2024/1183

30.4.2024

UREDBA (EU) 2024/1183 EVROPSKEGA PARLAMENTA IN SVETA

z dne 11. aprila 2024

o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo evropskega okvira za 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]),

ob upoštevanju mnenja Odbora regij ([2]),

v skladu z rednim zakonodajnim postopkom ([3]),

ob upoštevanju naslednjega:

(1) V sporočilu Komisije z dne 19. februarja 2020 z naslovom „Oblikovanje digitalne prihodnosti Evrope“ je napovedana revizija Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta ([4]) za izboljšanje njene učinkovitosti, razširitev njene koristi na zasebni sektor ter spodbujanje zaupanja vrednih digitalnih identitet za vse Evropejce.

(2) Evropski svet je v svojih sklepih z dne 1. in 2. oktobra 2020 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 programu politike Digitalno desetletje do leta 2030, vzpostavljenim s Sklepom (EU) 2022/2481 Evropskega parlamenta in Sveta ([5]), so določeni digitalni cilji okvira Unije, ki naj bi do leta 2030 omogočili široko uporabo zaupanja vredne in prostovoljne digitalne identitete pod nadzorom uporabnika, ki je priznana po vsej Uniji in vsakemu uporabniku omogoča nadzor nad njegovimi podatki v spletnih interakcijah.

(4) V Evropski deklaraciji o digitalnih pravicah in načelih za digitalno desetletje, ki so jo razglasili Evropski parlament, Svet in Komisija ([6]) (v nadaljnjem besedilu: Deklaracija), je poudarjena pravica vseh do dostopa do digitalnih tehnologij, izdelkov in storitev, ki so po zasnovi varni in zaščiteni ter varujejo zasebnost. To pomeni tudi, da bo vsem ljudem, ki živijo v Uniji, ponujena dostopna, varna in zaupanja vredna digitalna identiteta, ki jim bo omogočila dostop do široke palete spletnih in nespletnih storitev in ki je zaščitena pred tveganji za kibernetsko varnost in kibernetsko kriminaliteto, vključno s kršitvami varnosti podatkov in krajo identitete ali manipuliranjem z njo. V Deklaraciji je zapisano tudi, da ima vsakdo pravico do varstva svojih osebnih podatkov. Ta pravica vključuje nadzor nad tem, kako se podatki uporabljajo in s kom se izmenjujejo.

([1]) UL C 105, 4.3.2022, str. 81.
([2]) UL C 61, 4.2.2022, str. 42.
([3]) Stališče Evropskega parlamenta z dne 29. februarja 2024 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 26. marca 2024.
([4]) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73).
([5]) Sklep (EU) 2022/2481 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o vzpostavitvi programa politike Digitalno desetletje do leta 2030 (UL L 323, 19.12.2022, str. 4).
([6]) UL C 23, 23.1.2023, str. 1.

(5) Državljani in rezidenti Unije bi morali imeti pravico do digitalne identitete pod svojim izključnim nadzorom, ki jim omogoča uresničevanje pravic, ki jih imajo v digitalnem okolju, ter udeležbo v digitalnem gospodarstvu. Za doseganje tega cilja bi bilo treba vzpostaviti evropski okvir za digitalno identiteto, ki bi državljanom in rezidentom Unije omogočal dostop do javnih in zasebnih spletnih in nespletnih storitev po vsej Uniji.

(6) Usklajen okvir za digitalno identiteto bi moral prispevati k ustvarjanju bolj digitalno povezane Unije tako, da bi zmanjšal digitalne ovire med državami članicami ter državljane in rezidente Unije opolnomočal, da izkoristijo prednosti digitalizacije, hkrati pa bi povečal preglednost in varstvo njihovih pravic.

(7) Bolj usklajen pristop k elektronski identifikaciji bi moral zmanjšati tveganja in znižati stroške sedanje razdrobljenosti zaradi uporabe različnih nacionalnih rešitev ali neobstoja takih rešitev elektronske identifikacije v nekaterih državah članicah. Tak pristop naj bi okrepil notranji trg, tako da bi državljanom in rezidentom Unije, kot so opredeljeni v nacionalnem pravu, in podjetjem omogočil, da se identificirajo ter zagotovijo spletno in nespletno avtentikacijo svoje identitete na varen, zaupanja vreden, uporabniku prijazen, priročen, dostopen in usklajen način po vsej Uniji. Evropska denarnica za digitalno identiteto bi morala fizičnim in pravnim osebam po vsej Uniji zagotoviti harmonizirano sredstvo elektronske identifikacije, ki omogoča 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 elektronskih potrdilih o atributih, kot so akademske kvalifikacije, vključno z univerzitetnimi diplomami, ali drugi izobraževalni oziroma poklicni dosežki. Evropski okvir za digitalno identiteto naj bi uresničil prehod z zanašanja samo na nacionalne rešitve digitalne identitete na zagotavljanje elektronskih potrdil o atributih, veljavnih in zakonsko priznanih po vsej Uniji. Ponudniki elektronskih potrdil o atributih bi morali imeti koristi od jasnih in enotnih pravil, javnim upravam pa bi moralo biti omogočeno, da se zanesejo na elektronske dokumente v določeni obliki.

(8) Več držav članic je uvedlo in uporablja sredstva elektronske identifikacije, ki jih ponudniki storitev v Uniji sprejemajo. Poleg tega so bile izvedene naložbe v nacionalne in čezmejne rešitve na podlagi Uredbe (EU) št. 910/2014, vključno z interoperabilnostjo priglašenih shem elektronske identifikacije na podlagi navedene uredbe. 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 učinek na obstoječe ponudnike storitev, bi bilo treba pri evropskih denarnicah za digitalno identiteto izkoristiti izkušnje, pridobljene na podlagi uporabe obstoječih sredstev elektronske identifikacije, ter infrastrukturo za priglašene sheme elektronske identifikacije, vzpostavljeno na ravni Unije in nacionalni ravni.

(9) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta ([7]) in, kadar je ustrezno, Direktiva 2002/58/ES Evropskega parlamenta in Sveta ([8]) se uporabljata za vse dejavnosti obdelave osebnih podatkov na podlagi Uredbe (EU) št. 910/2014. Rešitve na podlagi interoperabilnostnega okvira iz te uredbe so prav tako skladne s temi pravili. Pravo Unije o varstvu podatkov določa načela varstva podatkov, kot je načelo najmanjšega obsega podatkov in načelo omejitve namena, ter obveznosti, kot je vgrajeno in privzeto varstvo podatkov.

(10) Za podpiranje konkurenčnosti podjetij v Uniji bi moralo biti ponudnikom spletnih in nespletnih storitev omogočeno, da se zanašajo na rešitve digitalne identitete, priznane po vsej Uniji, ne glede na državo članico, v kateri se te rešitve zagotavljajo, ter tako izkoriščajo usklajen pristop Unije k zaupanju, varnosti in interoperabilnosti. Uporabniki in ponudniki storitev bi morali imeti koristi od enake pravne veljave, ki je zagotovljena elektronskim potrdilom o atributih po vsej Uniji. Z usklajenim okvirom za digitalno identiteto naj bi se omogočilo ustvarjanje ekonomske vrednosti, tako da se olajša dostop do blaga in storitev in znatno zmanjšajo operativni stroški, povezani s postopki elektronske identifikacije in avtentikacije, na primer pri postopkih pristopa novih strank, ter da se zmanjšajo možnosti za kibernetsko kriminaliteto, kot so kraja identitete, kraja podatkov in spletne goljufije, s čimer bi se spodbujala čim večja učinkovitost in varna digitalna preobrazba mikro, malih in srednjih podjetij Unije (MSP).

([7]) 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).

([8]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

(11) Evropske denarnice za digitalno identiteto bi morale olajšati uporabo načela „samo enkrat“, s čimer bi se zmanjšalo upravno breme in podprla čezmejna mobilnost državljanov in rezidentov Unije ter podjetij po vsej Uniji ter spodbujalo razvoj interoperabilnih storitev e-uprave po vsej Uniji.

(12) Uredba (EU) 2016/679, Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta ([9]) ter Direktiva 2002/58/ES se uporabljajo za obdelavo osebnih podatkov pri izvajanju te uredbe. Zato bi morali biti v tej uredbi določeni posebni zaščitni ukrepi, ki bi ponudnikom sredstev elektronske identifikacije in elektronskih potrdil o atributih preprečevali združevanje osebnih podatkov, pridobljenih pri zagotavljanju drugih storitev, z osebnimi podatki, obdelanimi za namene zagotavljanja storitev, ki spadajo na področje uporabe te uredbe. Osebni podatki povezani z zagotavljanjem evropskih denarnic za digitalno identiteto bi se morali na logičen način hraniti ločeni od vseh drugih podatkov, ki jih hrani ponudnik evropske denarnice za digitalno identiteto. Ta uredba ponudnikom evropskih denarnic za digitalno identiteto ne bi smela preprečevati uporabe dodatnih tehničnih ukrepov, ki prispevajo k varstvu osebnih podatkov, kot je fizično ločevanje osebnih podatkov povezanih z zagotavljanjem evropskih denarnic za digitalno identiteto od vseh drugih podatkov, ki jih ponudnik hrani. Ta uredba brez poseganja v Uredbo (EU) 2016/679 nadalje določa uporabo načel omejitve namena, najmanjšega obsega podatkov ter vgrajenega in privzetega varstva podatkov.

(13) Evropske denarnice za digitalno identiteto bi morale imeti že vgrajeno skupno nadzorno ploščo, da se zagotovijo boljša preglednost, večja zasebnost ter boljši nadzor uporabnikov nad njihovimi osebnimi podatki. Ta funkcija bi morala ponujati enostaven uporabniku prijazen vmesnik s pregledom nad vsemi zanašajočimi se strankami, s katerimi uporabnik izmenjuje podatke, vključno z atributi, ter nad vrsto podatkov, ki jih je izmenjal z vsako od zanašajočih se strank. Uporabnikom bi morala omogočiti spremljanje vseh transakcij, izvedenih z evropskimi denarnicami za digitalno identiteto, in vključevati vsaj naslednje podatke: čas in datum transakcije, identifikacijo druge strani, zahtevane osebne podatke in izmenjane podatke. Te informacije bi bilo treba shraniti, tudi če transakcija ni bila zaključena. Ne bi smelo biti mogoče zanikati verodostojnosti informacij iz zgodovine transakcij. Ta funkcija bi morala biti privzeto vključena. Uporabnikom bi morala omogočati, da neposredno prek evropske denarnice za digitalno identiteto na preprost način zahtevajo, da zanašajoča stranka nemudoma izbriše osebne podatke na podlagi člena 17 Uredbe (EU) 2016/679 in da zanašajočo se stranko preprosto prijavijo pristojnemu nacionalnemu organu za varstvo podatkov, kadar pride do prejema domnevno nezakonitih ali sumljivih zahtev za osebne podatke.

(14) Države članice bi morale v evropsko denarnico za digitalno identiteto vključiti različne tehnologije za ohranjanje zasebnosti, kot je dokaz brez razkritja znanja. Te kriptografske metode bi morale zanašajoči se stranki omogočiti, da potrdi, ali je določena izjava, ki temelji na identifikacijskih podatkih in potrdilih o atributih osebe, resnična, ne da bi razkrila kakršne koli podatke, na katerih temelji navedena izjava, s čimer bi se ohranila zasebnost uporabnika.

(15) Ta uredba določa usklajene pogoje za vzpostavitev okvira za evropske denarnice za digitalno identiteto, ki naj bi jih zagotavljale države članice. Vsi državljani in rezidenti Unije, kakor so opredeljeni v nacionalnem pravu, bi morali imeti možnost, da na varen način zahtevajo, izbirajo, združujejo, shranjujejo, brišejo, izmenjujejo in predstavljajo podatke, povezane z njihovo identiteto, ter zahtevajo izbris svojih osebnih podatkov na uporabniku prijazen in priročen način pod izključnim nadzorom uporabnika, hkrati pa omogočajo selektivno razkrivanje osebnih podatkov. Ta uredba odraža skupne evropske vrednote in spoštuje temeljne pravice, pravna jamstva in odgovornost ter tako ščiti demokratične družbe, državljane in rezidente Unije. Razviti bi bilo treba tehnologije, ki bi se uporabljale za uresničevanje teh ciljev ter bi bile namenjene doseganju najvišje ravni varnosti, zasebnosti, priročnosti za uporabnike, dostopnosti, široke uporabnosti in nemotene interoperabilnosti. Države članice bi morale vsem svojim državljanom in rezidentom zagotoviti enak dostop do elektronske identifikacije. Države članice ne bi smele neposredno ali posredno omejevati dostopa do javnih ali zasebnih storitev za fizične ali pravne osebe, ki se ne odločijo za uporabo evropskih denarnic za digitalno identiteto, in bi morale dati na voljo ustrezne alternativne rešitve.

([9]) 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).

(16) Države članice bi morale izkoristiti možnosti v okviru te uredbe, da bi v skladu s svojo odgovornostjo zagotovile evropske denarnice za digitalno identiteto, ki bi jih uporabljale fizične in pravne osebe, ki prebivajo na njihovem ozemlju. Da bi državam članicam omogočili prilagodljivost in izkoristili najsodobnejšo tehnologijo, bi morala ta uredba omogočiti, da se evropske denarnice za digitalno identiteto zagotovijo neposredno s strani države članice, na podlagi pooblastila države članice ali neodvisno od države članice, vendar z njenim priznanjem.

(17) Zanašajoče se stranke bi morale za namene registracije zagotoviti informacije, ki so potrebne za njihovo elektronsko identifikacijo in avtentikacijo v okviru evropskih denarnic za digitalno identiteto. Pri prijavi njihove nameravane uporabe evropske denarnice za digitalno identiteto bi morale zagotoviti informacije o morebitnih podatkih, ki jih bodo zahtevale za opravljanje svojih storitev, ter razloge za to zahtevo. Registracija zanašajočih se strank državam članicam olajša preverjanje glede zakonitosti dejavnosti teh strank v skladu s pravom Unije. Obveznost registracije iz te uredbe ne bi smela posegati v obveznosti, določene v drugem pravu Unije ali nacionalnem pravu, kot so informacije, ki jih je treba zagotoviti posameznikom, na katere se nanašajo osebni podatki, na podlagi Uredbe (EU) 2016/679. Zanašajoče se stranke bi morale ravnati v skladu z zaščitnimi ukrepi iz členov 35 in 36 navedene uredbe, zlasti tako, da izvedejo ocene učinka v zvezi z varstvom podatkov ter se posvetujejo s pristojnimi organi za varstvo podatkov pred obdelavo podatkov, kadar ocene učinka v zvezi z varstvom podatkov kažejo, da bi obdelava povzročila veliko tveganje. Tovrstni zaščitni ukrepi bi morali podpirati zakonito obdelavo osebnih podatkov s strani zanašajočih se strank, zlasti v zvezi s posebnimi vrstami podatkov, kot so zdravstveni podatki. Registracija zanašajočih se strank naj bi povečala preglednost in zaupanje v uporabo evropskih denarnic za digitalno identiteto. Registracija bi morala biti stroškovno učinkovita in sorazmerna s povezanimi tveganji, da se zagotovi uporaba s strani ponudnikov storitev. Tozadevno bi morala registracija omogočati uporabo avtomatiziranih postopkov, med drugim tako, da bi se države članice opirale na obstoječe registre in jih uporabljale, in ne bi smela vključevati postopka predhodne odobritve. Postopek registracije bi moral omogočati različne primere uporabe, ki se lahko razlikujejo glede načina delovanja, in sicer spletni ali nespletni način, ali v smislu zahtev glede avtentikacije naprav za namene povezovanja z evropsko denarnico za digitalno identiteto. Registracija bi se morala zahtevati izključno pri zanašajočih se strankah, ki zagotavljajo storitve na podlagi digitalne interakcije.

(18) Zaščita državljanov in rezidentov Unije pred nedovoljeno ali goljufivo uporabo evropskih denarnic za digitalno identiteto je zelo pomembna za zagotavljanje zaupanja v evropske denarnice za digitalno identiteto in njihovo široko uporabo. Uporabnikom bi bilo treba zagotoviti učinkovito zaščito pred takšno zlorabo. Zlasti kadar nacionalni pravosodni organ v okviru drugega postopka ugotovi dejstva, ki tvorijo podlago za goljufivo ali drugače nezakonito uporabo evropske denarnice za digitalno identiteto, bi morali nadzorni organi, pristojni za izdajatelje evropske denarnice za digitalno identiteto, po prejetju uradnega obvestila sprejeti potrebne ukrepe za zagotovitev, da se registracija zanašajočih se strank in njihova vključitev v mehanizem avtentikacije prekličeta ali začasno prekineta, dokler priglasitveni organ ne potrdi, da so bile ugotovljene nepravilnosti odpravljene.

