmov, da bi zagotovili varnost in zanesljivost svojih storitev zaupanja.

(36e) Ta uredba bi morala določati obveznost kvalificiranih ponudnikov storitev zaupanja, da preverijo identiteto fizične ali pravne osebe, kateri se izda kvalificirani certifikat, na podlagi različnih metod, usklajenih v EU. Takšna metoda lahko vključuje uporabo sredstev elektronske identifikacije, ki izpolnjujejo zahteve glede „srednje“ ravni zanesljivosti, v kombinaciji z dodatnimi usklajenimi postopki na daljavo, ki zagotavljajo identifikacijo osebe z visoko stopnjo zaupanja.

(36f) Izdajatelje evropskih denarnic za digitalno identiteto in izdajatelje priglašenih sredstev elektronske identifikacije, ki delujejo v okviru poslovne ali poklicne dejavnosti in uporabljajo jedrne platformne storitve, ki jih zagotavljajo vratarji za namene zagotavljanja blaga in storitev končnim uporabnikom ali med takim zagotavljanjem, bi bilo treba šteti za poslovne uporabnike v skladu s členom 2(21) Uredbe (EU) 2022/1925. Zato bi bilo treba od vratarjev zahtevati, da brezplačno zagotovijo učinkovito interoperabilnost z istimi funkcijami operacijskega sistema, strojne opreme ali programske opreme, ki so na voljo ali se uporabljajo pri zagotavljanju lastnih dopolnilnih in podpornih storitev in strojne opreme, ter dostop do njih za namene interoperabilnosti. To bi moralo izdajateljem evropskih denarnic za digitalno identiteto in izdajateljem priglašenih sredstev elektronske identifikacije omogočiti, da se prek vmesnikov ali podobnih rešitev tako učinkovito povežejo z zadevnimi funkcijami, kot se storitve ali strojna oprema vratarja.

(36g) Da bi bila ta uredba usklajena s trenutnim razvojem in da bi sledili praksam na notranjem trgu, bi bilo treba delegirane in izvedbene akte, ki jih sprejme Komisija, redno pregledovati in po potrebi posodabljati. Pri oceni potrebe po teh posodobitvah bi bilo treba upoštevati nove tehnologije, prakse, standarde ali tehnične specifikacije, ki se pojavijo na notranjem trgu.

„(37) Opravljeno je bilo posvetovanje z Evropskim nadzornikom za varstvo podatkov v skladu s členom 42(1) Uredbe (EU) 2018/1525 Evropskega parlamenta in Sveta[14].

„(38) Uredbo (EU) 910/2014 bi bilo zato treba ustrezno spremeniti –

[14] Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

SPREJELA NASLEDNJO UREDBO:

Člen 1

Uredba (EU) 910/2014 se spremeni:

„(1) člen 1 se nadomesti z naslednjim:

„Ta uredba je namenjena zagotovitvi pravilnega delovanja notranjega trga ter ustrezne ravni varnosti sredstev elektronske identifikacije in storitev zaupanja. V ta namen ta uredba:

(aa) določa pogoje, pod katerimi države članice zagotovijo in priznajo sredstva elektronske identifikacije fizičnih in pravnih oseb, ki so vključena v priglašeno shemo elektronske identifikacije druge države članice;

(ab) določa pogoje, pod katerimi države članice zagotavljajo in priznavajo evropske denarnice za digitalno identiteto;

(b) določa pravila za storitve zaupanja, zlasti za elektronske transakcije;

(c) določa pravni okvir za elektronske podpise, elektronske žige, elektronske časovne žige, elektronske dokumente, storitve elektronske priporočene dostave in storitve v zvezi s potrdili za avtentikacijo spletišč, elektronsko potrjevanje elektronskih podpisov, elektronskih žigov in njihovih potrdil, elektronsko potrjevanje potrdil za avtentikacijo spletišč, elektronsko hrambo elektronskih podpisov, elektronskih žigov in njihovih potrdil, elektronsko arhiviranje, elektronsko potrjevanje atributov, upravljanje naprav za ustvarjanje elektronskega podpisa in elektronskega žiga na daljavo ter elektronske evidence;“;

„(2) člen 2 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Ta uredba se uporablja za sheme elektronske identifikacije, ki jih priglasi država članica, za evropske denarnice za digitalno identiteto, ki jih zagotavljajo države članice, in za ponudnike storitev zaupanja s sedežem v Uniji.“;

(b) odstavek 3 se nadomesti z naslednjim:

„3. Ta uredba ne vpliva na nacionalno pravo ali pravo Unije, povezano s sklenitvijo in veljavnostjo pogodb ali drugimi pravnimi ali postopkovnimi obveznostmi glede obličnosti ali posebnimi sektorskimi zahtevami glede obličnosti.“;

„(3) člen 3 se spremeni:

(X) točka (1) se nadomesti z naslednjim:

„(1) ‚elektronska identifikacija‘ pomeni postopek uporabe identifikacijskih podatkov osebe v elektronski obliki, ki enolično predstavljajo bodisi fizično ali pravno osebo bodisi fizično osebo, ki zastopa fizično ali pravno osebo;“;

(a) točka (2) se nadomesti z naslednjim:

„(2) ‚sredstvo elektronske identifikacije‘ pomeni materialno in/ali nematerialno enoto, vključno z evropskimi denarnicami za digitalno identiteto, ki vsebuje identifikacijske podatke osebe in se uporablja za avtentikacijo pri spletnih storitvah ali, kjer je ustrezno, nespletnih storitvah;“;

(aa) točka (3) se nadomesti z naslednjim:

„(3) ‚identifikacijski podatki osebe‘ pomeni niz podatkov, izdanih v skladu s pravom Unije ali nacionalnim pravom in ki omogočajo, da se določi identiteta fizične ali pravne osebe ali fizične osebe, ki zastopa fizično ali pravno osebo;“;

(b) točka (4) se nadomesti z naslednjim:

„(4) ‚shema elektronske identifikacije‘ pomeni sistem za elektronsko identifikacijo, v okviru katerega se fizični ali pravni osebi ali fizični osebi, ki zastopa fizično ali pravno osebo, izdajo sredstva elektronske identifikacije;“;

(ba) točka (5) se nadomesti z naslednjim:

„(5) ‚avtentikacija‘ pomeni elektronski postopek, ki omogoča potrditev elektronske identifikacije fizične ali pravne osebe ali izvora in celovitosti podatkov v elektronski obliki;“;

(bb) vstavi se naslednja točka (5a):

„(5a) ‚uporabnik‘ pomeni fizično ali pravno osebo ali fizično osebo, ki zastopa fizično ali pravno osebo, in ki uporablja storitve zaupanja ali sredstva elektronske identifikacije, ki se zagotavljajo v skladu s to uredbo;“;

(c) točka (14) se nadomesti z naslednjim:

„(14) ‚potrdilo za elektronski podpis‘ pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe;“;

(d) točka (16) se nadomesti z naslednjim:

„(16) ‚storitev zaupanja‘ pomeni elektronsko storitev, ki se praviloma opravlja za plačilo in vključuje:

(a) izdajanje potrdil za elektronske podpise, potrdil za elektronske žige, potrdil za avtentikacijo spletišč ali potrdil za zagotavljanje drugih storitev zaupanja;

(aa) potrjevanje potrdil za elektronske podpise, potrdil za elektronske žige, potrdil za avtentikacijo spletišč ali potrdil za zagotavljanje drugih storitev zaupanja;

(b) ustvarjanje elektronskih podpisov ali elektronskih žigov;

(c) potrjevanje elektronskih podpisov ali elektronskih žigov;

(d) hrambo elektronskih podpisov, elektronskih žigov, potrdil za elektronske podpise ali potrdil za elektronske žige;

(e) upravljanje naprav za ustvarjanje kvalificiranega elektronskega podpisa na daljavo ali naprav za ustvarjanje kvalificiranega elektronskega žiga na daljavo;

(f) izdajanje elektronskih potrdil o atributih;

(fa) potrjevanje elektronskih potrdil o atributih;

(g) ustvarjanje elektronskih časovnih žigov;

(ga) potrjevanje elektronskih časovnih žigov;

(gb) zagotavljanje storitev elektronske priporočene dostave;

(gc) potrjevanje podatkov, poslanih prek storitev elektronske priporočene dostave, in s tem povezanih dokazov;

(h) elektronsko arhiviranje elektronskih podatkov ali

(i) beleženje elektronskih podatkov v elektronskih evidencah;“;

(da) točka (18) se nadomesti z naslednjim:

„(18) ‚organ za ugotavljanje skladnosti‘ pomeni organ, opredeljen v točki 13 člena 2 Uredbe (ES) št. 765/2008, ki je akreditiran v skladu z navedeno uredbo in je pristojen za ugotavljanje skladnosti ponudnika kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja, ki jih ta zagotavlja, ali za certificiranje evropskih denarnic za digitalno identiteto ali sredstev elektronske identifikacije;“;

(e) točka (21) se nadomesti z naslednjim:

„(21) ‚izdelek‘ pomeni strojno ali programsko opremo ali ustrezne sestavne dele strojne in/ali programske opreme, katerih uporaba je namenjena zagotavljanju storitev elektronske identifikacije in storitev zaupanja;“;

(f) vstavita se naslednji točki (23a) in (23b):

„(23a) ‚naprava za ustvarjanje kvalificiranega elektronskega podpisa na daljavo‘ pomeni napravo za ustvarjanje kvalificiranega elektronskega podpisa, ki jo v imenu podpisnika upravlja ponudnik kvalificiranih storitev zaupanja v skladu s členom 29a;

(23b) ‚naprava za ustvarjanje kvalificiranega elektronskega žiga na daljavo‘ pomeni napravo za ustvarjanje kvalificiranega elektronskega žiga, ki jo v imenu ustvarjalca žiga upravlja ponudnik kvalificiranih storitev zaupanja v skladu s členom 39a;“;

(g) točka (29) se nadomesti z naslednjim:

„(29) ‚potrdilo za elektronski žig‘ pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega žiga s pravno osebo in potrjuje ime te osebe;“;

(h) točka (41) se nadomesti z naslednjim:

„(41) ‚potrjevanje veljavnosti‘ pomeni postopek preverjanja in potrditve, da so podatki v elektronski obliki veljavni v skladu z zahtevami iz te uredbe;“;

(i) dodajo se naslednje točke od (42) do (55c):

„(42) ‚evropska denarnica za digitalno identiteto‘ je sredstvo elektronske identifikacije, ki uporabniku omogoča shranjevanje in dostop do podatkov o identiteti, vključno z identifikacijskimi podatki osebe, elektronskih potrdil o atributih, povezanih z njegovo identiteto, njihovo predložitev zanašajočim se strankam na zahtevo ter njihovo uporabo za spletno in, kjer je ustrezno, nespletno avtentikacijo za storitev v skladu s členom 6a, ter omogoča podpis s kvalificiranim elektronskim podpisom in žigosanje s kvalificiranim elektronskim žigom;

„(43) ‚atribut‘ predstavlja značilnost, naravo, pravico ali dovoljenje fizične ali pravne osebe ali predmeta;

„(44) ‚elektronsko potrdilo o atributih‘ pomeni potrdilo v elektronski obliki, ki omogoča avtentikacijo atributov;

„(45) ‚kvalificirano elektronsko potrdilo o atributih‘ pomeni elektronsko potrdilo o atributih, ki ga je izdal ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge V;

(45a) ‚elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir‘ pomeni elektronska potrdila o atributih, izdana s strani organa javnega sektorja, pristojnega za verodostojni vir, ali s strani organa javnega sektorja, ki ga država članica imenuje za izdajanje takih potrdil o atributih v imenu organov javnega sektorja, pristojnih za verodostojne vire v skladu s členom 45da in ki izpolnjujejo zahteve iz Priloge VII;