(19) Vse evropske denarnice za digitalno identiteto bi morale uporabnikom omogočiti, da se čezmejno elektronsko identificirajo in avtenticirajo v spletnem in nespletnem načinu, da lahko dostopajo do različnih javnih in zasebnih storitev. Brez poseganja v pristojnosti držav članic, kar zadeva identifikacijo njihovih državljanov in rezidentov, se lahko evropske denarnice za digitalno identiteto uporabljajo tudi za institucionalne potrebe javnih uprav, mednarodnih organizacij ter institucij, organov, uradov in agencij Unije. Avtentikacija v nespletnem načinu bi bila pomembna v številnih sektorjih, vključno z zdravstvenim, v katerem se storitve pogosto zagotavljajo z osebno interakcijo, pri e-receptih pa bi morala biti omogočena uporaba kod QR ali podobnih tehnologij za preverjanje avtentičnosti. Evropske denarnice za digitalno identiteto bi morale za izpolnitev varnostnih zahtev iz te uredbe izkoristiti potencial rešitev za zaščito pred nedovoljenimi posegi, kot so varnostni elementi, pri čemer se zanašajo na visoko raven zanesljivosti v zvezi s shemami elektronske identifikacije. Evropske denarnice za digitalno identiteto bi morale uporabnikom omogočati tudi ustvarjanje in uporabo kvalificiranih elektronskih podpisov in žigov, sprejetih po vsej Uniji. Ko je fizičnim osebam omogočen pristop k uporabi evropske denarnice za digitalno identiteto, bi morale imeti možnost, da jo uporabljajo kot privzet in brezplačen način za podpisovanje s kvalificiranimi elektronskimi podpisi, ne da bi jim bilo treba opraviti dodatne upravne postopke. Uporabniki bi morali imeti možnost, da podpišejo ali ožigosajo svoje izjave ali atribute. Za poenostavitev in koriščenje ugodnosti znižanja stroškov za osebe in podjetja po vsej Uniji, tudi z omogočanjem pooblastil za zastopanje in mandatov v elektronski obliki, bi morale države članice zagotavljati evropske denarnice za digitalno identiteto, ki temeljijo na skupnih standardih in tehničnih specifikacijah, da bi zagotovile nemoteno interoperabilnost in ustrezno povečale varnost informacijske tehnologije, okrepile odpornost na kibernetske napade in tako znatno zmanjšale morebitna tveganja sedanjega procesa digitalizacije za državljane in rezidente Unije ter podjetja. Visoko stopnjo zaupanja v ugotavljanje

identitete osebe lahko zagotovijo le pristojni organi držav članic, s čimer zagotovijo, da je oseba, ki izkazuje ali uveljavlja določeno identiteto, dejansko oseba, za katero se izkazuje. Zato se je treba pri zagotavljanju evropskih denarnic za digitalno identiteto zanašati na zakonsko veljavno identiteto državljanov in rezidentov Unije ali pravnih oseb. Zanašanje na zakonsko veljavno identiteto uporabnikov evropske denarnice za digitalno identiteto ne bi smelo ovirati pri dostopu do storitev z uporabo psevdonima, kadar za avtentikacijo zakonsko veljavna identiteta ni zakonsko zahtevana. Zaupanje v evropske denarnice za digitalno identiteto bi bilo okrepljeno, če bi strani izdajatelja in upravitelja morale izvajati ustrezne tehnične in organizacijske ukrepe za zagotovitev najvišje ravni varnosti, ki je sorazmerna s tveganji za pravice in svoboščine fizičnih oseb, v skladu z Uredbo (EU) 2016/679.

(20) Uporaba kvalificiranega elektronskega podpisa bi morala biti brezplačna za vse fizične osebe, kadar gre za nepoklicne namene. Države članice bi morale imeti možnost, da določijo ukrepe, s katerimi bi fizičnim osebam preprečile brezplačno uporabo kvalificiranih elektronskih podpisov v poklicne namene, hkrati pa zagotovile, da so vsi taki ukrepi sorazmerni z ugotovljenimi tveganji in upravičeni.

(21) Koristno bi bilo evropske denarnice za digitalno identiteto brezhibno vključiti v ekosistem javnih in zasebnih digitalnih storitev, ki se že izvajajo na nacionalni, lokalni ali regionalni ravni, ter tako olajšati uvajanje in uporabo teh denarnic. Za dosego tega cilja bi morale države članice imeti možnost določiti pravne in organizacijske ukrepe, da bi povečale prilagodljivost za ponudnike evropskih denarnic za digitalno identiteto in omogočile dodatne funkcionalnosti evropskih denarnic za digitalno identiteto, poleg že določenih funkcionalnosti iz te uredbe, med drugim z večjo interoperabilnostjo z obstoječimi nacionalnimi sredstvi elektronske identifikacije. Take dodatne funkcionalnosti nikakor ne bi smele ovirati zagotavljanja osnovnih funkcij evropskih denarnic za digitalno identiteto, določenih v tej uredbi, ali prednostno spodbujati obstoječih nacionalnih rešitev namesto evropskih denarnic za digitalno identiteto. Ker take dodatne funkcionalnosti presegajo to uredbo, se zanje ne uporabljajo določbe o čezmejni uporabi evropskih denarnic za digitalno identiteto iz te uredbe.

(22) Evropske denarnice za digitalno identiteto bi morale vključevati funkcionalnost za ustvarjanje psevdonimov, ki jih uporabniki sami izberejo in upravljajo, za namene avtentikacije pri dostopu do spletnih storitev.

(23) Za doseganje visoke ravni varnosti in zaupanja ta uredba določa zahteve za evropske denarnice za digitalno identiteto. Skladnost evropskih denarnic za digitalno identiteto s temi zahtevami bi morali certificirati akreditirani organi za ugotavljanje skladnosti, ki jih imenujejo države članice.

(24) Da bi se izognili različnim pristopom in uskladili izvajanje zahtev iz te uredbe, bi morala Komisija za namen certificiranja evropskih denarnic za digitalno identiteto sprejeti izvedbene akte za vzpostavitev seznama referenčnih standardov ter po potrebi določiti specifikacije in postopke za namen opredelitve podrobnih tehničnih specifikacij navedenih zahtev. Če certificiranje skladnosti evropskih denarnic za digitalno identiteto z ustreznimi zahtevami glede kibernetske varnosti ni zajeto v obstoječih certifikacijskih shemah za kibernetsko varnost iz te uredbe, ter v primeru zahtev, ki niso povezane s kibernetsko varnostjo in se nanašajo na evropske denarnice za digitalno identiteto, bi morale države članice vzpostaviti nacionalne certifikacijske sheme na podlagi usklajenih zahtev, določenih v tej uredbi in sprejetih na podlagi te uredbe. Države članice bi morale svoje osnutke nacionalnih certifikacijskih shem posredovati skupini za sodelovanje na področju evropske digitalne identitete, ki bi morala imeti možnost izdati mnenja in priporočila.

(25) Certificiranje skladnosti z zahtevami glede kibernetske varnosti iz te uredbe bi moralo, kadar je na voljo, temeljiti na ustreznih evropskih certifikacijskih shemah za kibernetsko varnost, vzpostavljenih na podlagi Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta ([10]), ki vzpostavlja prostovoljni evropski certifikacijski okvir za kibernetsko varnost za proizvode, postopke in storitve IKT.

([10]) 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).

(26) Da bi stalno ocenjevali in zmanjševali tveganja, povezana z varnostjo, bi morale biti certificirane evropske denarnice za digitalno identiteto predmet rednih ocen ranljivosti, da bi odkrili morebitne ranljivosti v certificiranih komponentah evropske denarnice za digitalno identiteto, povezanih s proizvodi, postopki in storitvami.

(27) Bistvene zahteve glede kibernetske varnosti iz te uredbe z zaščito uporabnikov in podjetij pred tveganji za kibernetsko varnost prispevajo tudi k izboljšanju varstva osebnih podatkov in zasebnosti posameznikov. V okviru sodelovanja med Komisijo, evropskimi organizacijami za standardizacijo, Agencijo Evropske unije za kibernetsko varnost (ENISA), Evropskim odborom za varstvo podatkov, ustanovljenim z Uredbo (EU) 2016/679, in nacionalnimi nadzornimi organi za varstvo podatkov bi bilo treba obravnavati sinergije glede standardizacije in certificiranja v zvezi z vidiki kibernetske varnosti.

(28) Pristop državljanov in rezidentov Unije k uporabi evropske denarnice 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, kadar usklajene tehnične specifikacije in postopki, pri katerih se uporabljajo sredstva elektronske identifikacije, izdana s srednjo ravnjo zanesljivosti, v kombinaciji z dodatnimi sredstvi za preverjanje identitete omogočajo izpolnjevanje zahtev glede visoke ravni zanesljivosti iz te uredbe. Taka dodatna sredstva bi morala biti zanesljiva in enostavna za uporabo ter bi lahko temeljila na možnosti uporabe postopkov pristopa na daljavo, kvalificiranih potrdil, podprtih s kvalificiranimi elektronskimi 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 usklajene tehnične specifikacije in postopke za pristop uporabnikov z uporabo sredstev elektronske identifikacije, vključno s tistimi, ki se izdajo na srednji ravni zanesljivosti.

(29) Cilj te uredbe je uporabniku zagotoviti popolnoma mobilno, varno in njemu prijazno evropsko denarnico za digitalno identiteto. Kot prehodni ukrep bi se morali za evropske denarnice za digitalno identiteto, dokler ne bodo na voljo certificirane rešitve, zaščitene pred nedovoljenimi posegi, na primer varnostni elementi v napravah uporabnikov, uporabljati certificirani zunanji varnostni elementi za zaščito kriptografskega materiala in drugih občutljivih podatkov ali priglašena sredstva elektronske identifikacije z visoko ravnjo zanesljivosti, da se dokaže skladnost z ustreznimi zahtevami iz te uredbe v zvezi z ravnjo zanesljivosti evropske denarnice za digitalno identiteto. Ta uredba ne bi smela posegati v nacionalne pogoje v zvezi z izdajo in uporabo certificiranega zunanjega varnostnega elementa, kadar prehodni ukrep temelji na njem.

(30) Evropske denarnice za digitalno identiteto bi morale zagotoviti najvišjo raven varstva in varnosti podatkov za namene elektronske identifikacije in avtentikacije, da se olajša dostop do javnih in zasebnih storitev, ne glede na to, ali se taki podatki hranijo lokalno ali v rešitvah v oblaku, ob ustreznem upoštevanju različnih ravni tveganja.

(31) Evropske denarnice za digitalno identiteto bi morale imeti vgrajeno varnost in bi morale uvajati napredne varnostne elemente za zaščito pred krajo identitete in drugih podatkov, zavrnitvijo storitve in vsemi drugimi kibernetskimi grožnjami. Taki varnostni elementi bi morali vključevati najsodobnejše metode šifriranja in shranjevanja, do katerih lahko dostopa in ki jih lahko dešifrira izključno uporabnik ter ki temeljijo na šifrirani komunikaciji od konca do konca z drugimi evropskimi denarnicami za digitalno identiteto in zanašajočimi se strankami. Poleg tega bi bilo treba za evropske denarnice za digitalno identiteto zahtevati varno, izrecno in aktivno potrditev uporabnika za operacije, ki se izvajajo prek evropskih denarnic za digitalno identiteto.

(32) Brezplačna uporaba evropskih denarnic za digitalno identiteto ne bi smela povzročiti obdelave podatkov, ki bi presegala podatke, ki so potrebni za zagotavljanje storitev evropske denarnice za digitalno identiteto. Ta uredba ponudniku evropske denarnice za digitalno identiteto ne bi smela omogočati obdelave osebnih podatkov, ki so shranjeni v evropski denarnici za digitalno identiteto ali so pridobljeni na podlagi njene uporabe, za namene, ki niso zagotavljanje storitev evropske denarnice za digitalno identiteto. Za zagotavljanje zasebnosti bi morali ponudniki evropske denarnice za digitalno identiteto zagotoviti, da uporabnikom ni mogoče slediti, tako da ne zbirajo podatkov in nimajo vpogleda v transakcije uporabnikov evropske denarnice za digitalno identiteto. To, da uporabnikom ni mogoče slediti, pomeni, da ponudniki ne morejo videti podrobnosti o transakcijah, ki jih je opravil uporabnik. Vendar bi se lahko ponudnikom evropskih denarnic za digitalno identiteto v posebnih primerih na podlagi izrecne predhodne privolitve uporabnika v vsakem od teh posebnih primerov in popolnoma v skladu

z Uredbo (EU) 2016/679 odobril dostop do informacij, potrebnih za zagotavljanje določene storitve, povezane z evropskimi denarnicami za digitalno identiteto.

(33) Preglednost evropskih denarnic za digitalno identiteto in odgovornost njihovih ponudnikov sta ključna elementa za ustvarjanje družbenega zaupanja in spodbujanje sprejemanja okvira. Delovanje evropskih denarnic za digitalno identiteto bi moralo biti zato pregledno in zlasti omogočati preverljivo obdelavo osebnih podatkov. Za doseganje tega bi morale države članice razkriti izvorno kodo komponent uporabniške aplikacijske programske opreme evropske denarnice za digitalno identiteto, tudi tisto, ki je povezana z obdelavo osebnih podatkov in podatkov pravnih oseb. Objava te izvorne kode na podlagi odprtokodne licence bi morala družbi, tudi uporabnikom in razvijalcem, omogočiti razumevanje njenega delovanja ter revizijo in pregled kode. To bi povečalo zaupanje uporabnikov v ekosistem in prispevalo k varnosti evropskih denarnic za digitalno identiteto, saj bi imel vsakdo možnost prijaviti ranljivosti in napake v kodi. To bi moralo na splošno spodbujati dobavitelje, da dobavijo in vzdržujejo zelo varen izdelek. Vendar bi v določenih primerih države članice iz ustrezno utemeljenih razlogov, zlasti zaradi javne varnosti, lahko omejile razkritje izvorne kode za uporabljene knjižnice, komunikacijski kanal ali druge elemente, ki ne gostujejo na uporabniški napravi.

(34) Uporaba evropskih denarnic za digitalno identiteto in prenehanje njihove uporabe bi morala biti izključna pravica in izbira uporabnikov. Države članice bi morale razviti enostavne in varne postopke, s katerimi lahko uporabniki zahtevajo takojšen preklic veljavnosti evropskih denarnic za digitalno identiteto, tudi v primeru izgube ali kraje. Ob smrti uporabnika ali prenehanju dejavnosti pravne osebe bi bilo treba vzpostaviti mehanizem, ki bi organu, pristojnemu za urejanje dedovanja fizične osebe ali premoženja pravne osebe, omogočil, da zahteva takojšen preklic evropske denarnice za digitalno identiteto.

(35) Da bi spodbudile uporabo evropskih denarnic za digitalno identiteto in širšo uporabo digitalnih identitet, bi morale države članice ne le spodbujati prednosti ustreznih storitev, temveč bi morale v sodelovanju z zasebnim sektorjem, raziskovalci in akademskimi krogi tudi razviti programe usposabljanja, namenjene krepitvi digitalnih spretnosti svojih državljanov in rezidentov, zlasti ranljivih skupin, kot so invalidi in starejši. Države članice bi morale prav tako s komunikacijskimi kampanjami ozaveščati o koristih in tveganjih evropskih denarnic za digitalno identiteto.

(36) Za zagotovitev, da je evropski okvir za digitalno identiteto odprt za inovacije in tehnološki razvoj ter pripravljen na izzive prihodnosti, se države članice spodbujajo 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 MSP, zagonskih podjetij ter posameznih inovatorjev in raziskovalcev ter ustreznih deležnikov iz industrije. Take pobude bi morale prispevati k usklajenosti s predpisi in tehnični stabilnosti evropskih denarnic za digitalno identiteto, ki se zagotovijo državljanom in rezidentom Unije, ter ju okrepiti, s čimer bi se preprečil razvoj rešitev, ki niso skladne s pravom Unije o varstvu podatkov oziroma ki so izpostavljene ranljivostim na področju varnosti.

(37) Uredba (EU) 2019/1157 Evropskega parlamenta in Sveta [11] krepi varnost osebnih izkaznic z izboljšanimi varnostnimi elementi do avgusta 2021. Države članice bi morale preučiti možnost njihove priglasitve v okviru shem elektronske identifikacije za razširitev čezmejne razpoložljivosti sredstev elektronske identifikacije.

(38) Postopek priglasitve shem elektronske identifikacije bi bilo treba poenostaviti in pospešiti za spodbujanje dostopa do priročnih, zaupanja vrednih, varnih in inovativnih rešitev avtentikacije in identifikacije ter, kadar je ustrezno, za spodbujanje zasebnih ponudnikov identitete, naj organom države članice ponujajo sheme elektronske identifikacije za priglasitev kot nacionalne sheme elektronske identifikacije na podlagi Uredbe (EU) št. 910/2014.

[11] 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).

(39) 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 so namenjeni spodbujanju sodelovanja držav članic na področju varnosti in interoperabilnosti njihovih priglašenih shem elektronske identifikacije.

(40) Države članice bi morale imeti koristi od novih prilagodljivih orodij za zagotavljanje izpolnjevanja zahtev iz te uredbe in ustreznih izvedbenih aktov, sprejetih na podlagi te uredbe. Ta uredba bi morala državam članicam omogočati uporabo poročil in ocen, ki jih izvedejo akreditirani organi za ugotavljanje skladnosti, kot je določeno v okviru certifikacijskih shem, ki se morajo vzpostaviti na ravni Unije na podlagi Uredbe (EU) 2019/881, v podporo njihovim zahtevam po uskladitvi shem ali njihovih delov z Uredbo (EU) št. 910/2014.

(41) Ponudniki javnih storitev uporabljajo identifikacijske podatke osebe, dostopne v okviru sredstev elektronske identifikacije na podlagi Uredbe (EU) št. 910/2014, da elektronsko identiteto uporabnikov iz drugih držav članic primerjajo z identifikacijskimi podatki osebe, zagotovljenim tem uporabnikom v državi članici, ki izvaja postopek čezmejnega ujemanja identitete. Vendar so v številnih primerih kljub uporabi minimalnega nabora podatkov, zagotovljenega v okviru priglašenih shem elektronske identifikacije, za zagotovitev natančnega ujemanja identitete, kadar države članice delujejo kot zanašajoče se stranke, potrebne dodatne informacije o uporabniku in posebni dopolnilni enolični postopki identifikacije, ki jih je treba izvesti na nacionalni ravni. Da bi dodatno podprli uporabnost sredstev elektronske identifikacije, zagotovili boljše spletne javne storitve in povečali pravno varnost v zvezi z elektronsko identiteto uporabnikov, bi bilo treba v Uredbi (EU) št. 910/2014 od držav članic zahtevati, da sprejmejo posebne spletne ukrepe za zagotovitev nedvoumnega ujemanja identitete, kadar nameravajo uporabniki dostopati do čezmejnih spletnih javnih storitev.

(42) Pri razvoju evropskih denarnic za digitalno identiteto je bistvenega pomena, da se upoštevajo potrebe uporabnikov. Na voljo bi morali biti smiselni primeri uporabe in spletne storitve, ki bi temeljile na evropskih denarnicah za digitalno identiteto. Zaradi večje priročnosti 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 bi temeljile na evropskih denarnicah za digitalno identiteto, bi lahko pripomogle k doseganju navedenega cilja. Take smernice bi bilo treba pripraviti ob upoštevanju interoperabilnostnega okvira Unije. Pri sprejemanju teh smernic bi morale imeti glavno vlogo države članice.

(43) V skladu z Direktivo (EU) 2019/882 Evropskega parlamenta in Sveta ([12]) 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, enako kot drugim uporabnikom.

(44) Za zagotavljanje učinkovitega izvrševanja te uredbe bi bilo treba določiti najnižjo mejo za najvišje globe za ponudnike kvalificiranih in nekvalificiranih storitev zaupanja. Države članice bi morale zagotoviti učinkovite, sorazmerne in odvračilne kazni. Pri določanju kazni bi bilo treba ustrezno upoštevati velikost prizadetih subjektov, njihove poslovne modele in resnost kršitev.