„(46) ‚verodostojni vir‘ je odložišče ali sistem v pristojnosti organa javnega sektorja ali zasebnega subjekta, ki vsebuje in zagotavlja atribute o fizični ali pravni osebi in se šteje za primarni vir takih informacij ali je priznan kot verodostojen v skladu s pravom Unije ali nacionalnim pravom, vključno z upravno prakso;

„(47) ‚elektronsko arhiviranje‘ pomeni storitev zagotavljanja prejema, hrambe, dostopanja do in brisanja elektronskih podatkov za zagotavljanje njihove trajnosti in berljivosti ter ohranjanje njihove celovitosti, zaupnosti in dokazila o poreklu v celotnem obdobju hrambe;

„(48) ‚kvalificirana storitev elektronskega arhiviranja‘ pomeni storitev elektronskega arhiviranja, ki izpolnjuje zahteve iz člena 45ga;

„(49) ‚znak zaupanja za evropsko denarnico za digitalno identiteto‘ pomeni preverljivo, enostavno, prepoznavno in jasno označbo, da je bila evropska denarnica za digitalno identiteto zagotovljena v skladu s to uredbo;

„(50) ‚močna avtentikacija uporabnika‘ pomeni avtentikacijo, ki temelji na uporabi najmanj dveh dejavnikov avtentikacije iz različnih kategorij, in sicer kategorije znanja (nekaj, kar ve samo uporabnik), imetja (nekaj, kar je v izključni lasti uporabnika) ali inherence (nekaj, kar uporabnik je), ki so neodvisni, tako da kršitev enega dejavnika ne zmanjšuje zanesljivosti drugih, ter je zasnovana tako, da varuje zaupnost avtentikacijskih podatkov;

„(53) ‚elektronska evidenca‘ pomeni zaporedje elektronskih podatkovnih zapisov, ki zagotavlja njihovo celovitost in točnost njihovega kronološkega vrstnega reda;

(53a) ‚kvalificirana elektronska evidenca‘ pomeni elektronsko evidenco, ki izpolnjuje zahteve iz člena 45i;

„(54) ‚osebni podatki‘ pomenijo vse informacije, kot so opredeljene v točki 1 člena 4 Uredbe (EU) 2016/679;

„(55) ‚usklajevanje evidenc‘ pomeni postopek, v katerem se identifikacijski podatki osebe, sredstva za identifikacijo osebe, kvalificirano elektronsko potrdilo o atributih ali potrdila o atributih, izdana s strani organa javnega sektorja, pristojnega za verodostojni vir, primerjajo ali povežejo z obstoječim računom, ki pripada isti osebi;

(55a) ‚enolični in stalni identifikator‘ pomeni identifikator, ki je lahko sestavljen iz enega ali več nacionalnih ali sektorskih identifikacijskih podatkov, je povezan z enim samim uporabnikom v danem sistemu in je trajen v času;

(55b) ‚podatkovni zapis‘ pomeni elektronske podatke, zabeležene s povezanimi metapodatki (ali atributi), ki podpirajo obdelavo podatkov;

(55c) ‚nespletna uporaba evropskih denarnic za digitalno identiteto‘ pomeni interakcijo med uporabnikom in zanašajočo se stranko na fizični lokaciji, pri čemer za denarnico za namene interakcije ni potreben dostop do sistemov na daljavo prek elektronskih komunikacijskih omrežij;“;

„*Člen 5*

Psevdonimi v elektronski transakciji

Brez poseganja v pravni učinek psevdonimov v skladu z nacionalnim pravom, uporaba psevdonimov v elektronskih transakcijah ni prepovedana.“;

„(5) v poglavju II se pred členom 6a vstavi naslednji naslov:

„ODDELEK I

Evropska denarnica za digitalno identiteto“;

„(7) vstavijo se naslednji členi 6a, 6b, 6c in 6d:

„Člen 6a

Evropske denarnice za digitalno identiteto

„1. Za zagotovitev, da imajo vse fizične in pravne osebe v Uniji varen, zaupanja vreden in nemoten čezmejni dostop do javnih in zasebnih storitev, vsaka država članica v 24 mesecih po začetku veljavnosti izvedbenih aktov iz odstavka 11 in člena 6c(4) zagotovi evropsko denarnico za digitalno identiteto.

„2. Evropske denarnice za digitalno identiteto se zagotovijo:

(a) s strani države članice;

(b) na podlagi pooblastila države članice ali

(c) neodvisno od države članice, vendar s priznanjem države članice.

„3. Evropske denarnice za digitalno identiteto so sredstvo elektronske identifikacije, ki uporabniku na pregleden in sledljiv način omogoča, da:

(a) varno zahteva, izbira, združuje, hrani in briše ter zanašajočim se stranem predloži elektronsko potrdilo o atributih in identifikacijske osebne podatke, tudi za spletno in, kjer je ustrezno, nespletno avtentikacijo, za uporabo javnih in zasebnih storitev, pri čemer omogoča selektivno razkritje podatkov;

(b) se podpiše s kvalificiranim elektronskim podpisom in žigosa s kvalificiranim elektronskim žigom.

„4. Evropske denarnice za digitalno identiteto zlasti:

(a) zagotavljajo skupen sklop vmesnikov:

„(1) za izdajo identifikacijskih podatkov osebe, kvalificiranih in nekvalificiranih elektronskih potrdil o atributih ali kvalificiranih in nekvalificiranih potrdil za evropsko denarnico za digitalno identiteto;

„(2) za zanašajoče se stranke, da lahko zahtevajo identifikacijske podatke osebe in elektronska potrdila o atributih;

„(3) za predstavitev identifikacijskih podatkov osebe ali elektronskega potrdila o atributih zanašajočim se strankam na spletu in, kjer je to ustrezno, tudi zunaj spleta;

„(4) za uporabnika, da se mu omogočita interakcija z evropsko denarnico za digitalno identiteto in prikaz ‚znaka zaupanja za evropsko denarnico za digitalno identiteto‘;

(b) ponudnikom storitev zaupanja, ki ponujajo elektronska potrdila o atributih, ne zagotavljajo nobenih informacij o uporabi teh atributov po njihovi izdaji;

(ba) zagotavljajo, da se lahko identiteta zanašajočih se strank potrdi z izvajanjem mehanizmov avtentikacije v skladu s členom 6b;

(c) izpolnjujejo zahteve iz člena 8 glede zagotavljanja ‚visoke‘ ravni zanesljivosti, ki se smiselno uporablja za upravljanje in uporabo identifikacijskih podatkov osebe prek denarnice, vključno z elektronsko identifikacijo in avtentikacijo;

(e) zagotavljajo, da identifikacijski podatki osebe iz člena 12(4), točka (d), enolično in stalno predstavljajo fizično osebo, pravno osebo ali fizično osebo, ki zastopa fizično ali pravno osebo, ki je povezana z denarnico.

4a. Države članice določijo postopke, ki uporabniku omogočajo, da prijavi morebitno izgubo ali zlorabo svoje denarnice in zahteva njen preklic.

„5. Države članice zagotovijo mehanizme potrjevanja za evropske denarnice za digitalno identiteto:

(a) da zagotovijo možnost preverjanja njihove avtentičnosti in veljavnosti;

(d) da uporabniku omogočijo avtentikacijo zanašajočih se strank v skladu s členom 6b.

„6. Evropske denarnice za digitalno identiteto se izdajajo v okviru priglašene sheme elektronske identifikacije z ‚visoko' ravnjo zanesljivosti.

6a. Izdaja, uporaba za avtentikacijo in preklic evropskih denarnic za digitalno identiteto so za fizične osebe brezplačni.

6b. Brez poseganja v člen 6db lahko države članice v skladu z nacionalnim pravom določijo dodatne funkcije evropskih denarnic za digitalno identiteto, vključno z interoperabilnostjo z obstoječimi nacionalnimi sredstvi elektronske identifikacije.

„7. Uporabniki imajo popoln nadzor nad uporabo evropske denarnice za digitalno identiteto in podatkov v svoji evropski denarnici za digitalno identiteto. Izdajatelj evropske denarnice za digitalno identiteto ne zbira informacij o uporabi denarnice, ki niso potrebne za zagotavljanje storitev denarnice, niti ne združuje identifikacijskih podatkov osebe in kakršnih koli drugih osebnih podatkov, ki se hranijo ali so povezani z uporabo evropske denarnice za digitalno identiteto, z osebnimi podatki iz katerih koli drugih storitev, ki jih ponuja ta izdajatelj, ali iz storitev tretjih oseb, ki niso potrebni za zagotavljanje storitev denarnice, razen če uporabnik tega izrecno ne zahteva. Osebni podatki v zvezi z zagotavljanjem evropskih denarnic za digitalno identiteto se hranijo logično ločeni od vseh drugih podatkov, ki jih hrani izdajatelj evropskih denarnic za digitalno identiteto. Če evropsko denarnico za digitalno identiteto zagotavljajo zasebne stranke v skladu z odstavkom 2(b) in (c), se smiselno uporabljajo določbe člena 45f, odstavek 4.

7a. Države članice brez nepotrebnega odlašanja Komisiji priglasijo informacije o:

(a) organu, odgovornem za vzpostavitev in vzdrževanje seznama priglašenih zanašajočih se strank, ki se zanašajo na evropske denarnice za digitalno identiteto v skladu s členom 6b(2);

(b) organih, odgovornih za zagotavljanje evropskih denarnic za digitalno identiteto v skladu s členom 6a(1);

(c) organih, odgovornih za zagotavljanje, da so osebni identifikacijski podatki povezani z denarnico v skladu s členom 6a(4)(e).

V priglasitvi se navedejo tudi informacije o mehanizmu, ki omogoča potrditev veljavnosti identifikacijskih podatkov osebe iz člena 12(4) in identitete zanašajočih se strank.

Komisija na varen način in v elektronsko podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo, da informacije iz tega odstavka na voljo javnosti.

„8. Za evropsko denarnico za digitalno identiteto se smiselno uporablja člen 11.

„9. Za izdajatelja evropskih denarnic za digitalno identiteto se smiselno uporablja člen 24(2), točke (b), (e), (g) in (h).

„10. Evropska denarnica za digitalno identiteto je v skladu z zahtevami glede dostopnosti iz Direktive 2019/882 dostopna invalidom.

„11. Komisija v šestih mesecih po začetku veljavnosti te uredbe z izvedbenim aktom o uvedbi evropske denarnice za digitalno identiteto določi tehnične in operativne specifikacije ter referenčne standarde za zahteve iz odstavkov 3, 4, 5 in 7a. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 48(2).

11a. Komisija določi tehnične in operativne specifikacije ter referenčne standarde, da bi uporabnikom olajšala vstop v evropsko denarnico za digitalno identiteto z uporabo bodisi sredstev elektronske identifikacije, ki ustrezajo ‚visoki' ravni, bodisi sredstev elektronske identifikacije, ki ustrezajo ‚znatni' ravni, v povezavi z dodatnimi postopki daljinskega vstopa, ki skupaj izpolnjujejo zahteve glede ‚visoke' ravni zanesljivosti. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 48(2).

Člen 6b

Stranke, ki se zanašajo na evropske denarnice za digitalno identiteto

1. Kadar se zanašajoče se stranke, ki zagotavljajo zasebne ali javne storitve, nameravajo zanašati na evropske denarnice za digitalno identiteto, zagotovljene v skladu s to uredbo, to priglasijo državi članici, v kateri imajo zanašajoče se stranke sedež.

1a. Postopek priglasitve je stroškovno učinkovit in sorazmeren s tveganjem ter zagotavlja, da zanašajoče se stranke zagotovijo vsaj informacije, potrebne za avtentikacijo v evropske denarnice za digitalno identiteto. To bi moralo vključevati vsaj državo članico, v kateri imajo sedež, in ime zanašajoče se stranke ter, kjer je to ustrezno, njeno registrsko številko, kot je navedena v uradnih evidencah.

1b. Obveznost priglasitve ne posega v druge zahteve glede priglasitve in registracije v skladu s pravom Unije ali nacionalnim pravom, kot so tiste, ki se uporabljajo za posebne kategorije osebnih podatkov, za katere se lahko zahtevajo dodatne zahteve glede pridobitve dovoljenja.

1c. Države članice lahko zanašajoče se stranke izvzamejo iz obveznosti priglasitve, kadar pravo Unije ali nacionalno pravo ne določa posebnih zahtev glede priglasitve ali registracije za dostop do informacij, zagotovljenih prek evropske denarnice za digitalno identiteto. Izvzetim zanašajočim se strankam se morda ni treba avtentificirati v evropske denarnice za digitalno identiteto.

1d. Zanašajoče se stranke, ki pošljejo priglasitev v skladu s tem členom, nemudoma obvestijo državo članico o vseh naknadnih spremembah prvotno zagotovljenih informacij.

„2. Zanašajoče se stranke zagotovijo izvajanje mehanizmov avtentikacije iz člena 6a(4)(ba).

„3. Zanašajoče se stranke so odgovorne za izvajanje postopka avtentikacije oseb in potrditve veljavnosti elektronskih potrdil o atributih, ki izvirajo iz evropskih denarnic za digitalno identiteto, pridobljenih prek skupnega vmesnika v skladu s členom 6a(4)(a)(2).

„4. Komisija v šestih mesecih po začetku veljavnosti te uredbe z izvedbenim aktom o uvedbi evropskih denarnic za digitalno identiteto iz člena 6a(11) določi tehnične in operativne specifikacije za zahteve iz odstavkov 1, 1a in 1d. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 48(2).

Člen 6c

Certificiranje evropskih denarnic za digitalno identiteto

„1. Skladnost evropskih denarnic za digitalno identiteto z zahtevami iz člena 6a(3), (4) in (5), zahtevo po logični ločitvi iz člena 6a(7) in, kjer je to ustrezno, zahtevami iz člena 6a(11a) potrdijo organi za ugotavljanje skladnosti, ki so akreditirani v skladu s členom 60 Akta o kibernetski varnosti ter s shemami, specifikacijami, standardi in postopki, na katere se sklicujejo v skladu z odstavkom 4, točke (a), (aa) in (aaa), ter ki jih imenujejo države članice. Veljavnost certificiranja ne presega petih let, odvisno od ocene ranljivosti, ki se izvaja redno vsaki dve leti. Kadar so ranljivosti ugotovljene, vendar niso odpravljene v treh mesecih, se certificiranje prekliče.

„2. Kar zadeva skladnost z zahtevami glede varstva podatkov na podlagi člena 6a(7), se lahko certificiranje iz odstavka 1 dopolni s certificiranjem v skladu s členom 42 Uredbe (EU) 2016/679.

„3. Skladnost evropskih denarnic za digitalno identiteto ali njihovih delov z ustreznimi zahtevami za kibernetsko varnost iz člena 6a(3), (4), (5), (7) in, kjer je to ustrezno, (11a) potrdijo organi za ugotavljanje skladnosti iz odstavka 1 v okviru ustreznih certifikacijskih shem za kibernetsko varnost v skladu z Uredbo (EU) 2019/881, kot so navedene v skladu z odstavkoma 4(a) in 4(aa).

3a. Za certificirane evropske denarnice za digitalno identiteto ne veljajo zahteve iz členov 7 in 9.

„4. Komisija v šestih mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi:

(a) seznam certifikacijskih shem za kibernetsko varnost v skladu z Uredbo (EU) 2019/881, ki se zahtevajo za certificiranje evropskih denarnic za digitalno identiteto iz odstavka 3;

(aa) specifikacije, postopke in referenčne standarde za njihovo uporabo v okviru ustreznih certifikacijskih shem za kibernetsko varnost, navedenih v skladu s točko (a);

(aaa) seznam specifikacij, postopkov in referenčnih standardov, ki določajo skupne zahteve za certificiranje, ki jih ustrezne certifikacijske sheme za kibernetsko varnost v skladu z Uredbo (EU) 2019/881 ne zajemajo za namene certificiranja iz odstavka 1, in katerih namen je dokazati, da evropska denarnica za digitalno identiteto izpolnjuje zahteve iz odstavka 1;

(b) tehnične, postopkovne, organizacijske in operativne specifikacije za imenovanje organov za ugotavljanje skladnosti iz odstavka 1 ter, kar zadeva zahteve za certificiranje, določene v skladu s točko (aaa), za spremljanje in pregled certifikacijskih shem in povezanih metod ocenjevanja, ki jih ti organi uporabljajo, ter certifikatov in poročil o certificiranju, ki jih izdajo.

„5. Države članice Komisiji sporočijo imena in naslove javnih ali zasebnih organov iz odstavka 1. Komisija poskrbi, da so te informacije na voljo državam članicam.

„6. Izvedbeni akti iz odstavka 4 se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 6d

Objava seznama certificiranih evropskih denarnic za digitalno identiteto

„1. Države članice brez nepotrebnega odlašanja obvestijo Komisijo o evropskih denarnicah za digitalno identiteto, ki so bile zagotovljene v skladu s členom 6a in so jih certificirali organi iz člena 6c, odstavek 1. Komisijo brez nepotrebnega odlašanja obvestijo tudi, kadar je certificiranje preklicano.

„2. Komisija na podlagi prejetih informacij pripravi, objavi in posodablja strojno berljiv seznam certificiranih evropskih denarnic za digitalno identiteto.

„3. Komisija v šestih mesecih po začetku veljavnosti te uredbe z izvedbenim aktom o uvedbi evropskih denarnic za digitalno identiteto iz člena 6a(11) opredeli oblike in postopke, ki se uporabljajo za namene odstavkov 1 in 2. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 48(2).

Člen 6da

Kršitev varnosti evropskih denarnic za digitalno identiteto

„1. Ob kršitvi ali delnem ogrožanju evropskih denarnic za digitalno identiteto, zagotovljenih v skladu s členom 6a ali mehanizmi potrjevanja veljavnosti iz člena 6a(5), točke (a), (d) ali (e), na način, ki vpliva na njihovo zanesljivost ali zanesljivost drugih evropskih denarnic za digitalno identiteto, izdajatelj zadevnih denarnic brez nepotrebnega odlašanja začasno razveljavi izdajo in uporabo evropske denarnice za digitalno identiteto. Država članica, v kateri so bile zagotovljene zadevne denarnice, o tem brez nepotrebnega odlašanja obvesti države članice in Komisijo. Izdajatelj zadevnih denarnic ali država članica ustrezno obvesti zanašajoče se stranke in uporabnike.

„2. Kadar je kršitev ali ogrožanje iz odstavka 1 odpravljeno, izdajatelj denarnice ponovno vzpostavi izdajo in uporabo evropske denarnice za digitalno identiteto. Država članica, v kateri so bile zagotovljene zadevne denarnice, o tem brez nepotrebnega odlašanja obvesti države članice in Komisijo. Izdajatelj zadevnih denarnic ali država članica brez nepotrebnega odlašanja obvesti zanašajoče se stranke in uporabnike.

„3. Če se kršitev ali ogrožanje iz odstavka 1 ne odpravi v treh mesecih po začasni razveljavitvi, zadevna država članica umakne zadevno evropsko denarnico za digitalno identiteto ter ustrezno obvesti druge države članice in Komisijo. Kadar je to upravičeno z resnostjo kršitve, se evropska denarnica za digitalno identiteto brez nepotrebnega odlašanja umakne.

„4. Komisija v Uradnem listu Evropske unije objavi ustrezne spremembe seznama iz člena 6d brez nepotrebnega odlašanja.

„5. Komisija v šestih mesecih po začetku veljavnosti te uredbe z izvedbenim aktom o uvedbi evropskih denarnic za digitalno identiteto iz člena 6a(11) natančneje opredeli ukrepe iz odstavkov 1, 2 in 3. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 48(2).

Člen 6db

Čezmejna uporaba evropskih denarnic za digitalno identiteto

„1. Države članice, ki za dostop do spletne storitve organa javnega sektorja zahtevajo elektronsko identifikacijo s sredstvi elektronske identifikacije in avtentikacijo, prav tako sprejmejo evropske denarnice za digitalno identiteto, zagotovljene v skladu s to uredbo, za avtentikacijo uporabnika.

„2. Kadar nacionalno pravo ali pravo Unije od zasebnih zanašajočih se strank, ki zagotavljajo storitve, z izjemo mikro in malih podjetij, kot so opredeljena v Priporočilu Komisije 2003/361/ES, zahteva uporabo močne avtentikacije uporabnika za spletno identifikacijo ali kadar se močna avtentikacija uporabnika zahteva na podlagi pogodbenih obveznosti, med drugim na področjih prometnih, energetskih, bančnih in finančnih storitev, socialnega varstva, zdravja, pitne vode, poštnih storitev, digitalne infrastrukture, izobraževanja ali telekomunikacij, zasebne zanašajoče se stranke najpozneje 12 mesecev po datumu zagotovitve evropskih denarnic za digitalno identiteto v skladu s členom 6a(1) in strogo na podlagi prostovoljne zahteve uporabnika sprejmejo tudi uporabo evropskih denarnic za digitalno identiteto, zagotovljenih v skladu s to uredbo, v zvezi z minimalnimi podatki, potrebnimi za posamezno spletno storitev, za katero se zahteva avtentikacija uporabnika.

„3. Kadar zelo velike spletne platforme, opredeljene v členu 25(1) uredbe [sklic na uredbo, tj. akt o digitalnih storitvah], od uporabnikov zahtevajo avtentikacijo za dostop do spletnih storitev, sprejmejo tudi uporabo evropskih denarnic za digitalno identiteto, zagotovljenih v skladu s to uredbo, za avtentikacijo uporabnika, in sicer strogo na podlagi prostovoljne zahteve uporabnika in ob upoštevanju minimalnih podatkov, potrebnih za določeno spletno storitev, za katero se zahteva avtentikacija.

„4. Komisija v sodelovanju z državami članicami spodbuja in lajša razvoj kodeksov ravnanja, da bi prispevala k širši razpoložljivosti in uporabnosti evropskih denarnic za digitalno identiteto v okviru področja uporabe te uredbe. S temi kodeksi ravnanja se olajša sprejetje sredstev elektronske identifikacije, vključno z evropskimi denarnicami za digitalno identiteto v okviru področja uporabe te uredbe, zlasti pri ponudnikih storitev, ki avtentikacijo uporabnikov opravljajo prek storitev elektronske identifikacije tretjih oseb. Komisija bo lajšala razvoj takih kodeksov ravnanja v tesnem sodelovanju z vsemi zadevnimi deležniki in spodbujala ponudnike storitev, da dokončajo njihovo pripravo in jih dejansko začnejo izvajati v 12 oziroma 18 mesecih po sprejetju te uredbe.

„5. Komisija bo v 24 mesecih po uvedbi evropskih denarnic za digitalno identiteto ocenila, ali bodo na podlagi dokazov o povpraševanju po evropski denarnici za digitalno identiteto ter njeni razpoložljivosti in uporabnosti k sprejetju njene uporabe strogo na podlagi prostovoljne zahteve uporabnika obvezani tudi dodatni zasebni ponudniki spletnih storitev. Merila za oceno vključujejo obseg baze uporabnikov, čezmejno prisotnost ponudnikov storitev, tehnološki razvoj, razvoj vzorcev uporabe in povpraševanje potrošnikov.“;

„(8) pred členom 7 se vstavi naslednji naslov:

„ODDELEK II

SHEME ELEKTRONSKE IDENTIFIKACIJE“;

„(9) uvodni stavek v členu 7 se nadomesti z naslednjim:

„V skladu s členom 9(1) države članice, ki tega še niso storile, v 24 mesecih po začetku veljavnosti izvedbenih aktov iz člena 6a(11) in člena 6c(4) priglasijo vsaj eno shemo elektronske identifikacije, ki vključuje vsaj eno identifikacijsko sredstvo ‚visoke‘ ravni zanesljivosti‘. Shema elektronske identifikacije je upravičena do priglasitve v skladu s členom 9(1), če so izpolnjeni vsi naslednji pogoji:“;

„(10) v členu 9 se odstavka 2 in 3 nadomestita z naslednjim:

„2. Komisija v Uradnem listu Evropske unije objavi seznam shem elektronske identifikacije, priglašenih v skladu z odstavkom 1 tega člena, in osnovne informacije o njih.