(45) Države članice bi morale določiti pravila o kaznih za kršitve, kot so neposredne ali posredne prakse, ki povzročajo zmedo glede tega, katere storitve zaupanja so nekvalificirane ali kvalificirane, ali zlorabo znaka zaupanja EU s strani ponudnikov nekvalificiranih storitev zaupanja. Znak zaupanja EU se ne bi smel uporabljati v okoliščinah, ki neposredno ali posredno vzbujajo vtis, da so katere koli nekvalificirane storitve zaupanja, ki jih nudijo ti ponudniki storitev, kvalificirane.

(46) Ta uredba ne bi smela zajemati vidikov, povezanih s sklepanjem in veljavnostjo pogodb ali drugih pravnih obveznosti, kadar pravo Unije ali nacionalno pravo določa zahteve glede oblične sti. Poleg tega ne bi smela vplivati na nacionalne zahteve glede oblične sti, ki zadevajo javne registre, zlasti poslovne registre in zemljiške knjige.

([12]) 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).

(47) Zagotavljanje in uporaba storitev zaupanja ter koristi v smislu priročnosti in pravne varnosti v okviru čezmejnih transakcij, zlasti kadar se uporabljajo kvalificirane storitve zaupanja, postajata vse pomembnejša za mednarodno trgovino in sodelovanje. Mednarodni partnerji Unije vzpostavljajo okvire zaupanja, ki se zgledujejo po Uredbi (EU) št. 910/2014. Za lažje priznavanje kvalificiranih storitev zaupanja in njihovih ponudnikov lahko Komisija sprejme izvedbene akte, s katerimi določi pogoje, pod katerimi bi se okviri zaupanja tretjih držav lahko šteli za enakovredne okviru zaupanja za kvalificirane storitve zaupanja in njihove ponudnike iz te uredbe. Tak pristop bi moral dopolnjevati možnost vzajemnega priznavanja storitev zaupanja in njihovih ponudnikov s sedežem v Uniji in v tretjih državah v skladu s členom 218 Pogodbe o delovanju Evropske unije (PDEU). Pri določanju pogojev, pod katerimi bi se okviri zaupanja tretjih držav lahko šteli za enakovredne okviru zaupanja za kvalificirane storitve zaupanja in njihove ponudnike na podlagi Uredbe (EU) št. 910/2014, sta bistvena elementa za krepitev zaupanja tudi zagotavljanje skladnosti z ustreznimi določbami Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta ([13]) in Uredbe (EU) 2016/679 ter uporaba zanesljivih seznamov.

(48) Ta uredba bi morala spodbujati izbiro in možnost menjave med evropskimi denarnicami za digitalno identiteto, kadar je država članica na svojem ozemlju podprla več kot eno rešitev za evropske denarnice za digitalno identiteto. Da bi se v takih primerih izognili učinkom vezanosti, bi morali ponudniki evropskih denarnic za digitalno identiteto, kadar je to tehnično izvedljivo, zagotoviti učinkovito prenosljivost podatkov na zahtevo uporabnikov evropske denarnice za digitalno identiteto, ne bi pa jim smelo biti dovoljeno uporabljati pogodbenih, ekonomskih ali tehničnih ovir za preprečevanje ali odvračanje od učinkovite menjave med različnimi evropskimi denarnicami za digitalno identiteto.

(49) Za zagotavljanje pravilnega delovanja evropskih denarnic za digitalno identiteto je treba ponudnikom evropske denarnice za digitalno identiteto zagotavljati učinkovito interoperabilnost ter pravične, razumne in nediskriminatorne pogoje, da lahko evropske denarnice za digitalno identiteto dostopajo do posebnih funkcij strojne in programske opreme mobilnih naprav. Te komponente bi lahko vključevale zlasti antene za komunikacijo v bližnjem polju in varnostne elemente, vključno z univerzalnimi karticami z integriranim vezjem, vgrajenimi varnostnimi elementi, karticami mikroSD in nizkoenergijskim Bluetooth. Dostop do teh komponent bi lahko nadzorovali operaterji mobilnih omrežij in proizvajalci opreme. Zato proizvajalci originalne opreme za mobilne naprave ali ponudniki elektronskih komunikacijskih storitev ne bi smeli zavrniti dostopa do takih komponent, kadar je to potrebno za zagotavljanje storitev evropskih denarnic za digitalno identiteto. Poleg tega bi morale za podjetja, ki so imenovana za vratarje za jedrne platformne storitve, kot jih je Komisija uvrstila na seznam na podlagi Uredbe (EU) 2022/1925 Evropskega parlamenta in Sveta ([14]), še naprej veljati posebne določbe navedene uredbe, in sicer na podlagi člena 6(7) navedene uredbe.

(50) Za racionalizacijo obveznosti v zvezi s kibernetsko varnostjo, naloženih ponudnikom storitev zaupanja, ter za omogočanje tem ponudnikom in njihovim zadevnim pristojnim organom, da izkoristijo pravni okvir, vzpostavljen z Direktivo (EU) 2022/2555, morajo ponudniki storitev zaupanja sprejeti ustrezne tehnične in organizacijske ukrepe na podlagi navedene direktive, kot so ukrepi za obravnavanje okvar sistema, človeških napak, zlonamernih dejanj ali naravnih pojavov, za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih ti ponudniki uporabljajo pri zagotavljanju svojih storitev, ter za priglasitev pomembnih incidentov in kibernetskih groženj v skladu z navedeno direktivo. 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, poškodbe omrežnega kabla ali incidenti, ki se zgodijo v okviru identifikacije oseb. Za zahteve glede obvladovanja tveganj za kibernetsko varnost in obveznosti poročanja iz Direktive (EU) 2022/2555 bi se moralo šteti, da dopolnjujejo zahteve, naložene ponudnikom storitev zaupanja na podlagi te uredbe. Kadar je to ustrezno, bi morali pristojni organi, imenovani na podlagi Direktive (EU) 2022/2555, še naprej uporabljati uveljavljene nacionalne prakse ali smernice v zvezi z izvajanjem zahtev glede varnosti in poročanja ter nadzorom nad izpolnjevanjem takih zahtev na podlagi Uredbe (EU) št. 910/2014. Ta uredba ne vpliva na obveznost obveščanja o kršitvah varnosti osebnih podatkov na podlagi Uredbe (EU) 2016/679.

([13]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80).

([14]) Uredba (EU) 2022/1925 Evropskega parlamenta in Sveta z dne 14. septembra 2022 o tekmovalnih in pravičnih trgih v digitalnem sektorju in spremembi direktiv (EU) 2019/1937 in (EU) 2020/1828 (akt o digitalnih trgih) (UL L 265, 12.10.2022, str. 1).

(51) Ustrezno pozornost bi bilo treba nameniti zagotavljanju učinkovitega sodelovanja med nadzornimi organi, imenovanimi na podlagi člena 46b Uredbe (EU) št. 910/2014, in pristojnimi organi, imenovanimi ali ustanovljenimi na podlagi člena 8(1) Direktive (EU) 2022/2555. Kadar ta nadzorni organ ni tudi pristojni organ, bi morala ta organa tesno in pravočasno sodelovati na podlagi izmenjave ustreznih informacij, da se zagotovita učinkovit nadzor in izpolnjevanje zahtev iz Uredbe (EU) št. 910/2014 in Direktive (EU) 2022/2555 s strani ponudnikov storitev zaupanja. Zlasti bi morali imeti nadzorni organi, imenovani na podlagi Uredbe (EU) št. 910/2014, pravico, da od pristojnih organov, imenovanih ali ustanovljenih na podlagi Direktive (EU) 2022/2555, zahtevajo, naj predložijo ustrezne informacije, potrebne za dodelitev kvalificiranega statusa in izvajanje nadzornih ukrepov za preverjanje, ali ponudniki storitev zaupanja izpolnjujejo ustrezne zahteve iz Direktive (EU) 2022/2555, oziroma da od njih zahtevajo, da te zahteve izpolnijo.

(52) Bistvenega pomena je zagotoviti, 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 storitve elektronske priporočene dostave po vsej Uniji. 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 zagotavljanju interoperabilnosti njihovih storitev s kvalificiranimi storitvami elektronske priporočene dostave, ki jih zagotavljajo drugi ponudniki kvalificiranih storitev zaupanja, da bi se olajšal prenos podatkov, poslanih prek storitev elektronske priporočene dostave, med dvema ali več ponudniki kvalificiranih storitev zaupanja in spodbujale poštene prakse na notranjem trgu.

(53) V večini primerov si državljani in rezidenti Unije ne morejo varno in z visoko ravnjo varstva podatkov čezmejno izmenjevati digitalnih informacij, povezanih z njihovo identiteto, kot so njihov naslov, starost, poklicne kvalifikacije, vozniška in druga dovoljenja ter podatki o plačilih.

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

(55) Vsak ponudnik storitev, ki izdaja potrjene atribute v elektronski obliki, kot so diplome, spričevala, rojstni listi ali pooblastila in mandati za zastopanje fizičnih ali pravnih oseb oziroma delovanje v njihovem imenu, bi bilo treba šteti za ponudnika storitev zaupanja, ki izdaja elektronska potrdila o atributih. Elektronskim potrdilom o atributih se 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. Določiti bi bilo treba splošne zahteve za zagotovitev, da ima kvalificirano elektronsko potrdilo 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, ki opredeljuje dodatne posebne sektorske zahteve glede obličnosti in s tem povezane pravne učinke ter zlasti čezmejno priznavanje kvalificiranih elektronskih potrdil o atributih, kadar je to ustrezno.

(56) Široka razpoložljivost in uporabnost evropskih denarnic za digitalno identiteto bi morala izboljšati njihovo sprejemanje in zaupanje vanje tako pri fizičnih osebah kot pri zasebnih ponudnikih storitev. Zasebne zanašajoče se stranke, ki zagotavljajo storitve na primer na področjih prometa, energetike, bančništva in finančnih storitev, socialnega varstva, zdravja, pitne vode, poštnih storitev, digitalne infrastrukture, telekomunikacij ali izobraževanja, bi morale zato sprejeti uporabo evropskih denarnic za digitalno identiteto za zagotavljanje storitev, za katere pravo Unije ali nacionalno pravo ali pogodbena obveznost zahteva močno avtentikacijo uporabnika za spletno identifikacijo. Vsaka zahteva zanašajoče se stranke po informacijah od uporabnika evropske denarnice za digitalno identifikacijo bi morala biti potrebna za predvideno uporabo v danem primeru in sorazmerna z njo, bi morala biti skladna z načelom najmanjšega obsega podatkov in bi morala zagotavljati preglednost glede tega, kateri podatki se izmenjujejo in za katere namene. Da bi spodbudili uporabo in sprejemanje evropskih denarnic za digitalno identiteto, bi bilo treba pri njihovi uvedbi upoštevati splošno sprejete sektorske standarde in specifikacije.

(57) Kadar zelo velike spletne platforme v smislu člena 33(1) Uredbe (EU) 2022/2065 Evropskega parlamenta in Sveta ([15]) od uporabnikov zahtevajo, da so za dostop do spletnih storitev avtenticirani, bi se moralo od teh platform zahtevati, da sprejmejo uporabo evropskih denarnic za digitalno identiteto na podlagi prostovoljne zahteve uporabnika. Uporabniki ne bi smeli biti zavezani k uporabi evropske denarnice za digitalno identiteto za dostop do zasebnih storitev in ne bi smeli biti omejeni ali ovirani pri dostopu do storitev na podlagi tega, da ne uporabljajo evropske denarnice za digitalno identiteto. Če pa uporabniki to želijo, bi jih morale zelo velike spletne platforme sprejeti v ta namen, pri tem pa spoštovati načelo najmanjšega obsega podatkov in pravico uporabnikov do uporabe psevdonimov, ki si jih svobodno izberejo. Glede na pomen zelo velikih spletnih platform zaradi njihovega dosega, izraženega zlasti kot število prejemnikov storitve in število gospodarskih transakcij, je obveznost, da sprejmejo evropske denarnice za digitalno identiteto, potrebna za povečanje zaščite uporabnikov pred goljufijami in zagotovitev visoke ravni varstva podatkov.

(58) Pripraviti bi bilo treba kodekse ravnanja na ravni Unije, 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, pri tistih ponudnikih storitev, ki se ne štejejo za zelo velike spletne platforme in za avtentikacijo uporabnika uporabljajo storitve elektronske identifikacije tretjih oseb.

(59) Selektivno razkrivanje je koncept, ki lastniku podatkov omogoča, da razkrije le nekatere dele večjega nabora podatkov, da bi lahko prejemnik pridobil le tiste informacije, ki so potrebne za zagotavljanje storitve, ki jo zahteva uporabnik. Evropska denarnica za digitalno identiteto bi morala tehnično omogočati selektivno razkrivanje atributov zanašajočim se strankam. Uporabniku bi moralo biti tehnično omogočeno, da selektivno razkrije atribute, tudi iz več ločenih elektronskih potrdil, ter jih brez težav združi in predstavi zanašajočim se strankam. To bi moralo postati osnovna značilnost zasnove evropskih denarnic za digitalno identiteto, s čimer bi se povečala priročnost in izboljšalo varstvo osebnih podatkov, vključno z najmanjšim obsegom podatkov.

(60) Dostop do storitev z uporabo psevdonima ne bi smel biti prepovedan, razen če posebna pravila prava Unije ali nacionalnega prava od uporabnikov zahtevajo, da se identificirajo.

(61) Atribute, ki jih zagotovijo ponudniki kvalificiranih storitev zaupanja v okviru kvalificiranih potrdil o atributih, bi bilo treba preverjati glede na verodostojne vire bodisi neposredno s strani ponudnika kvalificiranih storitev zaupanja bodisi prek imenovanih posrednikov, priznanih na nacionalni ravni v skladu s pravom Unije ali nacionalnim pravom, za namene varne izmenjave 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 in se pri tem opirali na verodostojne vire. Med ustrezne mehanizme bi moralo biti možno vključiti tudi uporabo posebnih posrednikov ali tehničnih rešitev v skladu z nacionalnim pravom, ki omogoča dostop do verodostojnih virov. Z zagotavljanjem razpoložljivosti mehanizma, ki omogoča preverjanje atributov na podlagi verodostojnih virov, naj bi ponudnikom kvalificiranih storitev zaupanja, ki izdajajo kvalificirana elektronska potrdila o atributih, olajšali izpolnjevanje njihovih obveznosti iz Uredbe (EU) št. 910/2014. Nova priloga k navedeni uredbi bi morala vključevati 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.

(62) Varna elektronska identifikacija in zagotavljanje potrjevanja atributov bi morala prinesti dodatno prilagodljivost 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 prihodnje uredbe, s katero bo vzpostavljen organ za preprečevanje pranja denarja, ali zahtev glede primernosti, ki izhajajo iz prava o varstvu vlagateljev, ali podpirale izpolnjevanje zahtev glede močne avtentikacije strank za spletno identifikacijo za namen prijave v račun in začetka transakcij na področju plačilnih storitev.

(63) Pravnega učinka elektronskega podpisa se ne bi smelo izpodbijati na podlagi tega, da je v elektronski obliki ali da ne izpolnjuje zahtev za kvalificirani elektronski podpis. Ta uredba določa, da se kvalificirani elektronski podpis šteje za enakovrednega lastnoročnemu podpisu. Vendar mora biti pravni učinek elektronskih podpisov določen v nacionalnem pravu, razen kar zadeva zahteve iz te uredbe, glede na katere se pravni učinek kvalificiranega

([15]) Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Akt o digitalnih storitvah) (UL L 277, 27.10.2022, str. 1).

elektronskega podpisa šteje za enakovrednega lastnoročnemu podpisu. Pri opredeljevanju pravnih učinkov elektronskih podpisov bi morale države članice upoštevati načelo sorazmernosti med pravno vrednostjo dokumenta, ki ga je treba podpisati, ter ravnjo varnosti in stroški, ki jih zahteva elektronski podpis. Da bi izboljšale dostopnost in povečale uporabo elektronskih podpisov, se države članice vzpodbuja, naj razmislijo o uporabi naprednih elektronskih podpisov pri vsakodnevnih transakcijah, za katere ponujajo zadostno raven varnosti in zaupanja.

(64) Da bi zagotovila skladnost praks certificiranja po vsej Uniji, 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 javnim ali zasebnim organom, ki so certificirali naprave za ustvarjanje kvalificiranega elektronskega podpisa, ne preprečujejo, da začasno ponovno certificirajo take naprave za krajše obdobje certificiranja na podlagi rezultatov predhodnega postopka certificiranja, kadar takega ponovnega certificiranja ni mogoče opraviti v zakonsko določenem časovnem okviru iz razloga, ki ni kršitev ali varnostni incident, brez poseganja v obveznost izvajanja ocene ranljivosti in brez poseganja v veljavno prakso certificiranja.