„3. Komisija seznam iz odstavka 2 objavi v Uradnem listu Evropske unije v enem mesecu od datuma prejema zadevne priglasitve.“;

„(12) vstavi se naslednji člen 11a:

„*Člen 11a*

Usklajevanje evidenc

„1. Če se priglašena sredstva elektronske identifikacije in evropske denarnice za digitalno identiteto uporabljajo za avtentikacijo, države članice, ko delujejo kot zanašajoče se stranke, zagotovijo usklajevanje evidenc.

„2. Države članice za namene zagotavljanja evropskih denarnic za digitalno identiteto v minimalni niz identifikacijskih podatkov osebe iz člena 12(4), točka (d), v skladu s pravom Unije in nacionalnim pravom vključijo vsaj en enolični in stalni identifikator za identifikacijo uporabnika na njegovo zahtevo v primerih, kadar se identifikacija uporabnika zahteva z zakonom.

2a. Države članice določijo tehnične in organizacijske ukrepe za zagotovitev visoke ravni varstva osebnih podatkov, ki se uporabljajo za usklajevanje evidenc, in za preprečevanje oblikovanja profilov uporabnikov.

2aa. Države članice lahko v skladu z nacionalnim pravom določijo, da lahko uporabnik evropske denarnice za digitalno identiteto zahteva, da se enolični in stalni identifikator, vključen v minimalni niz identifikacijskih podatkov osebe in povezan z denarnico v skladu s členom 6a(4)(e), nadomesti z drugim enoličnim in stalnim identifikatorjem, ki ga izda država članica.

„3. Komisija v šestih mesecih po začetku veljavnosti te uredbe z izvedbenim aktom natančneje opredeli ukrepe iz odstavka 1. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 48(2).

3a. Komisija v šestih mesecih po začetku veljavnosti te uredbe z izvedbenim aktom natančneje opredeli ukrepe iz odstavkov 2 in 2aa. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 48(2).“;

„(13) člen 12 se spremeni:

Sodelovanje in interoperabilnost

(a) v odstavku 3 se črta točka (d);

(b) v odstavku 4 se točka (d) nadomesti z naslednjim:

„(d) sklicevanje na minimalni niz identifikacijskih podatkov osebe, ki so potrebni za enolično in stalno predstavljanje fizične osebe, pravne osebe ali fizične osebe, ki predstavlja fizično ali pravno osebo;“;

(ba) v odstavku 5 se vstavi točka (c):

„(c) podoben pristop k spletnim storitvam, ki sprejemajo uporabo evropskih denarnic za digitalno identiteto, zagotovljenih v skladu s to uredbo;“;

(c) v odstavku 6 se točka (a) nadomesti z naslednjim:

„(a) izmenjavo informacij, izkušenj in dobrih praks v zvezi s shemami elektronske identifikacije in zlasti tehničnimi zahtevami, povezanimi z interoperabilnostjo, usklajevanjem evidenc in ravnmi zanesljivosti;“;

(ca) v odstavku 6 se vstavi točka (e):

„(e) izmenjavo informacij, izkušenj in dobrih praks ter izdajo smernic o tem, kako se lahko spletne storitve zasnujejo, razvijajo in izvajajo za namene zanašanja na evropske denarnice za digitalno identiteto.“;

„(14) vstavita se naslednja člena 12a in 12b:

„Člen 12a

Certificiranje shem elektronske identifikacije

1. Skladnost shem elektronske identifikacije, ki jih je treba priglasiti, z zahtevami iz te uredbe se certificira, da se dokaže skladnost takih shem ali njihovih delov z zahtevami iz člena 8(2) glede ravni zanesljivosti shem elektronske identifikacije v okviru ustrezne certifikacijske sheme za kibernetsko varnost v skladu z Uredbo (EU) 2019/881 ali njenih delov, kolikor potrdilo o kibernetski varnosti ali njegovi deli zajemajo zahteve iz člena 8(2) glede ravni zanesljivosti shem elektronske identifikacije. Certifikacija se ne opravi za več kot pet let, odvisno od ocene ranljivosti, ki se izvaja redno vsaki dve leti. Kadar so ranljivosti ugotovljene, vendar niso odpravljene v treh mesecih, se certifikacija prekliče.

   Certificiranje izvajajo akreditirani javni ali zasebni organi za ugotavljanje skladnosti, ki jih imenujejo države članice, v skladu z Uredbo (ES) št. 765/2008.

„2. Medsebojni strokovni pregledi shem elektronske identifikacije iz člena 12(6), točka (c), se ne uporabljajo za sheme elektronske identifikacije ali dele takih shem, certificiranih v skladu z odstavkom 1.

2a. Ne glede na odstavek 2 tega člena lahko države članice od države članice priglasiteljice zahtevajo dodatne informacije o shemah elektronske identifikacije ali delih takih shem, certificiranih v skladu z odstavkom 2 tega člena.

„3. Države članice Komisijo uradno obvestijo o imenih in naslovih javnega ali zasebnega organa iz odstavka 1. Komisija poskrbi, da so te informacije na voljo državam članicam.“;

„Člen 12b

Dostop do funkcij strojne in programske opreme

Izdajatelji evropskih denarnic za digitalno identiteto in izdajatelji priglašenih sredstev elektronske identifikacije, ki delujejo v okviru poslovne ali poklicne dejavnosti in uporabljajo jedrne platformne storitve, kot so opredeljene v členu 2(2) Uredbe (EU) 2022/1925, za namene zagotavljanja storitev evropske denarnice za digitalno identiteto in sredstev elektronske identifikacije končnim uporabnikom ali med takim zagotavljanjem, so poslovni uporabniki v skladu s členom 2(21) Uredbe (EU) 2022/1925.“;

„(17) v členu 13 se odstavek 1 nadomesti z naslednjim:

„1. Ne glede na odstavek 2 tega člena so ponudniki storitev zaupanja odgovorni za škodo, ki je namenoma ali malomarno povzročena fizični ali pravni osebi zaradi neizpolnjevanja obveznosti iz te uredbe.

Dokazno breme o namenu (naklepu) ali malomarnosti ponudnika nekvalificiranih storitev zaupanja nosi fizična ali pravna oseba, ki zatrjuje škodo iz prvega pododstavka.

Domneva se, da je ponudnik kvalificiranih storitev zaupanja škodo povzročil namenoma ali iz malomarnosti, razen če dokaže, da škode iz prvega pododstavka ni povzročil namenoma ali iz malomarnosti.“;

„(18) člen 14 se nadomesti z naslednjim:

„*Člen 14*

Mednarodni vidiki

1. Storitve zaupanja, ki jih zagotavljajo ponudniki storitev zaupanja s sedežem v tretji državi ali mednarodna organizacija, so pravno enakovredne kvalificiranim storitvam zaupanja, ki jih zagotavljajo ponudniki kvalificiranih storitev zaupanja s sedežem v Uniji, kadar se storitve zaupanja iz tretje države ali mednarodne organizacije priznajo na podlagi izvedbenega sklepa ali sporazuma, sklenjenega med Unijo in tretjo državo ali mednarodno organizacijo v skladu s členom 218 Pogodbe.

2. Z izvedbenimi sklepi in sporazumi iz odstavka 1 se zagotovi, da ponudniki storitev zaupanja v tretji državi ali mednarodne organizacije in storitve zaupanja, ki jih zagotavljajo, izpolnjujejo zahteve, ki veljajo za ponudnike kvalificiranih storitev zaupanja s sedežem v Uniji in za kvalificirane storitve zaupanja, ki jih zagotavljajo. Tretje države in mednarodne organizacije zlasti vzpostavijo, vodijo in objavijo zanesljiv seznam priznanih ponudnikov storitev zaupanja.

   S sporazumi iz odstavka 1 se zagotovi, da so kvalificirane storitve zaupanja, ki jih zagotavljajo ponudniki kvalificiranih storitev zaupanja s sedežem v Uniji, pravno enakovredne storitvam zaupanja, ki jih zagotavljajo ponudniki storitev zaupanja v tretji državi ali mednarodna organizacija, s katero je sklenjen sporazum.

3. Izvedbeni sklepi iz odstavka 1 se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(19) člen 15 se nadomesti z naslednjim:

„*Člen 15*

Dostopnost za invalide

V skladu z zahtevami glede dostopnosti za proizvode in storitve iz Direktive 2019/882 se zagotovi, da so storitve zaupanja in proizvodi za končne uporabnike, ki se uporabljajo pri zagotavljanju navedenih storitev, dostopni invalidom.“;

„(20) člen 17 se spremeni:

(a) odstavek 4 se spremeni:

„(1) točka (c) odstavka 4 se nadomesti z naslednjim:

„(c) obveščanje drugih ustreznih pristojnih nacionalnih organov zadevnih držav članic, imenovanih v skladu z Direktivo (EU) XXXX/XXXX [direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] o kršitvah varnosti ali izgubi celovitosti, s katero se seznanijo med izvajanjem svojih nalog. Kadar večja kršitev varnosti ali izguba celovitosti zadeva druge države članice, nadzorni organ o tem obvesti enotno kontaktno točko zadevne države članice, imenovano v skladu z Direktivo (EU) XXXX/XXXX (direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji), in nadzorne organe, imenovane v skladu s členom 17 te uredbe, v drugih zadevnih državah članicah. Uradno obveščeni nadzorni organ o tem obvesti javnost ali to zahteva od ponudnika storitev zaupanja, kadar ugotovi, da je razkritje kršitve varnosti ali izgube celovitosti v javnem interesu;“;

„(2) točka (f) se nadomesti z naslednjim:

„(f) sodelovanje s pristojnimi nadzornimi organi, ustanovljenimi v skladu z Uredbo (EU) 2016/679, zlasti takojšnje obveščanje teh organov o domnevnih kršitvah pravil o varstvu osebnih podatkov in o kršitvah varnosti, ki domnevno pomenijo kršitve varnosti osebnih podatkov;“;

(b) odstavek 6 se nadomesti z naslednjim:

„6. Vsako leto do 31. marca vsak nadzorni organ Komisiji predloži poročilo o svojih glavnih dejavnostih v predhodnem koledarskem letu.“;

(c) odstavek 8 se nadomesti z naslednjim:

„8. Komisija v 12 mesecih po začetku veljavnosti te uredbe sprejme smernice o tem, kako nadzorni organi izvajajo naloge iz odstavka 4, ter z izvedbenimi akti, sprejetimi v skladu s postopkom pregleda iz člena 48(2), določi oblike in postopke za poročilo iz odstavka 6.“;

„(21) člen 18 se spremeni:

(a) naslov člena 18 se nadomesti z naslednjim:

„Medsebojna pomoč in sodelovanje“;

(b) odstavek 1 se nadomesti z naslednjim:

„1. Nadzorni organi sodelujejo z namenom izmenjave dobre prakse in informacij o zagotavljanju storitev zaupanja.“;

(c) dodata se naslednja odstavka 4 in 5:

„4. Nadzorni organi in pristojni nacionalni organi iz Direktive (EU) XXXX/XXXX Evropskega parlamenta in Sveta [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] sodelujejo in si pomagajo, da bi zagotovili, da ponudniki storitev zaupanja izpolnjujejo zahteve iz te uredbe in Direktive (EU) XXXX/XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji]. Nadzorni organi od pristojnih nacionalnih organov na podlagi Direktive (EU) XXXX/XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] zahtevajo, naj izvajajo nadzorne ukrepe, s katerimi preverijo, ali ponudniki storitev zaupanja izpolnjujejo zahteve iz Direktive (EU) XXXX/XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji], naj od ponudnikov storitev zaupanja zahtevajo, da odpravijo morebitno neizpolnjevanje teh zahtev, naj pravočasno zagotovijo rezultate vseh nadzornih dejavnosti, povezanih s ponudniki storitev zaupanja, in naj nadzorne organe obvestijo o incidentih, priglašenih v skladu z Direktivo (EU) XXXX/XXXX [direktivo o ukrepih za visoko skupno raven kibernetske varnosti v Uniji].

„5. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi potrebno postopkovno ureditev za lažje sodelovanje med nadzornimi organi iz odstavka 1. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(21a) vstavi se naslednji člen 19a:

„Zahteve za ponudnike nekvalificiranih storitev zaupanja

„1. Ponudnik nekvalificiranih storitev zaupanja, ki zagotavlja nekvalificirane storitve zaupanja:

(a) ima ustrezne politike in sprejema ustrezne ukrepe v zvezi z obvladovanjem pravnih, poslovnih, operativnih in drugih neposrednih ali posrednih tveganj za zagotavljanje nekvalificiranih storitev zaupanja. Ne glede na določbe iz člena 18 Direktive (EU) XXXX/XXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] navedeni ukrepi vključujejo najmanj naslednje:

(i) ukrepe, povezane s postopki registracije in vstopanja v storitev;

(ii) ukrepe, povezane s postopkovnimi ali upravnimi pregledi;

(iii) ukrepe, povezane z upravljanjem in izvajanjem storitev;

(b) obvesti nadzorni organ, določljive prizadete posameznike, javnost, če je to v javnem interesu, in po potrebi druge ustrezne pristojne organe – brez nepotrebnega odlašanja, v vsakem primeru pa najpozneje v 24 urah po seznanitvi z njimi – o morebitnih kršitvah ali prekinitvah pri zagotavljanju storitve ali izvajanju ukrepov iz odstavka (a), točke (i), (ii) in (iii), ki pomembno vplivajo na zagotovljeno storitev zaupanja ali na osebne podatke, vsebovane v njej.

„2. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične značilnosti ukrepov iz odstavka 1(a). Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(22) člen 20 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Ponudnike kvalificiranih storitev zaupanja na njihove lastne stroške vsaj vsakih 24 mesecev revidira organ za ugotavljanje skladnosti. Revizija potrdi, ali ponudniki kvalificiranih storitev zaupanja in kvalificirane storitve zaupanja, ki jih zagotavljajo, izpolnjujejo zahteve iz te uredbe in iz člena 18 Direktive (EU) XXXX/XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji]. Ponudniki kvalificiranih storitev zaupanja zadevno poročilo o ugotavljanju skladnosti predložijo nadzornemu organu v treh delovnih dneh po njegovem prejemu.“;

(aa) vstavi se naslednji odstavek:

„1a. Države članice lahko določijo, da ponudniki kvalificiranih storitev zaupanja vnaprej obvestijo nadzorni organ o načrtovanih revizijah in na zahtevo omogočijo sodelovanje nadzornega organa kot opazovalca.“;

(b) v odstavku 2 se zadnji stavek nadomesti z naslednjim:

„V primeru, da so bila pravila o varstvu osebnih podatkov domnevno kršena, nadzorni organ brez odlašanja obvesti pristojne nadzorne organe iz Uredbe (EU) 2016/679.“;

(c) odstavka 3 in 4 se nadomestita z naslednjim:

„3. Kadar ponudnik kvalificiranih storitev zaupanja ne izpolnjuje nobene od zahtev iz te uredbe, nadzorni organ zahteva, naj po potrebi to težavo odpravi v določenem roku.

Kadar navedeni ponudnik ne odpravi težave, po potrebi v roku, ki ga določi nadzorni organ, lahko nadzorni organ ob upoštevanju zlasti obsega, trajanja in posledic takega neizpolnjevanja navedenemu ponudniku ali zadevni storitvi, ki jo ponudnik zagotavlja, odvzame kvalificirani status.

3a. Kadar pristojni nacionalni organi v skladu z Direktivo (EU) XXXX/XXXX [direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] obvestijo nadzorni organ, da ponudnik kvalificiranih storitev zaupanja ne izpolnjuje katere od zahtev iz člena 18 navedene direktive, lahko nadzorni organ ob upoštevanju zlasti obsega, trajanja in posledic takega neizpolnjevanja navedenemu ponudniku ali zadevni storitvi, ki jo ponudnik zagotavlja, odvzame kvalificirani status.

3b. Kadar nadzorni organi v skladu z Uredbo (EU) 2016/679 obvestijo nadzorni organ, da ponudnik kvalificiranih storitev zaupanja ne izpolnjuje katere od zahtev iz Uredbe (EU) 2016/679, lahko nadzorni organ ob upoštevanju zlasti obsega, trajanja in posledic takega neizpolnjevanja navedenemu ponudniku ali zadevni storitvi, ki jo ponudnik zagotavlja, odvzame kvalificirani status.

3c. Nadzorni organ obvesti ponudnika kvalificiranih storitev zaupanja o odvzemu kvalificiranega statusa temu ponudniku ali zadevnim storitvam. Nadzorni organ o tem obvesti organ iz člena 22(3), da se posodobijo zanesljivi seznami iz člena 22(1), in pristojni nacionalni organ iz Direktive XXXX [direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji].

„4. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za:

(a) akreditacijo organov za ugotavljanje skladnosti in za poročila o ugotavljanju skladnosti iz odstavka 1;

(b) revizijske zahteve, na podlagi katerih morajo organi za ugotavljanje skladnosti opraviti ugotavljanje skladnosti ponudnikov kvalificiranih storitev zaupanja iz odstavka 1;

(c) sheme ugotavljanja skladnosti za izvajanje ugotavljanja skladnosti ponudnikov kvalificiranih storitev zaupanja s strani organov za ugotavljanje skladnosti in za predložitev poročila iz odstavka 1.

Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(23) člen 21 se spremeni:

„1. Kadar nameravajo ponudniki storitev zaupanja začeti zagotavljati kvalificirane storitve zaupanja, svojo namero priglasijo nadzornemu organu ter mu predložijo poročilo o ugotavljanju skladnosti, ki ga izda organ za ugotavljanje skladnosti in v katerem je potrjeno izpolnjevanje zahtev iz te uredbe in člena 18 Direktive (EU) XXXX/XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji].“;

(a) odstavek 2 se nadomesti z naslednjim:

„2. Nadzorni organ preveri, ali ponudnik storitev zaupanja in storitve zaupanja, ki jih ta zagotavlja, izpolnjujejo zahteve iz te uredbe, zlasti zahteve za ponudnike kvalificiranih storitev zaupanja in za kvalificirane storitve zaupanja, ki jih ti zagotavljajo.

Da bi nadzorni organ preveril, ali ponudnik storitev zaupanja izpolnjuje zahteve iz člena 18 Direktive (EU) XXXX/XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji], od pristojnih organov iz navedene direktive zahteva, naj v zvezi s tem izvajajo nadzorne ukrepe in brez odlašanja, v vsakem primeru pa najpozneje v dveh mesecih po prejemu te zahteve s strani pristojnih organov iz Direktive XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji], zagotovijo informacije o rezultatih. Če preverjanje ni zaključeno v dveh mesecih od priglasitve, pristojni organi iz Direktive XXXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] o tem obvestijo nadzorni organ ter navedejo razloge za zamudo in rok, v katerem je treba preverjanje zaključiti.

Kadar nadzorni organ ugotovi, da ponudnik storitev zaupanja in storitve zaupanja, ki jih ta zagotavlja, izpolnjujejo zahteve, določene v tej uredbi, najpozneje tri mesece po priglasitvi v skladu z odstavkom 1 tega člena ponudniku storitev zaupanja in storitvam zaupanja, ki jih ponudnik zagotavlja, podeli kvalificirani status ter obvesti organ iz člena 22(3), da se posodobijo zanesljivi seznami iz člena 22(1).

Kadar nadzorni organ preverjanja ne konča v treh mesecih od priglasitve, o tem obvesti ponudnika storitev zaupanja ter navede razloge za zamudo in rok, v katerem bo preverjanje končano.“;

(b) odstavek 4 se nadomesti z naslednjim:

„4. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi oblike in postopke priglasitve in preverjanja za namene odstavkov 1 in 2. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(25) člen 24 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Ob izdaji kvalificiranega potrdila ali kvalificiranega elektronskega potrdila o atributih ponudnik kvalificiranih storitev zaupanja preveri identiteto in po potrebi druge posebne atribute fizične ali pravne osebe, za katero se bo izdalo kvalificirano potrdilo ali kvalificirano elektronsko potrdilo atributov.

Ponudnik kvalificiranih storitev zaupanja podatke iz prvega pododstavka preveri bodisi neposredno ali prek tretje osebe na enega od naslednjih načinov:

(a) z evropsko denarnico za digitalno identiteto ali priglašenimi sredstvi elektronske identifikacije, ki izpolnjujejo zahteve iz člena 8 v zvezi z „visoko“ ravnjo zanesljivosti;

(b) s kvalificiranim elektronskim potrdilom o atributih ali potrdilom kvalificiranega elektronskega podpisa ali kvalificiranega elektronskega žiga, izdanega v skladu s točko (a), (c) ali (d);

(c) z uporabo drugih načinov identifikacije, ki zagotavljajo identifikacijo osebe z visoko stopnjo zaupanja, katere skladnost potrdi organ za ugotavljanje skladnosti;

(d) s fizično prisotnostjo fizične osebe ali pooblaščenega predstavnika pravne osebe z ustreznimi postopki in v skladu z nacionalnimi predpisi.“;

(b) vstavi se naslednji odstavek 1a:

„1a. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi minimalne tehnične specifikacije, standarde in postopke v zvezi s preverjanjem identitete in atributov v skladu z odstavkom 1, točka c. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(c) odstavek 2 se spremeni:

„(0) točka (a) se spremeni:

„(a) obvesti nadzorni organ vsaj en mesec pred kakršno koli spremembo pri zagotavljanju svojih kvalificiranih storitev zaupanja oziroma vsaj tri mesece v primeru namere o prenehanju opravljanja teh dejavnosti. Nadzorni organ lahko zahteva dodatne informacije ali rezultate ugotavljanja skladnosti, preden izda dovoljenje za izvedbo načrtovanih sprememb kvalificiranih storitev zaupanja. Če preverjanje ni zaključeno v treh mesecih od priglasitve, nadzorni organ o tem obvesti ponudnika storitev zaupanja ter navede razloge za zamudo in rok, do katerega bo preverjanje končal.“;

„(1) točki (d) in (e) se nadomestita z naslednjim:

„(d) pred vstopom v pogodbeno razmerje vsako osebo, ki želi uporabljati kvalificirano storitev zaupanja, jasno, razumljivo in z omogočanjem enostavnega dostopa na javno dostopnem mestu in posamezno obvesti o natančnih splošnih pogojih uporabe zadevne storitve, tudi o morebitnih omejitvah njene uporabe;“

„(e) uporablja zaupanja vredne sisteme in izdelke, ki so zaščiteni pred spreminjanjem, ter zagotavlja tehnično varnost in zanesljivost postopkov, pri katerih se uporabljajo, vključno z uporabo ustreznih kriptografskih algoritmov, dolžin ključev in zgoščevalnih funkcij v sistemih, izdelkih in postopkih, pri katerih se uporabljajo;“;

„(2) vstavita se novi točki (fa) in (fb):

„(fa) ima ustrezne politike in sprejema ustrezne ukrepe v zvezi z obvladovanjem pravnih, operativnih in drugih neposrednih ali posrednih tveganj za zagotavljanje kvalificiranih storitev zaupanja. Ne glede na določbe iz člena 18 Direktive (EU) XXXX/XXX [direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji] navedeni ukrepi vključujejo najmanj naslednje:

(i) ukrepe, povezane s postopki registracije in vstopanja v storitev;

(ii) ukrepe, povezane s postopkovnimi ali upravnimi pregledi;

(iii) ukrepe, povezane z upravljanjem in izvajanjem storitev;“;