(65) Izdaja potrdil za avtentikacijo spletišč naj bi uporabnikom zagotavljala zanesljivost z visoko stopnjo zaupanja v identiteto subjekta, ki stoji za spletiščem, ne glede na platformo, ki je uporabljena za prikaz te identitete. Ta potrdila bi morala prispevati h krepitvi zaupanja v poslovanje prek spleta, saj bi uporabniki zaupali spletišču, ki je bilo avtenticirano. Uporaba takih potrdil s strani spletišč bi morala biti prostovoljna. Da bi avtentikacija spletišč postala sredstvo, s katerim bi krepili zaupanje, zagotavljali boljšo izkušnjo uporabnika ter spodbujali rast na notranjem trgu, ta uredba določa okvir zaupanja, vključno z minimalnimi obveznostmi glede varnosti in odgovornosti za ponudnike kvalificiranih potrdil za avtentikacijo spletišč in zahtevami za izdajo teh potrdil. Nacionalni zanesljivi seznami bi morali potrditi kvalificirani status storitev za avtentikacijo spletišč in njihovih ponudnikov storitev zaupanja, vključno z njihovim popolnim izpolnjevanjem zahtev iz te uredbe glede izdaje kvalificiranih potrdil za avtentikacijo spletišč. Priznavanje kvalificiranih potrdil za avtentikacijo spletišč pomeni, da ponudniki spletnih brskalnikov ne bi smeli zanikati avtentičnosti teh potrdil izključno za namene potrjevanja povezave med domenskim imenom spletišča in fizično ali pravno osebo, ki ji je potrdilo izdano, ali potrjevanja identitete te osebe. Ponudniki spletnih brskalnikov bi morali končnemu uporabniku prikazati certificirane podatke o identiteti in druge potrjene atribute v okolju brskalnika, in sicer na uporabniku prijazen način, s tehničnimi sredstvi po lastni izbiri. V ta namen bi morali ponudniki spletnih brskalnikov zagotavljati podporo in interoperabilnost s kvalificiranimi potrdili za avtentikacijo spletišč, izdanimi ob polnem spoštovanju določb te uredbe. Obveznost priznavanja in interoperabilnosti ter podpore za kvalificirana potrdila za avtentikacijo spletišč ne vpliva na svobodo ponudnikov spletnih brskalnikov, da zagotavljajo spletno varnost, avtentikacijo domen in šifriranje spletnega prometa na način in s tehnologijo, ki se jim zdita najustreznejša. Da bi prispevali k spletni varnosti končnih uporabnikov, bi morali imeti ponudniki spletnih brskalnikov v izjemnih okoliščinah možnost, da sprejmejo preventivne ukrepe, ki so potrebni in sorazmerni, v odziv na utemeljene pomisleke, povezane s kršitvami varnosti ali izgubo celovitosti identificiranega potrdila ali sklopa potrdil. Kadar ponudniki spletnih brskalnikov sprejmejo take preventivne ukrepe, bi morali ponudniki spletnih brskalnikov Komisiji, nacionalnemu nadzornemu organu, subjektu, za katerega je bilo potrdilo izdano, in ponudniku kvalificiranih storitev zaupanja, ki je izdal navedeno potrdilo ali sklop potrdil, brez nepotrebnega odlašanja uradno sporočiti vse pomisleke v zvezi s tako kršitvijo varnosti ali izgubo celovitosti, ter sprejete ukrepe, ki so povezani z enim potrdilom ali sklopom potrdil. Ti ukrepi ne bi smeli posegati v obveznost ponudnikov spletnih brskalnikov, da priznajo kvalificirana potrdila za avtentikacijo spletišč v skladu z nacionalnimi zanesljivimi seznami. Da bi dodatno zaščitili državljane in rezidente Unije in spodbudili uporabo kvalificiranih potrdil za avtentikacijo spletišč, bi morali javni organi v državah članicah razmisliti o vključitvi kvalificiranih potrdil za avtentikacijo spletišč na svoja spletišča. Ukrepi iz te uredbe, katerih cilj je povečati skladnost med različnimi pristopi in praksami držav članic v zvezi z nadzornimi postopki, naj bi prispevali k večjemu zaupanju v varnost, kakovost in razpoložljivost kvalificiranih potrdil za avtentikacijo spletišč.

(66) Številne države članice so uvedle nacionalne zahteve za storitve, ki zagotavljajo varno in zaupanja vredno elektronsko arhiviranje za omogočanje dolgoročne hrambe elektronskih podatkov in elektronskih dokumentov ter s tem 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. Pravni okvir za kvalificirane storitve elektronskega arhiviranja bi ponudnikom in uporabnikom storitev zaupanja moral ponujati 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 elektronske podatke in elektronske dokumente, ustvarjenimi v digitalni obliki, in dokumente v papirni obliki, ki so bili skenirani in digitalizirani. Te določbe bi morale po potrebi

dovoljevati prenos shranjenih elektronskih podatkov in elektronskih dokumentov na različne nosilce zapisov ali v različnih oblikah, da bi bili še naprej trajni in berljivi tudi po izteku obdobja tehnološke veljavnosti ter bi kar najbolje preprečili njihovo izgubo in spremembo. Kadar elektronski podatki in elektronski dokumenti, ki so predmet storitve elektronskega arhiviranja, 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 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 storitve zaupanja. Ker s to uredbo storitve elektronskega arhiviranja niso usklajene, bi morale imeti države članice možnost, da v skladu s pravom Unije glede teh storitev ohranijo ali uvedejo nacionalne določbe, na primer posebne določbe glede storitev, ki so integrirane v določeno organizacijo in se uporabljajo samo za notranje arhive te organizacije. V tej uredbi se ne bi smelo razlikovati med elektronskimi podatki in elektronskimi dokumenti, ustvarjenimi v digitalni obliki, in fizičnimi dokumenti, ki so bili digitalizirani.

(67) Dejavnosti nacionalnih arhivov in ustanov ohranjanja kulturne dediščine kot organizacij, katerih naloga je ohranjanje dokumentarne dediščine v javnem interesu, so običajno urejene v nacionalnem pravu, pri čemer niso nujno ponudniki storitev zaupanja v smislu te uredbe. Kolikor take institucije takih storitev zaupanja ne ponujajo, ta uredba ne posega v njihovo delovanje.

(68) Elektronske evidence so zaporedje elektronskih podatkovnih zapisov, ki bi moralo zagotavljati njihovo celovitost in točnost njihovega kronološkega zaporedja. Elektronske evidence bi morale določiti kronološko zaporedje podatkovnih zapisov. Skupaj z drugimi tehnologijami bi morale prispevati k rešitvam za učinkovitejše in transformativne javne storitve, kot so e-volitve, čezmejno sodelovanje carinskih organov, čezmejno sodelovanje akademskih ustanov in evidentiranje lastništva nepremičnin v decentraliziranih zemljiških knjigah. Kvalificirane elektronske evidence bi morale vzpostaviti pravno domnevo o enoličnosti in točnosti kronološkega zaporedja in celovitosti podatkovnih zapisov v evidenci. Zaradi njihovih posebnosti, kot je kronološko zaporedje podatkovnih zapisov, bi se morale elektronske evidence razlikovati od drugih storitev zaupanja, kot so elektronski časovni žigi in storitve elektronske priporočene dostave. Za zagotavljanje pravne varnosti in spodbujanje inovacij bi bilo treba vzpostaviti pravni okvir na ravni Unije, ki bi zagotavljal čezmejno priznavanje storitev zaupanja za beleženje podatkov v elektronskih evidencah. To bi moralo v zadostni meri preprečiti, da bi se isto digitalno sredstvo kopiralo in prodalo več kot enkrat različnim strankam. Postopek ustvarjanja in posodabljanja elektronske evidence je odvisen od vrste uporabljene evidence, in sicer ali je centralizirana ali distribuirana. Ta uredba bi morala zagotoviti tehnološko nevtralnost, in sicer ne bi smela dajati prednosti nobeni tehnologiji, ki se uporablja za izvajanje nove storitve zaupanja za elektronske evidence, oziroma je diskriminirati. Poleg tega bi morala Komisija pri pripravi izvedbenih aktov, ki določajo zahteve za kvalificirane elektronske evidence, pri kateri bi uporabljala ustrezne metodologije, upoštevati kazalnike trajnostnosti v zvezi z morebitnimi škodljivimi vplivi na podnebje ali drugimi škodljivimi vplivi, povezanimi z okoljem.

(69) Vloga ponudnikov storitev zaupanja, ki zagotavljajo elektronske evidence, bi morala biti določanje zaporedja beleženja podatkov v evidenci. Ta uredba ne posega v morebitne pravne obveznosti uporabnikov elektronskih evidenc po pravu Unije ali nacionalnem pravu. Denimo primeri uporabe, ki vključujejo obdelavo osebnih podatkov, bi morali biti skladni z Uredbo (EU) 2016/679, primeri uporabe, ki so povezani s finančnimi storitvami, pa bi morali biti skladni z ustreznim pravom Unije o finančnih storitvah.

(70) Da bi se izognili razdrobljenosti notranjega trga in oviram na notranjem trgu zaradi različnih standardov in tehničnih omejitev ter zagotovili usklajen postopek, s katerim bi se izognili negativnemu vplivanju na izvajanje evropskega okvira za digitalno identiteto, je potreben postopek tesnega in strukturiranega sodelovanja med Komisijo, državami članicami, civilno družbo, akademskimi krogi in zasebnim sektorjem. Za dosego tega cilja bi morale države članice in Komisija sodelovati v okviru, določenem v Priporočilu Komisije (EU) 2021/946 ([16]), da bi opredelile skupni unijski nabor orodij za okvir za evropsko digitalno identiteto. V zvezi s tem bi se morale države članice dogovoriti o celoviti tehnični arhitekturi in referenčnem okviru, sklopu skupnih standardov in tehničnih referenc, vključno s priznanimi obstoječimi standardi, ter sklopu smernic in opisov najboljših praks, ki bi zajemali vsaj vse funkcionalnosti in interoperabilnost evropskih denarnic za digitalno identiteto, vključno z e-podpisi, ter ponudnikov storitev zaupanja, ki izdajajo elektronska potrdila o atributih, kot je določeno v tej uredbi. V tem okviru bi se morale države članice tudi dogovoriti o skupnih elementih poslovnega modela in strukturi pristojbin za

([16]) Priporočilo Komisije (EU) 2021/946 z dne 3. junija 2021 o skupnem unijskem naboru orodij za usklajen pristop k okviru za evropsko digitalno identiteto (UL L 210, 14.6.2021, str. 51).

evropske denarnice za digitalno identiteto, da bi olajšale njihovo uvedbo, zlasti s strani MSP, v čezmejnem okviru. Vsebina nabora orodij bi se morala razvijati vzporedno z razpravo ter odražati rezultate te razprave in postopka sprejetja evropskega okvira za digitalno identiteto.

(71) Ta uredba zagotavlja usklajeno raven kakovosti, zaupanja in varnosti kvalificiranih storitev zaupanja, ne glede na to, kje se izvajajo dejavnosti. Zato bi bilo treba ponudniku kvalificiranih storitev zaupanja omogočiti, da svoje dejavnosti, povezane z zagotavljanjem kvalificiranih storitev zaupanja, odda v zunanje izvajanje tretji državi, kadar ta tretja država zagotovi ustrezna jamstva, da se lahko nadzorne dejavnosti in revizije izvršujejo, kot če bi se izvajale v Uniji. Če skladnosti s to 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.

(72) Za zagotovitev pravne varnosti v zvezi z veljavnostjo naprednih elektronskih podpisov, ki temeljijo na kvalificiranih potrdilih, je bistveno, da se opredeli ocena zanašajoče se stranke, ki izvaja postopek potrjevanja veljavnosti navedenega naprednega elektronskega podpisa na podlagi kvalificiranih potrdil.

(73) Ponudniki storitev zaupanja bi morali uporabljati kriptografske metode, ki odražajo trenutne najboljše prakse in zaupanja vredno izvajanje teh algoritmov, da bi zagotovili varnost in zanesljivost svojih storitev zaupanja.

(74) Ta uredba določa obveznost kvalificiranih ponudnikov storitev zaupanja, da preverijo identiteto fizične ali pravne osebe, ki se ji kvalificirano potrdilo ali kvalificirano elektronsko potrdilo o atributih izda na podlagi različnih metod, usklajenih po vsej Uniji. Za zagotovitev, da se kvalificirana potrdila in kvalificirana elektronska potrdila o atributih izdajo osebi, kateri pripadajo, ter da potrjujejo pravilen in enoličen nabor podatkov, ki predstavlja identiteto navedene osebe, bi morali ponudniki kvalificiranih storitev zaupanja, ki izdajajo kvalificirana potrdila ali kvalificirana elektronska potrdila o atributih, ob izdaji navedenih potrdil s popolno gotovostjo zagotoviti identifikacijo navedene osebe. Poleg tega bi morali ponudniki kvalificiranih storitev zaupanja poleg obveznega preverjanja identitete osebe, če je to potrebno za izdajo kvalificiranih potrdil in pri izdaji kvalificiranega elektronskega potrdila o atributih, s popolno gotovostjo zagotoviti pravilnost in točnost potrjenih atributov osebe, ki se ji izda kvalificirano potrdilo ali kvalificirano elektronsko potrdilo o atributih. Navedene obveznosti glede rezultatov in popolne gotovosti pri preverjanju potrjenih podatkov bi bilo treba podpreti z ustreznimi sredstvi, vključno z uporabo ene od posebnih metod iz te uredbe, ali, kadar je to potrebno, kombinacije teh metod. Navedene metode bi moralo biti mogoče kombinirati, da se zagotovi ustrezna podlaga za preverjanje identitete osebe, ki se ji izda kvalificirano potrdilo ali kvalificirano elektronsko potrdilo o atributih. Obstajati bi morala možnost, da taka kombinacija vključuje uporabo sredstev elektronske identifikacije, ki izpolnjujejo zahteve glede srednje ravni zanesljivosti v kombinaciji z drugimi sredstvi za preverjanje identitete. Taka elektronska identifikacija bi omogočila izpolnitev usklajenih zahtev iz te uredbe glede visoke ravni zanesljivosti v okviru dodatnih usklajenih postopkov na daljavo, s čimer se zagotovi identifikacija z visoko stopnjo zaupanja. Navedene metode bi morale vključevati možnost, da ponudnik kvalificiranih storitev zaupanja, ki izda kvalificirano elektronsko potrdilo o atributih, na zahtevo uporabnika v skladu s pravom Unije ali nacionalnim pravom preveri atribute, ki jih je treba potrditi z elektronskimi sredstvi, tudi na podlagi verodostojnih virov.

(75) Da bi bila ta uredba usklajena s svetovnim razvojem in da bi sledili najboljšim 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 navedenih posodobitvah bi bilo treba upoštevati nove tehnologije, prakse, standarde ali tehnične specifikacije.

(76) Ker ciljev te uredbe, in sicer razvoja evropskega okvira za digitalno identiteto in okvira storitev zaupanja na ravni Unije, države članice ne morejo zadovoljivo doseči, temveč se zaradi obsega in učinkov lažje dosežeta na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenih ciljev.

(77) Na podlagi člena 42(1) Uredbe (EU) 2018/1725 je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov.

(78) Uredbo (EU) št. 910/2014 bi bilo zato treba ustrezno spremeniti –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Spremembe Uredbe (EU) št. 910/2014

Uredba (EU) št. 910/2014 se spremeni:

(1) člen 1 se nadomesti z naslednjim:

„*Člen 1*

Predmet urejanja

Cilj te uredbe je zagotoviti pravilno delovanje notranjega trga in ustrezno raven varnosti sredstev elektronske identifikacije in storitev zaupanja, ki se uporabljajo po vsej Uniji, da se fizičnim in pravnim osebam omogoči in olajša uveljavljanje pravice do sodelovanja v digitalni družbi na varen način ter dostopa do spletnih javnih in zasebnih storitev po vsej Uniji. V ta namen ta uredba:

(a) določa pogoje, pod katerimi države članice priznavajo sredstva elektronske identifikacije fizičnih in pravnih oseb, ki spadajo v priglašeno shemo elektronske identifikacije druge države članice ter zagotavljajo in priznavajo evropske denarnice digitalne identitete;

(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, storitve v zvezi s potrdili za avtentikacijo spletišč, elektronsko arhiviranje in elektronsko potrjevanje atributov, naprave za ustvarjanje elektronskega podpisa, naprave za ustvarjanje elektronskega žiga 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 zagotavlja država članica, in za ponudnike storitev zaupanja s sedežem v Uniji.“;

(b) odstavek 3 se nadomesti z naslednjim:

„3. Ta uredba ne vpliva na pravo Unije ali nacionalno pravo, povezano s sklenitvijo in veljavnostjo pogodb, druge pravne ali postopkovne obveznosti glede obličnosti ali posebne sektorske zahteve glede obličnosti.

4. Ta uredba ne posega v Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta (*).

(*) 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).“;

(3) člen 3 se spremeni:

(a) točke 1 do 5 se nadomestijo 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 drugo fizično osebo ali pravno osebo;

(2) ‚sredstvo elektronske identifikacije' pomeni materialno in/ali nematerialno enoto, ki vsebuje identifikacijske podatke osebe in se uporablja za avtentikacijo pri spletni storitvi ali, kadar je ustrezno, nespletni storitvi;

(3) ‚identifikacijski podatki osebe' pomeni nabor podatkov, ki je izdan v skladu s pravom Unije ali nacionalnim pravom in omogoča, da se določi identiteta fizične ali pravne osebe ali fizične osebe, ki zastopa drugo fizično osebo ali pravno osebo;

(4) ‚shema elektronske identifikacije' pomeni sistem za elektronsko identifikacijo, v okviru katerega se fizičnim ali pravnim osebam ali fizičnim osebam, ki zastopajo druge fizične osebe ali pravne osebe, izdajo sredstva elektronske identifikacije;

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

(b) vstavi se naslednja točka:

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

(c) točka 6 se nadomesti z naslednjim:

„(6) ‚zanašajoča se stranka' pomeni fizično ali pravno osebo, ki se zanaša na elektronsko identifikacijo, evropske denarnice za digitalno identiteto ali druga sredstva elektronske identifikacije ali na storitev zaupanja;";

(d) točka 16 se nadomesti z naslednjim:

„(16) ‚storitev zaupanja' pomeni elektronsko storitev, ki se praviloma opravlja za plačilo in vključuje kar koli od naslednjega:

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

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

(c) ustvarjanje elektronskih podpisov ali elektronskih žigov;

(d) potrjevanje veljavnosti elektronskih podpisov ali elektronskih žigov;

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

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

(g) izdajo elektronskih potrdil o atributih;

(h) potrjevanje veljavnosti elektronskih potrdil o atributih;

(i) ustvarjanje elektronskih časovnih žigov;

(j) potrjevanje veljavnosti elektronskih časovnih žigov;

(k) zagotavljanje storitev elektronske priporočene dostave;

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

(m) elektronsko arhiviranje elektronskih podatkov in elektronskih dokumentov;

(n) beleženje elektronskih podatkov v elektronski evidenci;“;

(e) točka 18 se nadomesti z naslednjim:

„(18) ‚organ za ugotavljanje skladnosti‘ pomeni organ za ugotavljanje skladnosti, kakor je opredeljen v členu 2, točka 13, Uredbe (ES) št. 765/2008, ki je v skladu z navedeno uredbo akreditiran 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;“;

(f) točka 21 se nadomesti z naslednjim:

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

(g) vstavita se naslednji točki:

„(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;“;

(h) točka 38 se nadomesti z naslednjim:

„(38) ‚potrdilo za avtentikacijo spletišča‘ pomeni elektronsko potrdilo, ki omogoča avtentikacijo spletišča in spletišče povezuje s fizično ali pravno osebo, ki se ji izda potrdilo;“;

(i) točka 41 se nadomesti z naslednjim:

„(41) ‚potrjevanje veljavnosti‘ pomeni postopek preverjanja in potrditve, da so podatki v elektronski obliki veljavni v skladu s to uredbo;“;