„(fb) obvesti nadzorni organ, določljive prizadete posameznike, po potrebi druge ustrezne pristojne organe in, na zahtevo nadzornega organa, javnost, če je to v javnem interesu – brez nepotrebnega odlašanja in v vsakem primeru najpozneje v 24 urah po incidentu – o kakršnih koli kršitvah ali prekinitvah pri zagotavljanju storitve ali izvajanju ukrepov iz odstavka (fa), točke (i), (ii) in (iii), ki pomembno vplivajo na zagotovljeno storitev zaupanja ali osebne podatke, vsebovane v njej.“;

„(3) točki (g) in (h) se nadomestita z naslednjim:

„(g) sprejme ustrezne ukrepe proti ponarejanju, kraji ali protipravni prilastitvi podatkov ali neupravičenemu brisanju ali spreminjanju podatkov ali onemogočanju dostopa do njih;“;

„(h) potem ko je ponudnik kvalificiranih storitev zaupanja prenehal opravljati dejavnosti, toliko časa, kolikor je potrebno, beleži vse pomembne informacije o podatkih, ki jih je izdal in prejel ponudnik kvalificiranih storitev zaupanja, ter ohranja dostop do njih, da se zagotovijo dokazi v pravnih postopkih in neprekinjenost storitve. Beleženje je lahko elektronsko;“;

„(4) točka (j) se črta;

(d) vstavi se naslednji odstavek 4a:

„4a. Odstavka 3 in 4 se ustrezno uporabljata za preklic kvalificiranih elektronskih potrdil o atributih.“;

(e) odstavek 5 se nadomesti z naslednjim:

„5. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije, postopke in referenčne številke standardov za zahteve iz odstavka 2. Zahteve iz tega člena veljajo za izpolnjene v primeru izpolnjevanja navedenih tehničnih specifikacij, postopkov in standardov. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(f) vstavi se naslednji odstavek 6:

„6. Na Komisijo se prenese pooblastilo za sprejemanje izvedbenih aktov, s katerimi se določijo tehnične značilnosti ukrepov iz odstavka 2(fa).“;

(25a) člen 26 se spremeni:

„2. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za napredne elektronske podpise. Zahteve za napredne elektronske podpise veljajo za izpolnjene, če napredni elektronski podpis izpolnjuje te specifikacije in standarde. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

(25b) člen 27 se spremeni:

odstavek 4 se črta;

„(26) v členu 28 se odstavek 6 nadomesti z naslednjim:

„6. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za kvalificirana potrdila za elektronski podpis. Zahteve iz Priloge I veljajo za izpolnjene, če kvalificirano potrdilo za elektronski podpis izpolnjuje navedene specifikacije in standarde. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(27) V členu 29 se doda naslednji novi odstavek 1a:

„1a. Podatke za ustvarjanje elektronskega podpisa lahko v imenu podpisnika pridobiva, upravlja ali za namene varnostne kopije podvaja le ponudnik kvalificiranih storitev zaupanja za namene upravljanja naprav za ustvarjanje kvalificiranega elektronskega podpisa na daljavo.“;

„(28) vstavi se naslednji člen 29a:

„Člen 29a

Zahteve za kvalificirane storitve upravljanja naprav za ustvarjanje kvalificiranega elektronskega podpisa na daljavo

„1. Naprave za ustvarjanje kvalificiranega elektronskega podpisa na daljavo lahko upravlja samo ponudnik kvalificiranih storitev zaupanja, ki:

(a) pridobiva ali upravlja podatke za ustvarjanje elektronskega podpisa v imenu podpisnika;

(b) ne glede na točko 1(d) Priloge II lahko podatke za ustvarjanje elektronskega podpisa podvaja le za namene varnostne kopije, pod pogojem, da sta izpolnjeni naslednji zahtevi:

i. varnost podvojenih naborov podatkov je enaka ravni, ki jo ima varnost prvotnih naborov podatkov;

ii. število podvojenih naborov podatkov ni večje, kot je to nujno potrebno, da se zagotovi neprekinjenost storitve;

(c) izpolnjuje vse zahteve, ki so opredeljene v poročilu o certificiranju določene naprave za ustvarjanje kvalificiranega elektronskega podpisa na daljavo, izdanem v skladu s členom 30.

„2. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za namene odstavka 1.“;

„(29) v členu 30 se vstavi naslednji odstavek 3a:

„3a. Veljavnost certifikacije iz odstavka 1 ni daljša od pet let, odvisno od ocene ranljivosti, ki se izvaja redno vsaki dve leti. Kadar so ranljivosti ugotovljene, vendar niso odpravljene, se certifikacija prekliče.“;

„(30) v členu 31 se odstavek 3 nadomesti z naslednjim:

„3. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi oblike in postopke, ki se uporabljajo za namene odstavka 1. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(31) člen 32 se spremeni:

(a) v odstavku 1 se doda naslednji pododstavek:

„Zahteve iz prvega pododstavka veljajo za izpolnjene, če so pri potrjevanju veljavnosti kvalificiranih elektronskih podpisov izpolnjeni specifikacije in standardi iz odstavka 3.“;

(b) odstavek 3 se nadomesti z naslednjim:

„3. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi specifikacije in referenčne številke standardov za potrjevanje veljavnosti kvalificiranih elektronskih podpisov. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(31a) vstavi se naslednji člen 32a:

Zahteve za potrjevanje veljavnosti naprednih elektronskih podpisov na podlagi kvalificiranih potrdil

„1. S postopkom za potrjevanje veljavnosti naprednega elektronskega podpisa na podlagi kvalificiranega potrdila se potrdi veljavnost naprednega elektronskega podpisa na podlagi kvalificiranega potrdila pod pogojem, da:

(a) je bilo potrdilo, na katerem temelji podpis, v času podpisa kvalificirano potrdilo za elektronski podpis, ki je skladno s Prilogo I;

(b) je kvalificirano potrdilo izdal ponudnik kvalificiranih storitev zaupanja in je bilo veljavno v času podpisa;

(c) podatki za potrjevanje veljavnosti podpisa ustrezajo podatkom, predloženim zanašajočim se strankam;

(d) je enolični nabor podatkov, ki predstavlja podpisnika potrdila, pravilno predložen zanašajočim se strankam;

(e) je zanašajoči se stranki jasno sporočeno, če je bil v času podpisa uporabljen psevdonim;

(f) celovitost podpisanih podatkov ni ogrožena;

(g) so bile v času podpisa izpolnjene zahteve iz člena 26. Zahteve iz prvega pododstavka veljajo za izpolnjene, če so pri potrjevanju veljavnosti naprednih elektronskih podpisov na podlagi kvalificiranih potrdil izpolnjeni specifikacije in standardi iz odstavka 3.

„2. Sistem za potrjevanje veljavnosti naprednega elektronskega podpisa na podlagi kvalificiranega potrdila zanašajoči se stranki zagotavlja pravilne rezultate postopka potrjevanja veljavnosti in ji omogoča odkrivanje vseh zadevnih varnostnih vprašanj.

„3. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi specifikacije in referenčne številke standardov za potrjevanje veljavnosti naprednih elektronskih podpisov na podlagi kvalificiranih potrdil. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(31b) člen 33 se spremeni:

„1. Kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov lahko zagotavlja le ponudnik kvalificiranih storitev zaupanja, ki:“;

„2. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za kvalificirane storitve potrjevanja veljavnosti iz odstavka 1. Zahteve iz odstavka 1 veljajo za izpolnjene, če storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov izpolnjuje te specifikacije in standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(32) člen 34 se nadomesti z naslednjim:

„*Člen 34*

Kvalificirana storitev hrambe za kvalificirane elektronske podpise

„1. Kvalificirano storitev hrambe za kvalificirane elektronske podpise lahko zagotavlja le ponudnik kvalificiranih storitev zaupanja, ki uporablja postopke in tehnologije, s katerimi se zanesljivost kvalificiranega elektronskega podpisa lahko podaljša tudi po izteku obdobja tehnološke veljavnosti.

„2. Zahteve iz odstavka 1 veljajo za izpolnjene, če ureditve za kvalificirano storitev hrambe za kvalificirane elektronske podpise izpolnjujejo specifikacije in standarde iz odstavka 3.

„3. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za kvalificirano storitev hrambe za kvalificirane elektronske podpise. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(32a) v členu 36 se doda nov odstavek 2:

„2. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za napredne elektronske žige.

Zahteve za napredne elektronske žige veljajo za izpolnjene, če napredni elektronski žig izpolnjuje te specifikacije in standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(33) člen 37 se spremeni:

odstavek 4 se črta;

„(34) člen 38 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Kvalificirana potrdila za elektronske žige izpolnjujejo zahteve iz Priloge III. Zahteve iz Priloge III veljajo za izpolnjene, če kvalificirano potrdilo za elektronski žig izpolnjuje specifikacije in standarde iz odstavka 6.“;

(b) odstavek 6 se nadomesti z naslednjim:

„6. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za kvalificirana potrdila za elektronske žige. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(35) vstavi se naslednji člen 39a:

„Člen 39a

Zahteve za kvalificirane storitve upravljanja naprav za ustvarjanje kvalificiranega elektronskega žiga na daljavo

Člen 29a se smiselno uporablja za kvalificirane storitve upravljanja naprav za ustvarjanje kvalificiranega elektronskega žiga na daljavo.“;

(35a) vstavi se naslednji člen 40a:

„*Člen 40a*

Zahteve za potrjevanje veljavnosti naprednih elektronskih žigov na podlagi kvalificiranih potrdil

(1) Člen 32a se smiselno uporablja za potrjevanje veljavnosti naprednih elektronskih žigov na podlagi kvalificiranih potrdil.“;

„(36) člen 42 se spremeni:

(a) vstavi se naslednji nov odstavek 1a:

„1a. Zahteve iz odstavka 1 veljajo za izpolnjene, če povezava datuma in časa s podatki in točen časovni vir izpolnjujeta specifikacije in standarde iz odstavka 2.“;

(b) odstavek 2 se nadomesti z naslednjim:

„2. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za povezavo datuma in časa s podatki in za točen časovni vir. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(36a) v členu 43 se doda nov odstavek 3:

2a. Kvalificirana storitev elektronske priporočene dostave v eni državi članici se prizna kot kvalificirana storitev elektronske priporočene dostave v kateri koli drugi državi članici.“;

„(37) člen 44 se spremeni:

(a) vstavi se naslednji odstavek 1a:

„1a. Zahteve iz odstavka 1 veljajo za izpolnjene, če postopek pošiljanja in prejemanja podatkov izpolnjuje specifikacije in standarde iz odstavka 2.“;

(b) odstavek 2 se nadomesti z naslednjim:

„2. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za postopke pošiljanja in prejemanja podatkov. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(c) vstavita se naslednja odstavka 3 in 4:

„3. Ponudniki kvalificiranih storitev elektronske priporočene dostave se lahko dogovorijo o interoperabilnosti kvalificiranih storitev elektronske priporočene dostave, ki jih zagotavljajo. Tak okvir interoperabilnosti je skladen z zahtevami iz odstavka 1. Skladnost potrdi organ za ugotavljanje skladnosti.“;

„4. Komisija lahko z izvedbenim aktom določi tehnične specifikacije in referenčne številke standardov, da se olajša prenos podatkov med dvema ali več ponudniki kvalificiranih storitev zaupanja. Tehnične specifikacije in vsebina standardov so stroškovno učinkovite in sorazmerne. Izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 48(2).“;

„(38) člen 45 se nadomesti z naslednjim:

„*Člen 45*

Zahteve za kvalificirana potrdila za avtentikacijo spletišč

„1. Kvalificirana potrdila za avtentikacijo spletišč izpolnjujejo zahteve iz Priloge IV. Ocenjevanje izpolnjevanja zahtev iz Priloge IV se izvede v skladu s specifikacijami in standardi iz odstavka 4.