(j) dodajo se naslednje točke:

„(42) ‚evropska denarnica za digitalno identiteto‘ pomeni sredstvo elektronske identifikacije, ki uporabniku omogoča, da varno shranjuje, upravlja in potrjuje veljavnost identifikacijskih podatkov osebe in elektronskih potrdil o atributih z namenom njihovega zagotavljanja zanašajočim se strankam in drugim uporabnikom evropskih denarnic za digitalno identiteto, ter da podpisuje s kvalificiranimi elektronskimi podpisi ali žigosa s kvalificiranimi elektronskimi žigi;

(43) ‚atribut‘ pomeni 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;

(46) ‚elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir‘ pomeni elektronsko potrdilo o atributih, ki ga izda organ javnega sektorja, pristojen za verodostojni vir, ali organ 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 45f in s Prilogo VII;

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

(48) ‚elektronsko arhiviranje‘ pomeni storitev zagotavljanja prejema, shranjevanja, priklica in izbrisa elektronskih podatkov in elektronskih dokumentov za zagotavljanje njihove trajnosti in berljivosti ter ohranjanje njihove celovitosti, zaupnosti in dokazila o poreklu v celotnem obdobju hrambe;

(49) ‚kvalificirana storitev elektronskega arhiviranja‘ pomeni storitev elektronskega arhiviranja, ki jo opravlja ponudnik kvalificiranih storitev zaupanja in ki izpolnjuje zahteve iz člena 45j;

(50) ‚znak zaupanja za evropsko denarnico za digitalno identiteto‘ pomeni preverljivo, enostavno in prepoznavno označbo, ki na jasen način sporoča, da je bila evropska denarnica za digitalno identiteto zagotovljena v skladu s to uredbo;

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

(52) ‚elektronska evidenca‘ pomeni zaporedje elektronskih podatkovnih zapisov, ki zagotavlja celovitost teh zapisov in točnost kronološkega vrstnega reda teh zapisov;

(53) ‚kvalificirana elektronska evidenca‘ pomeni elektronsko evidenco, ki jo zagotavlja ponudnik kvalificiranih storitev zaupanja in ki izpolnjuje zahteve iz člena 45l;

(54) ‚osebni podatki‘ pomeni vse informacije, kakor so opredeljene v členu 4, točka 1, Uredbe (EU) 2016/679;

(55) ‚ujemanje identitete‘ pomeni postopek, v katerem se identifikacijski podatki osebe ali sredstva elektronske identifikacije osebe primerjajo ali povežejo z obstoječim računom, ki pripada isti osebi;

(56) ‚podatkovni zapis‘ pomeni elektronske podatke, zabeležene s povezanimi metapodatki, ki podpirajo obdelavo podatkov;

(57) ‚nespletni način‘ pomeni, kar zadeva uporabo evropskih denarnic za digitalno identiteto, interakcijo med uporabnikom in tretjo osebo na fizični lokaciji z uporabo tehnologij neposredne bližine, pri čemer za evropsko denarnico za digitalno identiteto za namene interakcije ni potreben dostop do sistemov na daljavo prek elektronskih komunikacijskih omrežij.“;

(4) člen 5 se nadomesti z naslednjim:

„Člen 5

Psevdonimi v elektronski transakciji

Brez poseganja v posebna pravila prava Unije ali nacionalnega prava, ki od uporabnikov zahtevajo, da se identificirajo, ali v pravni učinek psevdonimov na podlagi nacionalnega prava uporaba psevdonimov, ki jih izbere uporabnik, ni prepovedana.“;

(5) v poglavje II se vstavi naslednji oddelek:

„ODDELEK 1

EVROPSKA DENARNICA ZA DIGITALNO IDENTITETO

Člen 5a

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, pri tem pa popoln nadzor nad svojimi podatki, vsaka država članica v 24 mesecih od datuma začetka veljavnosti izvedbenih aktov iz odstavka 23 tega člena in člena 5c(6) zagotovi vsaj eno evropsko denarnico za digitalno identiteto.

2. Evropske denarnice za digitalno identiteto se zagotovijo na enega ali več od naslednjih načinov:

(a) neposredno s strani države članice;

(b) na podlagi pooblastila države članice;

(c) neodvisno od države članice, vendar z njenim priznanjem.

3. Izvorna koda komponent aplikacijske programske opreme evropskih denarnic za digitalno identiteto ima odprtokodno licenco. Države članice lahko določijo, da se iz ustrezno utemeljenih razlogov izvorna koda določenih komponent, ki niso komponente, vgrajene na naprave uporabnikov, ne razkrije.

4. Evropske denarnice za digitalno identiteto uporabniku na pregleden ter njemu prijazen in sledljiv način omogočajo, da:

(a) varno zahteva, pridobi, izbira, združuje, hrani, briše, izmenjuje in predstavi, izključno pod svojim nadzorom, identifikacijske podatke osebe, po potrebi v kombinaciji z elektronskimi potrdili o atributih, zanašajočim se strankam v avtentikacijo, in sicer v spletnem in, kadar je to ustrezno, v nespletnem načinu, za dostop do javnih in zasebnih storitev, pri čemer omogočajo selektivno razkritje podatkov;

(b) ustvarja psevdonime in jih v šifrirani obliki hrani lokalno v evropski denarnici za digitalno identiteto;

(c) varno avtenticira evropsko denarnico za digitalno identiteto druge osebe ter na varen način prejema in izmenjuje identifikacijske podatke osebe in elektronska potrdila o atributih med zadevnima evropskima denarnicama za digitalno identiteto;

(d) dostopa do evidence vseh transakcij, opravljenih prek evropske denarnice za digitalno identiteto, in sicer prek skupne nadzorne plošče, ki uporabniku omogoča, da:

(i) si ogleda posodobljeni seznam zanašajočih se strank, s katerimi je uporabnik vzpostavil povezavo, in po potrebi vseh izmenjanih podatkov;

(ii) od zanašajoče se stranke na enostaven način zahteva izbris osebnih podatkov na podlagi člena 17 Uredbe (EU) 2016/679;

(iii) pristojnemu nacionalnemu organu za varstvo podatkov enostavno prijavi zanašajočo se stranko, kadar je prejeta domnevno nezakonita ali sumljiva zahteva za podatke;

(e) se podpiše s kvalificiranimi elektronskimi podpisi ali žigosa s kvalificiranimi elektronskimi žigi;

(f) prenese, kolikor je to tehnično izvedljivo, uporabnikove podatke, elektronsko potrdilo o atributih in konfiguracije;

(g) uveljavlja pravice uporabnika do prenosljivosti podatkov.

5. Evropske denarnice za digitalno identiteto zlasti:

(a) podpirajo skupne protokole in vmesnike:

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

(ii) za zanašajoče se stranke, da lahko zahtevajo in potrdijo veljavnost identifikacijskih podatkov osebe in elektronskih potrdil o atributih;

(iii) za izmenjavo in predstavitev identifikacijskih podatkov osebe, elektronskega potrdila o atributih ali selektivno razkritih povezanih podatkov v spletnem in, kadar je to ustrezno, nespletnem načinu zanašajočim se strankam;

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

(v) za varen pristop uporabnika z uporabo sredstva elektronske identifikacije v skladu s členom 5a(24);

(vi) za interakcijo med evropskima denarnicama za digitalno identiteto dveh oseb za namen prejemanja, potrjevanja veljavnosti in izmenjave identifikacijskih podatkov osebe in elektronskih potrdil o atributih na varen način;

(vii) za avtentikacijo in identifikacijo zanašajočih se strank z izvajanjem mehanizmov avtentikacije v skladu s členom 5b;

(viii) za zanašajoče se stranke, da lahko preverijo avtentičnost in veljavnost evropskih denarnic za digitalno identiteto;

(ix) za zahtevanje od zanašajoče se stranke, da izbriše osebne podatke na podlagi člena 17 Uredbe (EU) 2016/679;

(x) za prijavo zanašajoče se stranke pristojnemu nacionalnemu organu za varstvo podatkov, kadar je prejeta domnevno nezakonita ali sumljiva zahteva za podatke;

(xi) za ustvarjanje kvalificiranih elektronskih podpisov ali elektronskih žigov z napravami za ustvarjanje kvalificiranega elektronskega podpisa ali elektronskega žiga;

(b) ne dajejo ponudnikom storitev zaupanja, ki zagotavljajo elektronska potrdila o atributih, nobenih informacij o uporabi navedenih elektronskih potrdil;

(c) zagotavljajo, da se lahko zanašajoče se stranke avtenticira in identificira z izvajanjem mehanizmov avtentikacije v skladu s členom 5b;

(d) izpolnjujejo zahteve iz člena 8 glede zagotavljanja visoke ravni zanesljivosti, zlasti v zvezi z zahtevami za dokazovanje in preverjanje identitete ter upravljanja sredstev elektronske identifikacije in avtentikacije;

(e) v primeru elektronskega potrdila o atributih z vgrajenimi politikami razkrivanja izvajajo ustrezen mehanizem za obveščanje uporabnika, da ima zanašajoča se stranka ali uporabnik evropske denarnice za digitalno identiteto, ki je zahteval navedeno elektronsko potrdilo o atributih, dovoljenje za dostop do njega;

(f) zagotavljajo, da identifikacijski podatki osebe, ki so na voljo v shemi elektronske identifikacije, v okviru katere se zagotavlja evropska denarnica za digitalno identiteto, enolično predstavljajo fizično osebo, pravno osebo ali fizično osebo, ki zastopa fizično ali pravno osebo, in so povezani z navedeno evropsko denarnico za digitalno identiteto;

(g) vsem fizičnim osebam ponujajo možnost privzetega in brezplačnega podpisovanja s kvalificiranimi elektronskimi podpisi.

Ne glede na točko (g) prvega pododstavka lahko države članice določijo sorazmerne ukrepe za zagotovitev, da je brezplačna uporaba kvalificiranih elektronskih podpisov s strani fizičnih oseb omejena na nepoklicne namene.

6. Države članice uporabnike nemudoma obvestijo o vseh kršitvah varnosti, ki so lahko v celoti ali delno ogrozile njihovo evropsko denarnico za digitalno identiteto ali njene vsebine, zlasti če je prišlo do začasne razveljavitve ali preklica njihove evropske denarnice za digitalno identiteto na podlagi člena 5e.

7. Brez poseganja v člen 5f lahko države članice v skladu z nacionalnim pravom določijo dodatne funkcionalnosti evropskih denarnic za digitalno identiteto, vključno z interoperabilnostjo z obstoječimi nacionalnimi sredstvi elektronske identifikacije. Navedene dodatne funkcionalnosti so skladne s tem členom.

8. Države članice brezplačno zagotovijo mehanizme potrjevanja veljavnosti, da:

(a) zagotovijo možnost preverjanja avtentičnosti in veljavnosti evropskih denarnic za digitalno identiteto;

(b) uporabnikom omogočijo preverjanje avtentičnosti in veljavnosti identitete zanašajočih se strank, registriranih v skladu s členom 5b.

9. Države članice zagotovijo, da je mogoče veljavnost evropske denarnice za digitalno identiteto preklicati v naslednjih primerih:

(a) na izrecno zahtevo uporabnika;

(b) kadar je ogrožena varnost evropske denarnice za digitalno identiteto;

(c) v primeru smrti uporabnika ali če pravna oseba preneha opravljati dejavnost.

10. Ponudniki evropskih denarnic za digitalno identiteto poskrbijo, da lahko uporabniki enostavno zaprosijo za tehnično podporo in prijavijo tehnične probleme ali druge incidente, ki negativno vplivajo na uporabo evropskih denarnic za digitalno identiteto.

11. Evropske denarnice za digitalno identiteto se zagotavljajo v okviru sheme elektronske identifikacije z visoko ravnjo zanesljivosti.

12. Evropske denarnice za digitalno identiteto zagotavljajo vgrajeno varnost.

13. Izdaja, uporaba in preklic evropskih denarnic za digitalno identiteto je brezplačna za vse fizične osebe.

14. Uporabniki imajo popoln nadzor nad uporabo svoje evropske denarnice za digitalno identiteto in podatki v njej. Ponudnik evropske denarnice za digitalno identiteto ne zbira informacij o uporabi evropske denarnice za digitalno identiteto, ki niso potrebne za zagotavljanje storitev evropske denarnice za digitalno identiteto, niti ne združuje identifikacijskih podatkov osebe ali kakršnih koli drugih osebnih podatkov, ki se hranijo v evropski denarnici za digitalno identiteto ali so povezani z njeno uporabo, z osebnimi podatki iz katerih koli drugih storitev, ki jih ponuja ta ponudnik, ali iz storitev tretjih oseb, ki niso potrebni za zagotavljanje storitev evropske denarnice za digitalno identiteto, razen če uporabnik tega izrecno ne zahteva. Osebni podatki v zvezi z zagotavljanjem evropske denarnice za digitalno identiteto se na logičen način hranijo ločeni od vseh drugih podatkov, ki jih ima ponudnik evropske denarnice za digitalno identiteto. Če evropsko denarnico za digitalno identiteto zagotavljajo zasebne stranke v skladu z odstavkom 2, točki (b) in (c), tega člena, se smiselno uporabljajo določbe člena 45h(3).

15. Uporaba evropskih denarnic za digitalno identiteto je prostovoljna. Fizičnim in pravnim osebam, ki ne uporabljajo evropskih denarnic za digitalno identiteto, se nikakor ne omejuje ali ovira dostop do javnih in zasebnih storitev, dostop do trga dela in svoboda gospodarske pobude. Dostop do javnih in zasebnih storitev je še naprej mogoč z drugimi obstoječimi sredstvi identifikacije in avtentikacije.

16. Tehnični okvir evropske denarnice za digitalno identiteto:

(a) ponudnikom elektronskih potrdil o atributih ali kateri koli drugi osebi po izdaji potrdila o atributih ne omogoča pridobitve podatkov, ki omogočajo sledenje, povezovanje, korelacijo ali drugačno pridobivanje znanja o transakcijah ali vedenju uporabnikov, razen če uporabnik to izrecno dovoli;

(b) omogoča tehnike za ohranjanje zasebnosti, ki zagotavljajo nepovezljivost, kadar za potrjevanje atributov ni potrebna identifikacija uporabnika.

17. Kakršna koli obdelava osebnih podatkov, ki jo izvajajo države članice ali jo v njihovem imenu izvajajo organi ali strani, pristojne za zagotavljanje evropskih denarnic za digitalno identiteto kot sredstev elektronske identifikacije, se izvaja v skladu z ustreznimi in učinkovitimi ukrepi za varstvo podatkov. Skladnost take obdelave z Uredbo (EU) 2016/679 se mora dokazati. Države članice lahko uvedejo nacionalne določbe za podrobnejšo opredelitev uporabe takih ukrepov.

18. Države članice brez nepotrebnega odlašanja uradno obvestijo Komisijo o informacijah o:

(a) organu, pristojnem za vzpostavitev in vodenje seznama registriranih zanašajočih se strank, ki se zanašajo na evropske denarnice za digitalno identiteto v skladu s členom 5b(5), ter lokaciji navedenega seznama;

(b) organih, pristojnih za zagotavljanje evropskih denarnic za digitalno identiteto v skladu s členom 5a(1);

(c) organih, pristojnih za zagotavljanje, da so identifikacijski podatki osebe povezani z evropsko denarnico za digitalno identiteto v skladu s členom 5a(5), točka (f);

(d) mehanizmu, ki omogoča potrditev veljavnosti identifikacijskih podatkov osebe iz člena 5a(5), točka (f), in identitete zanašajočih se strank;

(e) mehanizmu, s katerim se potrdi avtentičnost in veljavnost evropskih denarnic za digitalno identiteto.

Komisija da informacije, uradno sporočene na podlagi prvega pododstavka, na voljo javnosti na varen način in v elektronsko podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo.

19. Brez poseganja v odstavek 22 tega člena se za evropsko denarnico za digitalno identiteto smiselno uporablja člen 11.

20. Za ponudnike evropskih denarnic za digitalno identiteto se smiselno uporablja člen 24(2), točka (b) in točke (d) do (h).

21. Evropske denarnice za digitalno identiteto so v skladu z Direktivo (EU) 2019/882 Evropskega parlamenta in Sveta (*) invalidom dostopne za uporabo enako kot drugim uporabnikom.

22. Za namene zagotavljanja evropskih denarnic za digitalno identiteto v zvezi z evropskimi denarnicami za digitalno identiteto in shemami elektronske identifikacije, v okviru katerih se zagotavljajo, ne veljajo zahteve iz členov 7, 9, 10, 12 in 12a.

23. Komisija do 21. novembra 2024 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za zahteve iz odstavkov 4, 5, 8 in 18 tega člena v zvezi z izvajanjem evropske denarnice za digitalno identiteto. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

24. Komisija z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke, da bi uporabnikom olajšala pristop k uporabi evropske denarnice za digitalno identiteto z uporabo sredstev elektronske identifikacije, ki ustrezajo visoki ravni zanesljivosti, ali sredstev elektronske identifikacije, ki ustrezajo srednji ravni zanesljivosti, v povezavi z dodatnimi postopki pristopa na daljavo, ki skupaj izpolnjujejo zahteve glede visoke ravni zanesljivosti. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 5b

Stranke, ki se zanašajo na evropsko denarnico za digitalno identiteto

1. Kadar se zanašajoča se stranka namerava zanašati na evropske denarnice za digitalno identiteto za zagotavljanje javnih ali zasebnih storitev na podlagi digitalnih interakcij, se registrira v državi članici, v kateri ima sedež.

2. Postopek registracije je stroškovno učinkovit in sorazmeren s tveganjem. Zanašajoča se stranka zagotovi vsaj:

(a) informacije, potrebne za avtentikacijo evropskih denarnic za digitalno identiteto, ki vključujejo vsaj:

(i) državo članico, v kateri ima zanašajoča se stranka sedež, in

(ii) ime zanašajoče se stranke in po potrebi njeno registrsko številko, kot sta navedena v uradni evidenci, skupaj z identifikacijskimi podatki iz te uradne evidence;

(b) kontaktne podatke zanašajoče se stranke;

(c) predvideno uporabo evropskih denarnic za digitalno identiteto, vključno z navedbo podatkov, ki jih bo zanašajoča se stranka zahtevala od uporabnikov.

3. Zanašajoče se stranke od uporabnikov ne zahtevajo, da zagotovijo druge podatke, razen tistih navedenih na podlagi odstavka 2, točka (c).

4. Odstavka 1 in 2 ne posegata v pravo Unije ali nacionalno pravo, ki se uporablja za zagotavljanje posebnih storitev.

5. Države članice informacije iz odstavka 2 objavijo na spletu v elektronsko podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo.

6. Zanašajoče se stranke, registrirane v skladu s tem členom, nemudoma obvestijo države članice o vseh spremembah informacij, zagotovljenih v okviru registracije na podlagi odstavka 2.

7. Države članice zagotovijo skupni mehanizem, ki omogoča identifikacijo in avtentikacijo zanašajočih se strank, kot je navedeno v členu 5a(5), točka (c).

8. Kadar se zanašajoče se stranke nameravajo zanašati na evropske denarnice za digitalno identiteto, se morajo identificirati pri uporabniku.

9. Zanašajoče se stranke so odgovorne za izvajanje postopka avtentikacije in potrjevanja veljavnosti identifikacijskih podatkov osebe in elektronskih potrdil o atributih, ki se zahtevajo iz evropskih denarnic za digitalno identiteto. Zanašajoče se stranke ne zavrnejo uporabe psevdonimov, kadar se identifikacija uporabnika ne zahteva na podlagi prava Unije ali nacionalnega prava.

10. Posredniki, ki delujejo v imenu zanašajočih se strank, se štejejo za zanašajoče se stranke in ne shranjujejo podatkov o vsebini transakcije.

11. Komisija do 21. novembra 2024 z izvedbenimi akti določi tehnične specifikacije in postopke za zahteve iz odstavkov 2, 5 in 6 do 9 tega člena v zvezi z izvajanjem evropskih denarnic za digitalno identiteto, kot je navedeno v členu 5a(23). Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 5c

Certificiranje evropskih denarnic za digitalno identiteto

1. Skladnost evropskih denarnic za digitalno identiteto in sheme elektronske identifikacije, v okviru katere so zagotovljene, z zahtevami iz člena 5a(4), (5) in (8), zahtevo po ločevanju na logičen način iz člena 5a(14) ter po potrebi s standardi in tehničnimi specifikacijami iz člena 5a(24) certificirajo organi za ugotavljanje skladnosti, ki jih imenujejo države članice.

2. Certificiranje skladnosti evropskih denarnic za digitalno identiteto z ustreznimi zahtevami za kibernetsko varnost iz odstavka 1 tega člena ali njihovimi deli se izvaja v skladu z evropskimi certifikacijskimi shemami za kibernetsko varnost, sprejetimi na podlagi Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta (**) ter navedenimi v izvedbenih aktih iz odstavka 6 tega člena.

3. Za zahteve iz odstavka 1 tega člena, ki niso povezane s kibernetsko varnostjo, ter za zahteve iz odstavka 1 tega člena, ki so povezane s kibernetsko varnostjo, in sicer takrat, ko certifikacijske sheme za kibernetsko varnost, kot so navedene v odstavku 2 tega člena, ne zajemajo teh zahtev glede kibernetske varnosti ali jih zajemajo le delno, države članice tudi za navedene zahteve vzpostavijo nacionalne certifikacijske sheme v skladu z zahtevami iz izvedbenih aktov iz odstavka 6 tega člena. Države članice svoje osnutke nacionalnih certifikacijskih shem pošljejo skupini za sodelovanje na področju evropske digitalne identitete, ustanovljeni na podlagi člena 46e(1) (v nadaljnjem besedilu: skupina za sodelovanje). Skupina za sodelovanje lahko izdaja mnenja in priporočila.

4. Certificiranje na podlagi odstavka 1 velja do pet let, pod pogojem, da se ocena ranljivosti izvede vsaki dve leti. Kadar je ranljivost ugotovljena, vendar ni pravočasno odpravljena, se certificiranje razveljavi.

5. Skladnost z zahtevami iz člena 5a te uredbe v zvezi z obdelavo osebnih podatkov se lahko certificira na podlagi Uredbe (EU) 2016/679.

6. Komisija do 21. novembra 2024 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za certificiranje evropskih denarnic za digitalno identiteto iz odstavkov 1, 2 in 3 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

7. Države članice Komisiji sporočijo imena in naslove organov za ugotavljanje skladnosti iz odstavka 1. Komisija poskrbi, da so te informacije na voljo vsem državam članicam.

8. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 47 za določitev posebnih meril, ki jih morajo izpolnjevati imenovani organi za ugotavljanje skladnosti iz odstavka 1 tega člena.

Člen 5d

Objava seznama certificiranih evropskih denarnic za digitalno identiteto

1. Države članice brez nepotrebnega odlašanja obvestijo Komisijo in skupino za sodelovanje, ustanovljeno na podlagi člena 46e(1), o evropskih denarnicah za digitalno identiteto, ki so bile zagotovljene na podlagi člena 5a in so jih certificirali organi za ugotavljanje skladnosti iz člena 5c(1). Komisijo in skupino za sodelovanje, ustanovljeno na podlagi člena 46e(1), brez nepotrebnega odlašanja obvestijo o razveljavitvi certificiranja in navedejo razloge za razveljavitev.

2. Brez poseganja v člen 5a(18) informacije iz odstavka 1 tega člena, ki jih zagotovijo države članice, vključujejo vsaj:

(a) certifikat in poročilo o oceni certificiranja certificirane evropske denarnice za digitalno identiteto;

(b) opis sheme elektronske identifikacije, v okviru katere se zagotavlja evropska denarnica za digitalno identiteto;

(c) veljavno ureditev nadzora in informacije o ureditvi odgovornosti v zvezi s stranko, ki zagotavlja evropsko denarnico za digitalno identiteto;

(d) organ ali organe, pristojne za shemo elektronske identifikacije;

(e) ureditve začasne razveljavitve ali preklica elektronske identifikacijske sheme ali avtentikacije ali zadevnih ogroženih delov.

3. Komisija na podlagi informacij, prejetih na podlagi odstavka 1, pripravi, objavi v *Uradnem listu Evropske unije* in vodi v strojno berljivi obliki seznam certificiranih evropskih denarnic za digitalno identiteto.

4. Država članica lahko Komisiji predloži zahtevek, da se s seznama iz odstavka 3 umakneta evropska denarnica za digitalno identiteto in shema elektronske identifikacije, v okviru katere se zagotavlja.

5. Država članica v primeru sprememb informacij, predloženih na podlagi odstavka 1, Komisiji predloži posodobljene informacije.

6. Komisija seznam iz odstavka 3 posodablja tako, da objavi ustrezne spremembe seznama v *Uradnem listu Evropske unije* v roku enega meseca od prejema zahtevka na podlagi odstavka 4 ali posodobljenih informacij na podlagi odstavka 5.

7. Komisija do 21. novembra 2024 z izvedbenimi akti določi oblike in postopke, ki se uporabljajo za namene odstavkov 1, 4 in 5 tega člena, v zvezi z izvajanjem evropskih denarnic za digitalno identiteto, kot je navedeno v členu 5a(23). Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 5e

Kršitev varnosti evropskih denarnic za digitalno identiteto

1. Kadar kršitev ali delno ogrožanje prizadene evropske denarnice za digitalno identiteto, zagotovljene na podlagi člena 5a, mehanizme potrjevanja veljavnosti iz člena 5a(8) ali sheme elektronske identifikacije, v okviru katere se zagotavljajo evropske denarnice za digitalno identiteto, na način, ki vpliva na njihovo zanesljivost ali zanesljivost drugih evropskih denarnic za digitalno identiteto, država članica, ki je zagotovila evropske denarnice za digitalno identiteto, brez nepotrebnega odlašanja začasno prekine zagotavljanje in uporabo evropskih denarnic za digitalno identiteto.

Kadar je to upravičeno zaradi resnosti kršitve varnosti ali ogrožanja iz prvega pododstavka, država članica brez nepotrebnega odlašanja umakne evropske denarnice za digitalno identiteto.

Država članica o tem ustrezno obvesti prizadete uporabnike, enotne kontaktne točke, imenovane na podlagi člena 46c (1), zanašajoče se stranke in Komisijo.

2. Če kršitev varnosti ali ogrožanje iz odstavka 1, prvi pododstavek, tega člena ni odpravljeno v treh mesecih od začasne razveljavitve, država članica, ki je zagotovila evropske denarnice za digitalno identiteto, umakne evropske denarnice za digitalno identiteto in prekliče njihovo veljavnost. Država članica o umiku ustrezno obvesti prizadete uporabnike, enotne kontaktne točke, imenovane na podlagi člena 46c(1), zanašajoče se stranke in Komisijo.

3. Kadar je kršitev varnosti ali ogrožanje iz odstavka 1, prvi pododstavek, tega člena odpravljeno, država članica, ki je zagotovila evropske denarnice za digitalno identiteto, ponovno vzpostavi zagotavljanje in uporabo evropskih denarnic za digitalno identiteto ter o tem brez nepotrebnega odlašanja obvesti prizadete uporabnike in zanašajoče se stranke, enotne kontaktne točke, imenovane na podlagi člena 46c(1), ter Komisijo.

4. Komisija v *Uradnem listu Evropske unije* objavi ustrezne spremembe seznama iz člena 5d brez nepotrebnega odlašanja.

5. Komisija do 21. novembra 2024 z izvedbenimi akti določi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za ukrepe iz odstavkov 1, 2 in 3 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 5f

Čezmejno zanašanje na evropske denarnice za digitalno identiteto

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

2. Kadar pravo Unije ali nacionalno pravo od zasebnih zanašajočih se strank, ki zagotavljajo storitve, z izjemo mikro in malih podjetij, kot so opredeljena v členu 2 Priloge k Priporočilu Komisije 2003/361/ES (***), zahteva uporabo močne avtentikacije uporabnika za spletno identifikacijo ali kadar se močna avtentikacija uporabnika za spletno identifikacijo 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, navedene zasebne zanašajoče se stranke najpozneje 36 mesecev od datuma začetka veljavnosti izvedbenih aktov iz člena 5a(23) in člena 5c(6) ter samo na podlagi prostovoljne zahteve uporabnika sprejmejo tudi evropske denarnice za digitalno identiteto, ki so zagotovljene v skladu s to uredbo.

3. Kadar ponudniki zelo velikih spletnih platform, kot so navedene v členu 33 Uredbe (EU) 2022/2065 Evropskega parlamenta in Sveta (****), zahtevajo avtentikacijo uporabnika za dostop do spletnih storitev, sprejmejo in omogočijo tudi uporabo evropskih denarnic za digitalno identiteto, ki so zagotovljene v skladu s to uredbo, za avtentikacijo uporabnika, in sicer samo na podlagi prostovoljne zahteve uporabnika in ob upoštevanju minimalnih podatkov, potrebnih za določeno spletno storitev, za katero se zahteva avtentikacija.

4. Komisija skupaj z državami članicami olajša pripravo kodeksov ravnanja v tesnem sodelovanju z vsemi ustreznimi deležniki, vključno s civilno družbo, da bi prispevala k široki razpoložljivosti in uporabnosti evropskih denarnic za digitalno identiteto v okviru področja uporabe te uredbe ter ponudnike storitev spodbudila, da dokončajo pripravo kodeksov ravnanja.

5. Komisija v 24 mesecih po uvedbi evropskih denarnic za digitalno identiteto oceni povpraševanje in razpoložljivost ter uporabnost evropskih denarnic za digitalno identiteto, pri čemer upošteva merila, kot so uporaba s strani uporabnikov, čezmejna prisotnost ponudnikov storitev, tehnološki razvoj, razvoj vzorcev uporabe in povpraševanje potrošnikov.

(*) 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).

(**) 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).

(***) Priporočilo Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij) (UL L 124, 20.5.2003, str. 36).

(****) Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Akt o digitalnih storitvah) (UL L 277, 27.10.2022, str. 1).“;

(6) pred členom 6 se vstavi naslednji naslov:

„ODDELEK 2

SHEME ELEKTRONSKE IDENTIFIKACIJE“;

(7) v členu 7 se točka (g) nadomesti z naslednjim:

„(g) vsaj šest mesecev pred priglasitvijo v skladu s členom 9(1) država članica priglasiteljica drugim državam članicam za namene člena 12(5) zagotovi opis navedene sheme v skladu s postopkovno ureditvijo, sprejeto na podlagi člena 12(6);“;

(8) v členu 8(3) se prvi pododstavek nadomesti z naslednjim:

„3. Do 18. septembra 2015 ter ob upoštevanju ustreznih mednarodnih standardov in odstavka 2 Komisija z izvedbenimi akti določi minimalne tehnične specifikacije, standarde in postopke, na podlagi katerih se določijo nizka, srednja in visoka raven zanesljivosti za sredstva elektronske identifikacije.“;

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

„2. Komisija v *Uradnem listu Evropske unije* brez nepotrebnega odlašanja objavi seznam shem elektronske identifikacije, priglašenih v skladu z odstavkom 1, skupaj z osnovnimi informacijami o teh shemah.

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

(10) v členu 10 se naslov nadomesti z naslednjim:

„Kršitev varnosti shem elektronske identifikacije“;

(11) vstavi se naslednji člen:

„Člen 11a

Čezmejno ujemanje identitete

1. Kadar države članice delujejo kot zanašajoče se stranke za čezmejne storitve, zagotovijo nedvoumno ujemanje identitete za fizične osebe, ki uporabljajo priglašena sredstva elektronske identifikacije ali evropske denarnice za digitalno identiteto.

2. Države članice določijo tehnične in organizacijske ukrepe za zagotavljanje visoke ravni varstva osebnih podatkov, ki se uporabljajo za ujemanje identitete, in za preprečevanje oblikovanja profilov uporabnikov.

3. Komisija do 21. novembra 2024 z izvedbenimi akti določi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za zahteve iz odstavka 1 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(12) člen 12 se spremeni:

(a) naslov se nadomesti z naslednjim:

„Interoperabilnost“;

(b) odstavek 3 se spremeni:

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

„(c) lajša izvajanje vgrajene zasebnosti in vgrajene varnosti;“;

(ii) točka (d) se črta;

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

„(d) sklicevanje na minimalni nabor identifikacijskih podatkov osebe, potreben za enolično predstavljanje fizične ali pravne osebe ali fizične osebe, ki zastopa drugo fizično osebo ali pravno osebo, ki je dostopen v okviru shem elektronske identifikacije;“;

(d) odstavka 5 in 6 se nadomestita z naslednjim:

„5. Države članice izvajajo medsebojne strokovne preglede shem elektronske identifikacije, ki spadajo na področje uporabe te uredbe in ki jih je treba priglasiti v skladu s členom 9(1), točka (a).

6. Komisija do 18. marca 2025 z izvedbenimi akti določi potrebno postopkovno ureditev za medsebojne strokovne preglede iz odstavka 5 tega člena, da se spodbudi visoka raven zaupanja in varnosti, ki ustreza stopnji tveganja. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(e) odstavek 7 se črta;

(f) odstavek 8 se nadomesti z naslednjim:

„8. Komisija do 18. septembra 2025 za določitev enotnih pogojev izvajanja zahteve iz odstavka 1 tega člena sprejme izvedbene akte o interoperabilnostnem okviru, opredeljenem v odstavku 4 tega člena, pri tem pa upošteva merila iz odstavka 3 tega člena in rezultate sodelovanja med državami članicami. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(13) v Poglavju II se vstavita naslednja člena:

„Člen 12a

Certificiranje shem elektronske identifikacije

1. Skladnost shem elektronske identifikacije, ki jih je treba priglasiti, z zahtevami glede kibernetske varnosti iz te uredbe, vključno s skladnostjo z ustreznimi zahtevami za kibernetsko varnost iz člena 8(2) glede ravni zanesljivosti shem elektronske identifikacije, certificirajo organi za ugotavljanje skladnosti, ki jih imenujejo države članice.

2. Certificiranje na podlagi odstavka 1 tega člena se izvaja v okviru ustrezne certifikacijske sheme za kibernetsko varnost na podlagi Uredbe (EU) 2019/881 ali njenih delov, kolikor certifikat kibernetske varnosti ali njegovi deli zajemajo navedene zahteve glede kibernetske varnosti.

3. Certificiranje na podlagi odstavka 1 velja do pet let, pod pogojem, da se izvede ocena ranljivosti vsaki dve leti. Kadar je ranljivost ugotovljena, vendar ni odpravljena v treh mesecih po taki ugotovitvi, se certificiranje razveljavi.

4. Ne glede na odstavek 2 lahko države članice od države članice priglasiteljice v skladu z navedenim odstavkom zahtevajo dodatne informacije o shemah elektronske identifikacije ali njihovih certificiranih delih.

5. Medsebojni strokovni pregledi shem elektronske identifikacije iz člena 12(5) se ne uporabljajo za sheme elektronske identifikacije ali dele takih shem, certificiranih v skladu z odstavkom 1 tega člena. Države članice lahko v zvezi z ravnjo zanesljivosti shem elektronske identifikacije uporabijo certifikat ali izjavo o skladnosti, izdano v skladu z ustrezno certifikacijsko shemo ali deli take sheme, z zahtevami iz člena 8(2), ki niso povezane s kibernetsko varnostjo.

6. Države članice Komisiji sporočijo imena in naslove organov za ugotavljanje skladnosti iz odstavka 1. Komisija poskrbi, da so te informacije na voljo vsem državam članicam.

Člen 12b

Dostop do funkcij strojne in programske opreme

Kadar so ponudniki evropskih denarnic za digitalno identiteto in izdajatelji priglašenih sredstev elektronske identifikacije, ki delujejo v okviru poslovne ali poklicne dejavnosti in uporabljajo jedrne platformne storitve, kakor so opredeljene v členu 2, točka 2, Uredbe (EU) 2022/1925 Evropskega parlamenta in Sveta (*), za namen ali med zagotavljanjem storitev evropske denarnice za digitalno identiteto in sredstev elektronske identifikacije končnim uporabnikom, poslovni uporabniki, kakor so opredeljeni v členu 2, točka 21, navedene uredbe, jim vratarji zlasti za namene interoperabilnosti omogočijo učinkovito interoperabilnost z istim operacijskim sistemom, funkcijami strojne opreme ali programske opreme ter dostop do njih. Taka učinkovita interoperabilnost in dostop sta omogočena brezplačno in ne glede na to, ali so funkcije strojne ali programske opreme del operacijskega sistema, ki so navedenemu vratarju na voljo ali jih ta uporablja pri zagotavljanju takih storitev v smislu člena 6(7) Uredbe (EU) 2022/1925. Ta člen ne posega v člen 5a(14) te uredbe.