„2. Kvalificirana potrdila za avtentikacijo spletišč iz odstavka 1 so priznana na spletnih brskalnikih. Spletni brskalniki za navedene namene zagotovijo, da se podatki o identiteti, zagotovljeni s katero koli metodo, prikažejo na uporabniku prijazen način. Spletni brskalniki zagotovijo podporo in interoperabilnost s kvalificiranimi potrdili za avtentikacijo spletišč iz odstavka 1, z izjemo podjetij, ki se štejejo za mikro in mala podjetja v skladu s Priporočilom Komisije 2003/361/ES, v prvih petih letih delovanja v vlogi ponudnikov storitev spletnih brskalnikov.

„4. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi specifikacije in referenčne številke standardov za kvalificirana potrdila za avtentikacijo spletišč iz odstavkov 1 in 2. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(39) za členom 45 se vstavijo naslednji oddelki 9, 10 in 11:

„ODDELEK 9

ELEKTRONSKO POTRDILO O ATRIBUTIH

Člen 45a

Pravni učinki elektronskega potrdila o atributih

„1. Elektronskemu potrdilu o atributih se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker je v elektronski obliki ali ker ne izpolnjuje zahtev za kvalificirana elektronska potrdila o atributih.

„2. Kvalificirano elektronsko potrdilo o atributih in potrdila o atributih, izdana s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, imajo enak pravni učinek kot zakonito izdana potrdila v papirni obliki.

„3. Kvalificirano elektronsko potrdilo o atributih, izdano v eni državi članici, se prizna kot kvalificirano elektronsko potrdilo o atributih v kateri koli drugi državi članici.

„4. Potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, se prizna kot potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, v vseh državah članicah.

Člen 45b

Elektronsko potrdilo o atributih na področju javnih storitev

Če nacionalno pravo za dostop do spletne storitve, ki jo zagotavlja organ javnega sektorja, predpisuje elektronsko identifikacijo z uporabo sredstva elektronske identifikacije in avtentikacije, identifikacijski podatki osebe v elektronskem potrdilu o atributih za namene elektronske identifikacije ne nadomestijo elektronske identifikacije z uporabo sredstva elektronske identifikacije in avtentikacije, razen če to izrecno dovoljuje država članica. V takih primerih se sprejme tudi elektronsko potrdilo o atributih iz drugih držav članic.

Člen 45c

Zahteve za kvalificirana elektronska potrdila o atributih

„1. Kvalificirana elektronska potrdila o atributih izpolnjujejo zahteve iz Priloge V.

„1a. Ocena izpolnjevanja zahtev iz Priloge V se izvede v skladu s specifikacijami in standardi iz odstavka 4.

„2. Za kvalificirana elektronska potrdila o atributih ne veljajo nobene obvezne zahteve poleg zahtev iz Priloge V.

„3. Kadar se kvalificirano elektronsko potrdilo o atributih po prvi izdaji prekliče, preneha veljati v trenutku njegovega preklica, status pa se mu v nobenem primeru ne povrne v prejšnje stanje.

„4. Komisija v šestih mesecih po začetku veljavnosti te uredbe določi tehnične specifikacije in referenčne številke standardov za kvalificirana elektronska potrdila o atributih z izvedbenim aktom o uvedbi evropskih denarnic za digitalno identiteto, kot je določeno v členu 6a(11).

Člen 45d

Preverjanje atributov na podlagi verodostojnih virov

„1. Države članice v 24 mesecih po začetku veljavnosti izvedbenih aktov iz člena 6a(11) in člena 6c(4) zagotovijo, da so vsaj za atribute iz Priloge VI, kadar koli se ti atributi opirajo na verodostojne vire znotraj javnega sektorja, sprejeti ukrepi, ki ponudnikom kvalificiranih elektronskih potrdil o atributih omogočajo, da na zahtevo uporabnika z elektronskimi sredstvi preverijo te atribute v skladu z nacionalnim pravom ali pravom Unije.

„2. Komisija v šestih mesecih po začetku veljavnosti te uredbe ob upoštevanju ustreznih mednarodnih standardov z izvedbenim aktom o uvedbi evropskih denarnic za digitalno identiteto iz člena 6a(11) določi minimalne tehnične specifikacije, standarde in postopke na podlagi kataloga atributov in shem za potrjevanje atributov ter postopke preverjanja za kvalificirana elektronska potrdila o atributih.

Člen 45da

Zahteve za elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir

„1. Elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, izpolnjuje naslednje zahteve:

a) zahteve iz Priloge VII;

b) kvalificirano potrdilo, na katerem temelji kvalificirani elektronski podpis ali kvalificirani elektronski žig organa javnega sektorja iz člena 3(45a), opredeljenega kot izdajatelja iz točke (b) Priloge VII, vsebuje specifični nabor certificiranih atributov v obliki, primerni za avtomatsko obdelavo, ki:

(i) navaja, da je organ izdajatelj v skladu z nacionalnim pravom ali pravom Unije določen kot pristojen za verodostojni vir, na podlagi katerega je izdano elektronsko potrdilo o atributih, ali kot organ, imenovan, da ukrepa v njegovem imenu;

(ii) zagotavlja nabor podatkov, ki nedvoumno predstavlja verodostojni vir iz točke (i), in

(iii) določa nacionalno pravo ali pravo Unije iz točke (i).

„2. Država članica, v kateri imajo sedež organi javnega sektorja iz člena 3(45a), zagotovi, da je raven zanesljivosti organov javnega sektorja, ki izdajajo elektronska potrdila o atributih, enakovredna ravni zanesljivosti ponudnikov kvalificiranih storitev zaupanja v skladu s členom 24.

2a. Države članice organe javnega sektorja iz člena 3(45a) priglasijo Komisiji. Ta priglasitev vključuje poročilo o ugotavljanju skladnosti, ki ga izda organ za ugotavljanje skladnosti in ki potrjuje, da so zahteve iz odstavkov 1, 2 in 6 tega člena izpolnjene. Komisija da seznam organov javnega sektorja iz člena 3(45a) na voljo javnosti na varen način in v elektronsko podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo.

„3. Kadar je bilo elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, po prvotni izdaji preklicano, preneha veljati ob preklicu. Po preklicu se preklicani status elektronskega potrdila ne povrne v prejšnje stanje.

„4. Šteje se, da elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, izpolnjuje zahteve iz odstavka 1 tega člena, kadar izpolnjuje standarde iz odstavka 5.

„5. Komisija v šestih mesecih po začetku veljavnosti te uredbe določi tehnične specifikacije in referenčne številke standardov za elektronska potrdila o atributih, izdana s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, z izvedbenim aktom o uvedbi evropskih denarnic za digitalno identiteto iz člena 6a(11).

5a. Komisija v šestih mesecih po začetku veljavnosti te uredbe z izvedbenim aktom o uvedbi evropskih denarnic za digitalno identiteto iz člena 6a(11) opredeli oblike, postopke, specifikacije in standarde za namene iz odstavka 2a.

„6. Organi javnega sektorja iz člena 3(45a), ki izdajo elektronsko potrdilo o atributih, zagotovijo vmesnik za evropske denarnice za digitalno identiteto, zagotovljene v skladu s členom 6a.

Člen 45e

Izdaja elektronskih potrdil o atributih za evropske denarnice za digitalno identiteto

Ponudniki kvalificiranih elektronskih potrdil o atributih zagotovijo vmesnik za evropske denarnice za digitalno identiteto, zagotovljene v skladu s členom 6a.

Člen 45f

Dodatna pravila za zagotavljanje storitev elektronskega potrjevanja atributov

„1. Ponudniki kvalificiranih in nekvalificiranih storitev elektronskega potrjevanja atributov osebnih podatkov v zvezi z zagotavljanjem navedenih storitev ne združujejo z osebnimi podatki v zvezi s katerimi koli drugimi storitvami, ki jih ponujajo sami ali ki jih ponujajo njihovi poslovi partnerji.

„2. Osebni podatki v zvezi z zagotavljanjem storitev elektronskega potrjevanja atributov se hranijo logično ločeni od drugih podatkov, shranjenih pri zadevnem ponudniku elektronskega potrjevanja atributov.

„4. Ponudniki kvalificiranih storitev elektronskega potrjevanja atributov pri zagotavljanju takih storitev poskrbijo za funkcionalno ločitev.

ODDELEK 10

STORITVE ELEKTRONSKEGA ARHIVIRANJA

Člen 45g

Pravni učinek storitve elektronskega arhiviranja

„1. Elektronskim podatkom, shranjenim s storitvijo elektronskega arhiviranja, se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker so v elektronski obliki ali niso shranjeni s kvalificirano storitvijo elektronskega arhiviranja.

„2. V zvezi z elektronskimi podatki, shranjenimi s kvalificirano storitvijo elektronskega arhiviranja, se med obdobjem njihove hrambe pri ponudniku kvalificiranih storitev zaupanja ohrani domneva njihove celovitosti in porekla.

„3. Kvalificirana storitev elektronskega arhiviranja v eni državi članici se prizna kot kvalificirana storitev elektronskega arhiviranja v kateri koli drugi državi članici.

Člen 45ga

Zahteve za kvalificirane storitve elektronskega arhiviranja

„1. Kvalificirane storitve elektronskega arhiviranja izpolnjujejo naslednje zahteve:

(a) zagotavljajo jih ponudniki kvalificiranih storitev zaupanja;

(b) uporabljajo postopke in tehnologije, s katerimi se lahko zagotovi, da so elektronski podatki obstojni in berljivi tudi po izteku obdobja tehnološke veljavnosti ter vsaj med celotnim pravnim ali pogodbenim obdobjem hrambe, pri čemer sta ohranjena njihova celovitost in poreklo;

(c) zagotavljajo, da so elektronski podatki shranjeni tako, da so zavarovani pred izgubo ali spreminjanjem, z izjemo sprememb njihovega nosilca ali elektronske oblike;

(d) pooblaščenim zanašajočim se strankam omogočajo, da na avtomatiziran način prejmejo poročilo, ki v zvezi z elektronskim podatkom iz kvalificiranega elektronskega arhiva potrjuje, da zanj obstaja domneva celovitosti podatkov od začetka obdobja hrambe do trenutka, ko so do njih dobile dostop. To poročilo se zagotovi na zanesljiv in učinkovit način ter je opremljeno s kvalificiranim elektronskim podpisom ali kvalificiranim elektronskim žigom ponudnika kvalificiranih storitev elektronskega arhiviranja.

„2. Komisija v 12 mesecih po začetku veljavnosti te uredbe z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za kvalificirane storitve elektronskega arhiviranja. Zahteve za kvalificirane storitve elektronskega arhiviranja veljajo za izpolnjene, če kvalificirana storitev elektronskega arhiviranja izpolnjuje te specifikacije in standarde. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

ODDELEK 11

ELEKTRONSKE EVIDENCE

Člen 45h

Pravni učinki elektronskih evidenc

„1. Elektronski evidenci se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker je v elektronski obliki ali ne izpolnjuje zahtev za kvalificirane elektronske evidence.

„2. V zvezi s podatkovnimi zapisi v kvalificirani elektronski evidenci se domneva, da so navedeni v enoličnem in točnem kronološkem zaporedju ter da so celoviti.

„3. Kvalificirana elektronska evidenca v eni državi članici se prizna kot kvalificirana elektronska evidenca v kateri koli drugi državi članici.

Člen 45i

Zahteve za kvalificirane elektronske evidence

„1. Kvalificirane elektronske evidence izpolnjujejo naslednje zahteve:

(a) pripravlja jih eden ali več ponudnikov kvalificiranih storitev zaupanja;

(b) dokazujejo poreklo podatkovnih zapisov v evidenci;

(c) zagotavljajo enolično kronološko zaporedje podatkovnih zapisov v evidenci;

(d) podatke beležijo tako, da je vsako naknadno spremembo podatkov mogoče takoj ugotoviti, ter tako zagotavljajo njihovo celovitost skozi čas.

„2. Zahteve iz odstavka 1 veljajo za izpolnjene, kadar elektronska evidenca izpolnjuje specifikacije in standarde iz odstavka 3.