(*) Uredba (EU) 2022/1925 Evropskega parlamenta in Sveta z dne 14. septembra 2022 o tekmovalnih in pravičnih trgih v digitalnem sektorju in spremembi direktiv (EU) 2019/1937 in (EU) 2020/1828 (akt o digitalnih trgih) (UL L 265, 12.10.2022, str. 1).“;

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

„1. Ne glede na odstavek 2 tega člena in brez poseganja v Uredbo (EU) 2016/679 so ponudniki storitev zaupanja odgovorni za škodo, ki je namenoma ali malomarno povzročena fizični ali pravni osebi zaradi neizpolnjevanja obveznosti iz te uredbe. Vsaka fizična ali pravna oseba, ki je utrpela premoženjsko ali nepremoženjsko škodo, ker je ponudnik storitev zaupanja kršil to uredbo, ima pravico zahtevati povrnitev škode v skladu s pravom Unije in nacionalnim pravom.

Dokazno breme o namenu 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 iz prvega pododstavka povzročil namenoma ali iz malomarnosti, razen če ta ponudnik kvalificiranih storitev zaupanja ne dokaže nasprotno.“;

(15) členi 14, 15 in 16 se nadomestijo 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 s strani mednarodne organizacije priznajo z izvedbenimi akti ali sporazumom, sklenjenim med Unijo in tretjo državo ali mednarodno organizacijo na podlagi člena 218 PDEU.

Izvedbeni akti iz prvega pododstavka se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

2. Z izvedbenimi akti in sporazumom iz odstavka 1 se zagotovi, da ponudniki storitev zaupanja v zadevni 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 ti zagotavljajo. Tretje države in mednarodne organizacije zlasti vzpostavijo, vodijo in objavijo zanesljiv seznam priznanih ponudnikov storitev zaupanja.

3. 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.

Člen 15

Dostopnost za invalide in osebe s posebnimi potrebami

Zagotavljanje sredstev elektronske identifikacije, storitev zaupanja in proizvodov za končne uporabnike, ki se uporabljajo pri zagotavljanju zadevnih storitev, mora biti na voljo v preprostem in razumljivem jeziku v skladu s Konvencijo Združenih narodov o pravicah invalidov in zahtevami glede dostopnosti iz Direktive (EU) 2019/882, s čimer imajo korist tudi osebe s funkcijskimi omejitvami, kot so starejši ljudje, in osebe z omejenim dostopom do digitalnih tehnologij.

Člen 16

Kazni

1. Brez poseganja v člen 31 Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta (*) države članice določijo pravila o kaznih, ki se uporabljajo za kršitve te uredbe. Te kazni morajo biti učinkovite, sorazmerne in odvračilne.

2. Države članice zagotovijo, da se kršitve te uredbe s strani ponudnikov kvalificiranih in nekvalificiranih storitev zaupanja kaznujejo z najvišjimi globami v višini najmanj:

(a) 5 000 000 EUR, kadar je ponudnik storitev zaupanja fizična oseba, ali

(b) kadar je ponudnik storitev zaupanja pravna oseba, 5 000 000 EUR ali 1 % skupnega svetovnega letnega prometa podjetja, ki mu pripada ponudnik storitev zaupanja, v poslovnem letu pred letom, v katerem je prišlo do kršitve, pri čemer se upošteva višji znesek.

3. Glede na pravni sistem držav članic se lahko pravila o globah uporabljajo tako, da postopek za naložitev globe sproži pristojni nadzorni organ, naložijo pa jo pristojna nacionalna sodišča. Z uporabo takih pravil v navedenih državah članicah se zagotovi, da so navedena pravna sredstva učinkovita in imajo enak učinek kot globe, ki jih neposredno naložijo nadzorni organi.

(*) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80).“;

(16) v poglavju III, oddelek 2, se naslov spremeni z naslednjim:

„Nekvalificirane storitve zaupanja“;

(17) člena 17 in 18 se črtata;

(18) v poglavje III, oddelek 2, se vstavi naslednji člen:

„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, ki ne glede na člen 21 Direktive (EU) 2022/2555 vključujejo vsaj ukrepe, ki se nanašajo na:

(i) postopke registracije in pristopa k uporabi storitev zaupanja;

(ii) postopkovne ali upravne preglede, potrebne za zagotavljanje storitev zaupanja;

(iii) upravljanje in izvajanje storitev zaupanja;

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

2. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za namene odstavka 1, točka (a), tega člena. Zahteve iz tega člena veljajo za izpolnjene, kadar so izpolnjeni navedeni standardi, specifikacije in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(19) 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 21 Direktive (EU) 2022/2555. Ponudniki kvalificiranih storitev zaupanja zadevno poročilo o ugotavljanju skladnosti predložijo nadzornemu organu v treh delovnih dneh po njegovem prejemu.“;

(b) vstavita se naslednja odstavka:

„1a. Ponudniki kvalificiranih storitev zaupanja nadzorni organ obvestijo najpozneje en mesec pred načrtovanimi revizijami in nadzornemu organu na njegovo zahtevo omogočijo, da sodeluje kot opazovalec.

1b. Države članice Komisiji brez nepotrebnega odlašanja uradno sporočijo imena in naslove organov za ugotavljanje skladnosti iz odstavka 1 ter podrobnosti o njihovi akreditaciji ter vse naknadne spremembe v zvezi z njimi. Komisija poskrbi, da so te informacije na voljo vsem državam članicam.“;

(c) odstavki 2, 3 in 4 se nadomestijo z naslednjim:

„2. Brez poseganja v odstavek 1 lahko nadzorni organ – na stroške ponudnikov kvalificiranih storitev zaupanja – kadar koli revidira ponudnike kvalificiranih storitev zaupanja ali zahteva, da organ za ugotavljanje skladnosti opravi ugotavljanje skladnosti teh ponudnikov, da se potrdi, da ponudniki in kvalificirane storitve zaupanja, ki jih zagotavljajo, izpolnjujejo zahteve iz te uredbe. V primeru domnevne kršitve pravil o varstvu osebnih podatkov nadzorni organ brez nepotrebnega odlašanja obvesti pristojne nadzorne organe, ustanovljene na podlagi člena 51 Uredbe (EU) 2016/679.

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

Kadar navedeni ponudnik tega ne stori, po potrebi v roku, ki ga določi nadzorni organ, nadzorni organ, kadar je to utemeljeno zlasti z obsegom, trajanjem in posledicami tega neizpolnjevanja, navedenemu ponudniku ali zadevni storitvi, ki jo ponudnik zagotavlja, odvzame kvalificirani status.

3a. Kadar pristojni organi, imenovani ali ustanovljeni na podlagi člena 8(1) Direktive (EU) 2022/2555, obvestijo nadzorni organ, da ponudnik kvalificiranih storitev zaupanja ne izpolnjuje katere od zahtev iz člena 21 navedene direktive, nadzorni organ, kadar je to utemeljeno zlasti z obsegom, trajanjem in posledicami tega neizpolnjevanja, navedenemu ponudniku ali zadevni storitvi, ki jo ponudnik zagotavlja, odvzame kvalificirani status.

3b. Kadar nadzorni organi, ustanovljeni na podlagi člena 51 Uredbe (EU) 2016/679, obvestijo nadzorni organ, da ponudnik kvalificiranih storitev zaupanja ne izpolnjuje katere od zahtev iz navedene uredbe, nadzorni organ, kadar je to utemeljeno zlasti z obsegom, trajanjem in posledicami tega 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 zadevni storitvi. Nadzorni organ obvesti organ, priglašen na podlagi člena 22(3) te uredbe, za namene posodabljanja zanesljivih seznamov iz odstavka 1 navedenega člena in pristojni organ, imenovan ali vzpostavljen na podlagi člena 8(1) Direktive (EU) 2022/2555.

4. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za naslednje:

(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, vključno s sestavljenim ugotavljanjem;

(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.

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

(20) člen 21 se spremeni:

(a) odstavka 1 in 2 se nadomestita z naslednjim:

„1. Kadar nameravajo ponudniki storitev zaupanja začeti zagotavljati kvalificirano storitev 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 iz člena 21 Direktive (EU) 2022/2555.

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.

Nadzorni organ za namene preverjanja, ali ponudnik storitev zaupanja izpolnjuje zahteve iz člena 21 Direktive (EU) 2022/2555, od pristojnih organov, imenovanih ali ustanovljenih na podlagi člena 8(1) navedene direktive, zahteva, da brez nepotrebnega odlašanja, v vsakem primeru pa v dveh mesecih od prejema navedene zahteve, izvedejo nadzorne ukrepe v zvezi s tem in zagotovijo informacije o izidu. Če preverjanje ni zaključeno v dveh mesecih od priglasitve, navedeni pristojni organi o tem obvestijo nadzorni organ ter navedejo razloge za zamudo in rok, v katerem bo preverjanje zaključeno.

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 ta 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 do 21. maja 2025 z izvedbenimi akti določi oblike in postopke priglasitve in preverjanja za namene odstavkov 1 in 2 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(21) 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 izda kvalificirano potrdilo ali kvalificirano elektronsko potrdilo o atributih.

1a. Ponudnik kvalificiranih storitev zaupanja na ustrezen način izvede preverjanje identitete iz odstavka 1, bodisi neposredno bodisi s tretjo osebo, na podlagi ene od naslednjih metod ali njihove kombinacije, kadar je to potrebno, v skladu z izvedbenimi akti iz odstavka 1c:

(a) z evropsko denarnico za digitalno identiteto ali priglašenim sredstvom elektronske identifikacije, ki izpolnjuje zahteve iz člena 8 v zvezi z visoko ravnjo zanesljivosti;

(b) s 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 dokazi in postopki v skladu z nacionalnim pravom.

1b. Ponudnik kvalificiranih storitev zaupanja na ustrezen način izvede preverjanje atributov iz odstavka 1, bodisi neposredno bodisi s tretjo osebo, na podlagi ene od naslednjih metod ali njihove kombinacije, kadar je to potrebno, v skladu z izvedbenimi akti iz odstavka 1c:

(a) z evropsko denarnico za digitalno identiteto ali priglašenim sredstvom elektronske identifikacije, ki izpolnjuje zahteve iz člena 8 v zvezi z visoko ravnjo zanesljivosti;

(b) s potrdilom kvalificiranega elektronskega podpisa ali kvalificiranega elektronskega žiga, izdanega v skladu z odstavkom 1a, točka (a), (c) ali (d);

(c) s kvalificiranim elektronskim potrdilom o atributih;

(d) z uporabo drugih načinov, ki zagotavljajo preverjanje atributov z visoko stopnjo zaupanja, katere skladnost potrdi organ za ugotavljanje skladnosti;

(e) s fizično prisotnostjo fizične osebe ali pooblaščenega predstavnika pravne osebe z ustreznimi dokazi in postopki v skladu z nacionalnim pravom.

1c. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za preverjanje identitete in atributov v skladu z odstavki 1, 1a in 1b tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(b) odstavek 2 se spremeni:

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

„(a) obvesti nadzorni organ vsaj en mesec pred izvajanjem kakršne koli spremembe pri zagotavljanju svojih kvalificiranih storitev zaupanja oziroma vsaj tri mesece v primeru namere o prenehanju opravljanja teh dejavnosti;“;

(ii) točki (d) in (e) se nadomestita z naslednjim:

„(d) pred vstopom v pogodbeno razmerje vsako osebo, ki želi uporabljati kvalificirano storitev zaupanja, na jasen, razumljiv in zlahka dostopen način 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 zagotavljajo tehnično varnost in zanesljivost postopkov, pri katerih se uporabljajo, tudi z rabo ustreznih kriptografskih algoritmov;“;

(iii) vstavita se naslednji točki:

„(fa) brez poseganja v člen 21 Direktive (EU) 2022/2555 sprejme primerne politike in temu ustrezne ukrepe v zvezi z obvladovanjem pravnih, poslovnih, operativnih in drugih neposrednih ali posrednih tveganj za zagotavljanje kvalificiranih storitev zaupanja, med drugim vsaj ukrepe, povezane z naslednjim:

(i) postopki registracije in pristopa k uporabi storitve;

(ii) postopkovnimi ali upravnimi pregledi;

(iii) upravljanjem in izvajanjem storitev;

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

(iv) točke (g), (h) in (i) se nadomestijo z naslednjim:

„(g) sprejme ustrezne ukrepe proti ponarejanju, kraji ali protipravni prilastitvi podatkov ali neupravičenemu brisanju oziroma 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 ponudnik kvalificiranih storitev zaupanja izdal in prejel, ter ohranja dostop do njih, da se zagotovijo dokazi v pravnih postopkih in neprekinjenost storitve. Tako beleženje je lahko elektronsko;

(i) ima posodobljen načrt za prenehanje zagotavljanja storitve, da se zagotovi neprekinjenost storitve v skladu z določbami, ki jih nadzorni organ preveri na podlagi člena 46b(4), točka (i);“;

(v) točka (j) se črta;

(vi) doda se naslednji pododstavek:

„Nadzorni organ lahko zahteva dodatne informacije poleg tistih, priglašenih na podlagi točke (a) prvega pododstavka, ali rezultat ugotavljanja skladnosti in lahko postavi pogoje, preden da dovoljenje za izvedbo načrtovanih sprememb kvalificiranih storitev zaupanja. Če 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.“;

(c) odstavek 5 se nadomesti z naslednjim:

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

4b. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 47 za določitev dodatnih ukrepov iz odstavka 2, točka (fa), tega člena.

5. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za zahteve iz odstavka 2 tega člena. Zahteve iz tega odstavka veljajo za izpolnjene, če so izpolnjeni navedeni standardi, specifikacije in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(22) v poglavje III, oddelek 3, se vstavi naslednji člen:

„Člen 24a

Priznavanje kvalificiranih storitev zaupanja

1. Kvalificirani elektronski podpisi, ki temeljijo na kvalificiranem potrdilu, izdanem v eni državi članici, ter kvalificirani elektronski žigi, ki temeljijo na kvalificiranem potrdilu, izdanem v eni državi članici, se priznajo kot kvalificirani elektronski podpisi oziroma kvalificirani elektronski žigi v vseh drugih državah članicah.

2. Naprave za ustvarjanje kvalificiranega elektronskega podpisa ter naprave za ustvarjanje kvalificiranega elektronskega žiga, certificirane v eni državi članici, se priznajo kot naprave za ustvarjanje kvalificiranega elektronskega podpisa oziroma naprave za ustvarjanje kvalificiranega elektronskega žiga v vseh drugih državah članicah.

3. Kvalificirano potrdilo za elektronske podpise, kvalificirano potrdilo za elektronske žige, kvalificirana storitev zaupanja za upravljanje naprav za ustvarjanje kvalificiranega elektronskega podpisa na daljavo oziroma kvalificirana storitev zaupanja za upravljanje naprav za ustvarjanje kvalificiranega elektronskega žiga na daljavo, zagotovljena v eni državi članici, se prizna kot kvalificirano potrdilo za elektronske podpise, kvalificirano potrdilo za elektronske žige, kvalificirana storitev zaupanja za upravljanje naprav za ustvarjanje kvalificiranega elektronskega podpisa na daljavo oziroma kvalificirana storitev zaupanja za upravljanje naprav za ustvarjanje kvalificiranega elektronskega žiga na daljavo v vseh drugih državah članicah.

4. Kvalificirana storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov oziroma kvalificirana storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov, zagotovljena v eni državi članici, se prizna kot kvalificirana storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov oziroma kvalificirana storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov v vseh drugih državah članicah.

5. Kvalificirana storitev hrambe kvalificiranih elektronskih podpisov oziroma kvalificirana storitev hrambe kvalificiranih elektronskih žigov, zagotovljena v eni državi članici, se prizna kot kvalificirana storitev hrambe kvalificiranih elektronskih podpisov oziroma kvalificirana storitev hrambe kvalificiranih elektronskih žigov v vseh drugih državah članicah.

6. Kvalificirani elektronski časovni žig, zagotovljen v eni državi članici, se prizna kot kvalificirani elektronski časovni žig v vseh drugih državah članicah.

7. Kvalificirano potrdilo za avtentikacijo spletišč, izdano v eni državi članici, se prizna kot kvalificirano potrdilo za avtentikacijo spletišč v vseh drugih državah članicah.

8. Kvalificirana storitev elektronske priporočene dostave, zagotovljena v eni državi članici, se prizna kot kvalificirana storitev elektronske priporočene dostave v vseh drugih državah članicah.

9. Kvalificirano elektronsko potrdilo o atributih, izdano v eni državi članici, se prizna kot kvalificirano elektronsko potrdilo o atributih v vseh drugih državah članicah.

10. Kvalificirana storitev elektronskega arhiviranja, zagotovljena v eni državi članici, se prizna kot kvalificirana storitev elektronskega arhiviranja v vseh drugih državah članicah.

11. Kvalificirana elektronska evidenca, zagotovljena v eni državi članici, se prizna kot kvalificirana elektronska evidenca v vseh drugih državah članicah.“;

(23) v členu 25 se črta odstavek 3;

(24) člen 26 se spremeni:

(a) edini odstavek postane odstavek 1;

(b) doda se naslednji odstavek:

„2. Komisija do 21. maja 2026 oceni, ali je treba sprejeti izvedbene akte, da se vzpostavi seznam referenčnih standardov ter po potrebi določijo specifikacije in postopki za napredne elektronske podpise. Komisija lahko na podlagi te ocene sprejme take izvedbene akte. Zahteve za napredne elektronske podpise veljajo za izpolnjene, kadar je napredni elektronski podpis skladen s temi standardi, specifikacijami in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(25) v členu 27 se črta odstavek 4;

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

„6. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za kvalificirana potrdila za elektronski podpis. Zahteve iz Priloge I veljajo za izpolnjene, kadar je kvalificirano potrdilo za elektronski podpis skladno s temi standardi, specifikacijami in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(27) v členu 29 se vstavi naslednji odstavek:

„1a. Podatke za ustvarjanje elektronskega podpisa se ustvari ali upravlja ali za namene varnostne kopije podvaja zgolj v imenu podpisnika in na njegovo zahtevo s strani ponudnika kvalificiranih storitev zaupanja, ki zagotavlja kvalificirano storitev zaupanja za upravljanje naprave za ustvarjanje kvalificiranega elektronskega podpisa na daljavo.“;

(28) vstavi se naslednji člen:

„Člen 29a

Zahteve za kvalificirano storitev upravljanja naprav za ustvarjanje kvalificiranega elektronskega podpisa na daljavo

1. Upravljanje naprav za ustvarjanje kvalificiranega elektronskega podpisa na daljavo kot kvalificirano storitev izvaja samo ponudnik kvalificiranih storitev zaupanja, ki:

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

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

(i) varnost podvojenih naborov podatkov mora biti na enaki ravni kot varnost prvotnih naborov podatkov;

(ii) število podvojenih naborov podatkov ne sme biti 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 na podlagi člena 30.