„3. Komisija z izvedbenimi akti določi tehnične specifikacije in referenčne številke standardov za ustvarjenje in delovanje kvalificirane elektronske evidence. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

„(40) vstavi se naslednji člen 48a:

„*Člen 48a*

Zahteve glede poročanja

„1. Države članice zagotovijo zbiranje statističnih podatkov v zvezi z delovanjem evropskih denarnic za digitalno identiteto, ko se začnejo zagotavljati na njihovem ozemlju.

„2. Statistični podatki, zbrani v skladu z odstavkom 1, vključujejo naslednje:

(a) število fizičnih in pravnih oseb z veljavno evropsko denarnico za digitalno identiteto;

(b) vrsto in število storitev, ki sprejemajo uporabo evropske denarnice za digitalno identiteto;

(c) zbirno poročilo s podatki o incidentih, ki so onemogočili uporabo evropske denarnice za digitalni identiteto.

„3. Statistični podatki iz odstavka 2 se dajo na voljo javnosti v odprti in splošno uporabljeni ter strojno berljivi obliki.

„4. Države članice do 31. marca vsakega leta predložijo Komisiji poročilo o statističnih podatkih, zbranih v skladu z odstavkom 2.“;

„(41) člen 49 se nadomesti z naslednjim:

„*Člen 49*

Pregled

„1. Komisija pregleda uporabo te uredbe ter o tem poroča Evropskemu parlamentu in Svetu v 36 mesecih po njenem začetku veljavnosti. Komisija oceni zlasti področje uporabe člena 6 in člena 6db ter ali bi bilo ustrezno spremeniti področje uporabe te uredbe ali njene posebne določbe, pri tem pa upošteva izkušnje, pridobljene pri uporabi te uredbe, pa tudi spremembe v potrošniškem povpraševanju ter tehnološke, tržne in pravne spremembe. Navedeno poročilo po potrebi vsebuje predlog za spremembo te uredbe.

„2. Poročilo o oceni vključuje oceno razpoložljivosti in uporabnosti evropskih denarnic za digitalno identiteto, ki spadajo na področje uporabe te uredbe, ter oceno o tem, ali so vsi zasebni ponudniki spletnih storitev, ki avtentikacijo uporabnikov opravljajo prek storitev elektronske identifikacije tretjih oseb, obvezani k sprejetju uporabe evropskih denarnic za digitalno identiteto.

„3. Komisija poleg tega Evropskemu parlamentu in Svetu vsaka štiri leta po predložitvi poročila iz prvega odstavka predloži poročilo o napredku pri doseganju ciljev te uredbe.“

„(42) člen 51 se nadomesti z naslednjim:

„*Člen 51*

Prehodni ukrepi

„1. Naprave za varno ustvarjanje podpisa, katerih skladnost je bila ugotovljena v skladu s členom 3(4) Direktive 1999/93/ES, se v obdobju 36 mesecev po začetku veljavnosti te uredbe še naprej štejejo za naprave za ustvarjanje kvalificiranega elektronskega podpisa na podlagi te uredbe.

„2. Kvalificirana potrdila, izdana fizičnim osebam na podlagi Direktive 1999/93/ES, se v obdobju 24 mescev po začetku veljavnosti te uredbe še naprej štejejo za kvalificirana potrdila za elektronske podpise po tej uredbi.“.

2a. Za upravljanje naprav za ustvarjanje kvalificiranega elektronskega podpisa in žiga na daljavo s strani ponudnikov kvalificiranih storitev zaupanja, ki niso ponudniki kvalificiranih storitev zaupanja, ki zagotavljajo kvalificirane storitve zaupanja za upravljanje naprav za ustvarjanje kvalificiranega elektronskega podpisa in žiga na daljavo v skladu s členoma 29a in 39a, se v obdobju 24 mesecev po začetku veljavnosti te uredbe še naprej šteje, da za zagotavljanje teh storitev upravljanja ni treba pridobiti kvalificiranega statusa.

2b. Ponudniki kvalificiranih storitev zaupanja, ki jim je bil dodeljen kvalificirani status na podlagi te uredbe pred [datum začetka veljavnosti uredbe o spremembi] in uporabljajo načine preverjanja identitete za izdajo kvalificiranih potrdil v skladu s členom 24(1), nadzornemu organu čim prej, najpozneje pa 30 mesecev po začetku veljavnosti uredbe o spremembi, predložijo poročilo o ugotavljanju skladnosti, ki dokazuje skladnost s členom 24(1). Dokler tako poročilo o ugotavljanju skladnosti ni predloženo in dokler nadzorni organ ne zaključi ocene, lahko ponudnik kvalificirane storitve zaupanja še naprej uporablja načine preverjanja identitete iz člena 24(1) Uredbe (EU) št. 910/2014.

„(43) Priloga I se spremeni v skladu s Prilogo I k tej uredbi;

„(44) Priloga II se nadomesti z besedilom iz Priloge II k tej uredbi;

„(45) Priloga III se spremeni v skladu s Prilogo III k tej uredbi;

„(46) Priloga IV se spremeni v skladu s Prilogo IV k tej uredbi;

„(47) doda se nova priloga V, kakor je določeno v Prilogi V k tej uredbi;

„(48) doda se nova Priloga VI k tej uredbi.

Člen 52

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju,

Za Evropski parlament Za Svet

predsednik/predsednicapredsednik/predsednica

PRILOGA I

V Prilogi I se točka (i) nadomesti z naslednjim:

„(i) informacije o storitvah ali lokacijo storitev, s katerimi je mogoče preveriti veljavnost kvalificiranega potrdila;“.

PRILOGA II

ZAHTEVE ZA NAPRAVE ZA USTVARJANJE KVALIFICIRANEGA ELEKTRONSKEGA PODPISA

„1. Naprave za ustvarjanje kvalificiranega elektronskega podpisa z ustrezno tehnologijo in postopki zagotavljajo vsaj, da:

(a) je razumno zagotovljena zaupnost podatkov za ustvarjanje elektronskega podpisa, s katerimi se ustvari elektronski podpis;

(b) se lahko podatki za ustvarjanje elektronskega podpisa, s katerimi se ustvari elektronski podpis, dejansko pojavijo samo enkrat;

(c) je razumno zagotovljeno, da do podatkov za ustvarjanje elektronskega podpisa, s katerimi se ustvari elektronski podpis, ni mogoče priti s sklepanjem in da je elektronski podpis z uporabo trenutno razpoložljive tehnologije zanesljivo zaščiten pred ponarejanjem;

(d) lahko zakoniti podpisnik zanesljivo zaščiti podatke za ustvarjanje elektronskega podpisa, s katerimi se ustvari elektronski podpis, pred tem, da bi jih lahko uporabljali drugi.

„2. Naprave za ustvarjanje kvalificiranega elektronskega podpisa ne spreminjajo podatkov, ki bodo podpisani, ali preprečijo, da bi se ti podatki podpisniku prikazali pred podpisom.

PRILOGA III

V Prilogi III se točka (i) nadomesti z naslednjim:

„(i) informacije o storitvah ali lokacijo storitev, s katerimi je mogoče preveriti veljavnost kvalificiranega potrdila;“.

PRILOGA IV

V Prilogi IV se točka (j) nadomesti z naslednjim:

„(j) informacije o storitvah za preverjanje veljavnosti potrdila ali lokacijo teh storitev, s katerimi je mogoče preveriti veljavnost kvalificiranega potrdila.“.

PRILOGA V

ZAHTEVE ZA KVALIFICIRANA ELEKTRONSKA POTRDILA O ATRIBUTIH

Kvalificirana elektronska potrdila o atributih vsebujejo:

(e) navedbo, vsaj v obliki, primerni za avtomatizirano obdelavo, da je bilo potrdilo izdano kot kvalificirano elektronsko potrdilo o atributih;

(f) nabor podatkov, ki nedvoumno predstavlja ponudnika kvalificiranih storitev zaupanja, ki izdaja kvalificirana elektronska potrdila o atributih, ter vključuje vsaj državo članico, v kateri ima zadevni ponudnik sedež, in:

– za pravne osebe ime in po potrebi registrsko številko, kot sta navedena v uradnih evidencah,

– za fizične osebe ime osebe;

(g) nabor podatkov, ki nedvoumno predstavlja subjekt, na katerega se nanašajo potrjeni atributi; če je uporabljen psevdonim, se to jasno navede;

(h) potrjeni atribut ali atribute, po potrebi vključno z informacijami, potrebnimi za opredelitev obsega navedenih atributov;

(i) podrobnosti o začetku in koncu obdobja veljavnosti potrdila;

(j) identifikacijsko kodo potrdila, ki mora biti enolična za ponudnika kvalificiranih storitev zaupanja, in, če je primerno, navedbo sheme potrdil, med katere spada potrdilo o atributih;

(k) kvalificirani elektronski podpis ali kvalificirani elektronski žig ponudnika kvalificiranih storitev zaupanja, ki izdaja potrdilo;

(l) lokacijo, na kateri je potrdilo, ki podpira kvalificirani elektronski podpis ali kvalificirani elektronski žig iz točke (g), na voljo brezplačno;

(m) informacije o storitvah ali lokacijo storitev, s katerimi je mogoče preveriti veljavnost kvalificiranega potrdila.

PRILOGA VI

MINIMALNI SEZNAM ATRIBUTOV

Države članice na podlagi člena 45d zagotovijo, da se sprejmejo ukrepi, s katerimi lahko ponudniki kvalificiranih elektronskih potrdil o atributih z elektronskimi sredstvi na zahtevo uporabnika preverijo avtentičnost naslednjih atributov na podlagi ustreznega verodostojnega vira na nacionalni ravni ali prek imenovanih posrednikov, priznanih na nacionalni ravni, v skladu z nacionalnim pravom ali pravom Unije, kadar se ti atributi opirajo na verodostojne vire znotraj javnega sektorja:

1. naslov;
2. starost;
3. spol;
4. osebno stanje;
5. sestava družine;
6. državljanstvo ali nacionalna pripadnost;
7. izobrazba, nazivi in licence;
8. poklicne kvalifikacije, nazivi in licence;
9. javna dovoljenja in licence;
10. finančni podatki in podatki o družbi.

PRILOGA VII

ZAHTEVE ZA ELEKTRONSKO POTRDILO O ATRIBUTIH, IZDANO S STRANI ALI V IMENU ORGANA JAVNEGA SEKTORJA, PRISTOJNEGA ZA VERODOSTOJNI VIR

Elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, vsebuje:

a) navedbo, vsaj v obliki, primerni za avtomatizirano obdelavo, da je bilo potrdilo izdano kot elektronsko potrdilo o atributih, izdano s strani ali v imenu javnega organa, pristojnega za verodostojni vir;
b) nabor podatkov, ki nedvoumno predstavlja javni organ, ki izdaja elektronsko potrdilo o atributih, ki zajemajo vsaj državo članico, v kateri ima ta javni organ sedež, ter njegovo ime in po potrebi registrsko številko, kot sta navedena v uradnih evidencah;
c) nabor podatkov, ki nedvoumno predstavlja subjekt, na katerega se nanašajo potrjeni atributi; če je uporabljen psevdonim, se to jasno navede;
d) potrjeni atribut ali atribute, po potrebi vključno z informacijami, potrebnimi za opredelitev obsega navedenih atributov;
e) podrobnosti o začetku in koncu obdobja veljavnosti potrdila;
f) identifikacijsko kodo potrdila, ki mora biti enolična za javni organ izdajatelj, in, če je primerno, navedbo sheme potrdil, med katere spada potrdilo o atributih;
g) kvalificirani elektronski podpis ali kvalificirani elektronski žig organa izdajatelja;
h) lokacijo, na kateri je potrdilo, ki podpira kvalificirani elektronski podpis ali kvalificirani elektronski žig iz točke (g), na voljo brezplačno;
i) informacije o storitvah ali lokacijo storitev, s katerimi je mogoče preveriti veljavnost potrdila.