2. Komisija do 21. maja 2025 z izvedbenimi akti določi seznam referenčnih standardov ter po potrebi specifikacije in postopke za namene odstavka 1 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(29) v členu 30 se vstavi naslednji odstavek:

„3a. Veljavnost certifikacije iz odstavka 1 ni daljša od pet let, če se ocene ranljivosti izvajajo vsaki dve leti. Kadar so ugotovljene ranljivosti, ki pa niso odpravljene, se certificiranje razveljavi.“;

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

„3. Komisija do 21. maja 2025 z izvedbenimi akti določi oblike in postopke, ki se uporabljajo za namene odstavka 1 tega člena. Ti 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 tega odstavka veljajo za izpolnjene, kadar je potrjevanje veljavnosti kvalificiranih elektronskih podpisov skladno s standardi, specifikacijami in postopki iz odstavka 3.“;

(b) odstavek 3 se nadomesti z naslednjim:

„3. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za potrjevanje veljavnosti kvalificiranih elektronskih podpisov. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(32) vstavi se naslednji člen:

„*Člen 32a*

Zahteve za potrjevanje veljavnosti naprednih elektronskih podpisov, ki temeljijo na kvalificiranih potrdilih

1. S postopkom za potrjevanje veljavnosti naprednega elektronskega podpisa, ki temelji na kvalificiranem potrdilu, se potrdi veljavnost naprednega elektronskega podpisa, ki temelji na kvalificiranem potrdilu, 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 zanašajoči se stranki;

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

(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.

2. Sistem za potrjevanje veljavnosti naprednega elektronskega podpisa, ki temelji na kvalificiranem potrdilu, zanašajoči se stranki zagotavlja pravilne rezultate postopka potrjevanja veljavnosti in ji omogoča, da zazna vse zadevne varnostne probleme.

3. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za potrjevanje veljavnosti naprednih elektronskih podpisov, ki temeljijo na kvalificiranih potrdilih. Zahteve iz odstavka 1 tega člena veljajo za izpolnjene, kadar so pri potrjevanju veljavnosti naprednega elektronskega podpisa, ki temelji na kvalificiranem potrdilu, skladne s temi standardi, specifikacijami in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(33) v členu 33 se odstavek 2 nadomesti z naslednjim:

„2. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za kvalificirano storitev potrjevanja veljavnosti iz odstavka 1 tega člena. Zahteve iz odstavka 1 tega člena veljajo za izpolnjene, kadar je storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov skladna s temi standardi, specifikacijami in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48 (2).“;

(34) člen 34 se spremeni:

(a) vstavi se naslednji odstavek:

„1a. Zahteve iz odstavka 1 veljajo za izpolnjene, kadar je ureditev za kvalificirano storitev hrambe kvalificiranih elektronskih podpisov skladna s standardi, specifikacijami in postopki iz odstavka 2.“;

(b) odstavek 2 se nadomesti z naslednjim:

„2. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za kvalificirano storitev hrambe kvalificiranih elektronskih podpisov. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(35) v členu 35 se črta odstavek 3;

(36) člen 36 se spremeni:

(a) edini odstavek postane odstavek 1;

(b) doda se naslednji odstavek:

„2. Komisija do 21. maja 2026 oceni, ali je treba sprejeti izvedbene akte, da se vzpostavi seznam referenčnih standardov ter po potrebi določijo specifikacije in postopki za napredne elektronske žige. Komisija lahko na podlagi te ocene sprejme take izvedbene akte. Zahteve za napredne elektronske žige veljajo za izpolnjene, kadar je napredni elektronski žig skladen s temi standardi, specifikacijami in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(37) v členu 37 se črta odstavek 4;

(38) v členu 38 se odstavek 6 nadomesti z naslednjim:

„6. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za kvalificirana potrdila za elektronske žige. Zahteve iz Priloge III veljajo za izpolnjene, kadar je kvalificirano potrdilo za elektronski žig skladno s temi standardi, specifikacijami in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(39) vstavi se naslednji člen:

„Člen 39a

Zahteve za kvalificirano storitev upravljanja naprav za ustvarjanje kvalificiranega elektronskega žiga na daljavo

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

(40) v poglavje III, oddelek 5, se vstavi naslednji člen:

„Člen 40a

Zahteve za potrjevanje veljavnosti naprednih elektronskih žigov, ki temeljijo na kvalificiranih potrdilih

Člen 32a se smiselno uporablja za potrjevanje veljavnosti naprednih elektronskih žigov, ki temeljijo na kvalificiranih potrdilih.“;

(41) v členu 41 se črta odstavek 3;

(42) člen 42 se spremeni:

(a) vstavi se naslednji odstavek:

„1a. Zahteve iz odstavka 1 veljajo za izpolnjene, kadar sta povezava datuma in časa s podatki in točnost časovnega vira skladna s standardi, specifikacijami in postopki iz odstavka 2.“;

(b) odstavek 2 se nadomesti z naslednjim:

„2. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za povezavo datuma in časa s podatki in za zagotovitev točnosti časovnih virov. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(43) člen 44 se spremeni:

(a) vstavi se naslednji odstavek:

„1a. Zahteve iz odstavka 1 veljajo za izpolnjene, kadar je postopek pošiljanja in prejemanja podatkov skladen s standardi, specifikacijami in postopki iz odstavka 2.“;

(b) odstavek 2 se nadomesti z naslednjim:

„2. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za postopek pošiljanja in prejemanja podatkov. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(c) vstavita se naslednja odstavka:

„2a. Ponudniki kvalificiranih storitev elektronske priporočene dostave se lahko dogovorijo o interoperabilnosti med kvalificiranimi storitvami elektronske priporočene dostave, ki jih zagotavljajo. Tak interoperabilnostni okvir mora biti skladen z zahtevami iz odstavka 1, tako skladnost pa potrdi organ za ugotavljanje skladnosti.

2b. Komisija lahko z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za interoperabilnostni okvir iz odstavka 2a tega člena. Tehnične specifikacije in vsebina standardov so stroškovno učinkovite in sorazmerne. Izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(44) 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. Ocena izpolnjevanja teh zahtev se izvede v skladu s standardi, specifikacijami in postopki iz odstavka 2 tega člena.

1a. Ponudniki spletnih brskalnikov priznavajo kvalificirana potrdila za avtentikacijo spletišč, izdana v skladu z odstavkom 1 tega člena. Ponudniki spletnih brskalnikov zagotovijo, da so podatki o identiteti, potrjeni v potrdilu, in dodatni potrjeni atributi prikazani na uporabniku prijazen način. Ponudniki spletnih brskalnikov zagotovijo podporo in interoperabilnost s kvalificiranimi potrdili za avtentikacijo spletišč iz odstavka 1 tega člena; z izjemo mikro- ali malih podjetij, kakor so opredeljena v členu 2 Priloge k Priporočilu 2003/361/ES, v prvih petih letih delovanja kot ponudniki storitev brskanja po spletu.

1b. Za kvalificirana potrdila za avtentikacijo spletišč ne veljajo nobene obvezne zahteve razen zahtev iz odstavka 1.

2. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za kvalificirana potrdila za avtentikacijo spletišč iz odstavka 1 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(45) vstavi se naslednji člen:

„*Člen 45a*

Preventivni ukrepi na področju kibernetske varnosti

1. Ponudniki spletnih brskalnikov ne sprejmejo nobenih ukrepov, ki bi bili v nasprotju z njihovimi obveznostmi iz člena 45, zlasti z zahtevami, da prepoznajo kvalificirana potrdila za avtentikacijo spletišč in da zagotovljene podatke o identiteti prikažejo na uporabniku prijazen način.

2. Z odstopanjem od odstavka 1 in samo v primeru utemeljenih pomislekov, povezanih s kršitvami varnosti ali izgubo celovitosti identificiranega potrdila ali sklopa potrdil, lahko ponudniki spletnih brskalnikov sprejmejo preventivne ukrepe v zvezi z navedenim potrdilom ali sklopom potrdil.

3. Kadar ponudnik spletnega brskalnika sprejme preventivne ukrepe na podlagi odstavka 2, ponudnik spletnega brskalnika o svojih pomislekih brez nepotrebnega odlašanja pisno uradno obvesti Komisijo, pristojni nadzorni organ, subjekt, za katerega je bilo potrdilo izdano, in ponudnika kvalificiranih storitev zaupanja, ki je izdal navedeno potrdilo ali sklop potrdil, skupaj z opisom ukrepov, sprejetih za njihovo odpravo. Pristojni nadzorni organ ob prejemu takega uradnega obvestila zadevnemu ponudniku spletnega brskalnika izda potrdilo o prejemu.

4. Pristojni nadzorni organ vprašanja iz uradnega obvestila preišče v skladu s členom 46b(4), točka (k). Če na podlagi rezultata te preiskave potrdilu ni odvzet kvalificirani status, nadzorni organ o tem ustrezno obvesti ponudnika spletnega brskalnika in od njega zahteva, da prekliče preventivne ukrepe iz odstavka 2 tega člena.“;

(46) v poglavju III se dodajo naslednji oddelki:

„ODDELEK 9

ELEKTRONSKO POTRDILO O ATRIBUTIH

Člen 45b

Pravni učinki elektronskega potrdila o atributih

1. Elektronskemu potrdilu o atributih se ne odvzameta pravni učinek ali 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. Potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir v eni državi članici, se prizna kot potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, v vseh državah članicah.

Člen 45c

Elektronsko potrdilo o atributih na področju javnih storitev

Kadar se na podlagi nacionalnega prava za dostop do spletne storitve, ki jo zagotavlja organ javnega sektorja, zahteva elektronska identifikacija 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 45d

Zahteve za kvalificirana elektronska potrdila o atributih

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

2. Ocena izpolnjevanja zahtev iz Priloge V se izvede v skladu s standardi, specifikacijami in postopki iz odstavka 5 tega člena.

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

4. 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.

5. Komisija do 21. novembra 2024 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za kvalificirana elektronska potrdila o atributih. Ti izvedbeni akti so skladni z izvedbenimi akti iz člena 5a(23) o izvajanju evropske denarnice za digitalno identiteto. Sprejmejo se v skladu s postopkom pregleda iz člena 48(2).

Člen 45e

Preverjanje atributov na podlagi verodostojnih virov

1. Države članice v 24 mesecih od datuma začetka veljavnosti izvedbenih aktov iz členov 5a(23) in 5c(6) zagotovijo, da so vsaj v zvezi z atributi iz Priloge VI, kadar koli se ti opirajo na verodostojne vire znotraj javnega sektorja, sprejeti ukrepi, ki ponudnikom kvalificiranih storitev zaupanja, ki izdajajo kvalificirana elektronska potrdila o atributih, omogočajo, da na zahtevo uporabnika v skladu s pravom Unije ali nacionalnim pravom elektronsko preverijo navedene atribute.

2. Komisija do 21. novembra 2024 ob upoštevanju ustreznih mednarodnih standardov z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za katalog atributov in shem za potrjevanje atributov ter postopke preverjanja za kvalificirana elektronska potrdila o atributih za namene odstavka 1 tega člena. Ti izvedbeni akti so skladni z izvedbenimi akti iz člena 5a(23) o izvajanju evropske denarnice za digitalno identiteto. Sprejmejo se v skladu s postopkom pregleda iz člena 48(2).

Člen 45f

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, ki podpira kvalificirani elektronski podpis ali kvalificirani elektronski žig organa javnega sektorja iz člena 3, točka 46, opredeljenega kot izdajatelja iz točke (b) Priloge VII, ki vsebuje specifičen nabor certificiranih atributov v obliki, primerni za avtomatsko obdelavo:

(i) navaja, da je organ izdajatelj v skladu s pravom Unije ali nacionalnim pravom 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 pravo Unije ali nacionalno pravo iz točke (i).

2. Država članica, v kateri imajo sedež organi javnega sektorja iz člena 3, točka 46, 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.

3. Države članice organe javnega sektorja iz člena 3, točka 46, 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, točka 46, na voljo javnosti na varen način in v elektronsko podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo.

4. Kadar se elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir, po prvotni izdaji prekliče, preneha veljati ob preklicu, njegov status pa se ne povrne v prejšnje stanje.

5. 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, kadar je skladno s standardi, specifikacijami in postopki iz odstavka 6.

6. Komisija do 21. novembra 2024 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za elektronsko potrdilo o atributih, izdano s strani ali v imenu organa javnega sektorja, pristojnega za verodostojni vir. Ti izvedbeni akti so skladni z izvedbenimi akti iz člena 5a(23) o izvajanju evropske denarnice za digitalno identiteto. Sprejmejo se v skladu s postopkom pregleda iz člena 48(2).

7. Komisija do 21. novembra 2024 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za namene odstavka 3 tega člena. Ti izvedbeni akti so skladni z izvedbenimi akti iz člena 5a(23) o izvajanju evropske denarnice za digitalno identiteto. Sprejmejo se v skladu s postopkom pregleda iz člena 48(2).

8. Organi javnega sektorja iz člena 3, točka 46, ki izdajo elektronsko potrdilo o atributih, zagotovijo vmesnik za evropske denarnice za digitalno identiteto, ki so zagotovljene v skladu s členom 5a.

Člen 45g

Izdaja elektronskih potrdil o atributih za evropske denarnice za digitalno identiteto

1. Ponudniki elektronskih potrdil o atributih uporabnikom evropske denarnice za digitalno identiteto omogočijo, da elektronsko potrdilo o atributih zahtevajo, pridobijo, shranijo in upravljajo ne glede na to, v katerih državi članici se evropska denarnica za digitalno identiteto zagotavlja.

2. Ponudniki kvalificiranih elektronskih potrdil o atributih zagotovijo vmesnik za evropske denarnice za digitalno identiteto, ki so zagotovljene v skladu s členom 5a.

Člen 45h

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 njihovi poslovni partnerji.

2. Osebni podatki v zvezi z zagotavljanjem storitev elektronskega potrjevanja atributov se na logičen način hranijo ločeni od drugih podatkov, ki jih ima ponudnik elektronskega potrjevanja atributov.

3. Ponudniki kvalificiranih storitev elektronskega potrjevanja atributov take kvalificirane storitve zaupanja zagotavljajo na način, ki je funkcionalno ločen od drugih storitev, ki jih zagotavljajo.

ODDELEK 10

STORITVE ELEKTRONSKEGA ARHIVIRANJA

Člen 45i

Pravni učinek storitev elektronskega arhiviranja

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

2. V zvezi z elektronskimi podatki in elektronskimi dokumenti, shranjenimi s kvalificirano storitvijo elektronskega arhiviranja, velja med obdobjem njihove hrambe pri ponudniku kvalificiranih storitev zaupanja domneva o njihovi celovitosti in njihovem poreklu.

Člen 45j

Zahteve za kvalificirane storitve elektronskega arhiviranja

1. Kvalificirane storitve elektronskega arhiviranja izpolnjujejo naslednje zahteve:

(a) zagotavljajo jih ponudniki kvalificiranih storitev zaupanja;

(b) pri njih se uporabljajo postopki in tehnologije, s katerimi se lahko zagotovi, da so elektronski podatki in elektronski dokumenti trajni in berljivi tudi po izteku obdobja tehnološke veljavnosti ter vsaj med celotnim pravnim ali pogodbenim obdobjem hrambe, pri čemer se ohranita njihova celovitost in avtentičnost njihovega porekla;

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

(d) pooblaščenim zanašajočim se strankam omogočajo, da na avtomatiziran način prejmejo poročilo, ki potrjuje, da velja v zvezi z elektronskimi podatki in elektronskimi dokumenti priklicanimi iz kvalificiranega elektronskega arhiva domneva o njihovi celovitosti od začetka obdobja hrambe do trenutka priklica.

Poročilo iz točke (d) prvega pododstavka se zagotovi na zanesljiv in učinkovit način ter je opremljeno s kvalificiranim elektronskim podpisom ali kvalificiranim elektronskim žigom ponudnika kvalificirane storitve elektronskega arhiviranja.

2. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za kvalificirane storitve elektronskega arhiviranja. Zahteve za kvalificirane storitve elektronskega arhiviranja veljajo za izpolnjene, kadar je kvalificirana storitev elektronskega arhiviranja skladna s temi standardi, specifikacijami in postopki. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

ODDELEK 11

ELEKTRONSKE EVIDENCE

Člen 45k

Pravni učinki elektronskih evidenc

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

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

Člen 45l

Zahteve za kvalificirane elektronske evidence

1. Kvalificirane elektronske evidence izpolnjujejo naslednje zahteve:

(a) ustvari in upravlja 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 njihovo naknadno spremembo mogoče takoj ugotoviti, s čimer zagotavljajo njihovo celovitost skozi čas.

2. Zahteve iz odstavka 1 veljajo za izpolnjene, kadar je elektronska evidenca skladna s standardi, specifikacijami in postopki iz odstavka 3.

3. Komisija do 21. maja 2025 z izvedbenimi akti vzpostavi seznam referenčnih standardov ter po potrebi določi specifikacije in postopke za zahteve iz odstavka 1 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(47) vstavi se naslednje poglavje:

„POGLAVJE Iva

OKVIR ZA UPRAVLJANJE

Člen 46a

Nadzor okvira evropske denarnice za digitalno identiteto

1. Države članice imenujejo enega ali več nadzornih organov s sedežem na njihovem ozemlju.

Nadzorni organi, imenovani na podlagi prvega pododstavka, dobijo potrebna pooblastila in ustrezne vire za uspešno, učinkovito in neodvisno opravljanje svojih nalog.

2. Države članice Komisiji uradno sporočijo imena in naslove svojih nadzornih organov, imenovanih na podlagi odstavka 1, ter vse naknadne spremembe v zvezi z njimi. Komisija objavi seznam teh nadzornih organov.

3. Vloga nadzornih organov, imenovanih na podlagi odstavka 1, je:

(a) nadzirati ponudnike evropskih denarnic za digitalno identiteto s sedežem na ozemlju države članice, ki je imenovala zadevni nadzorni organ, ter na podlagi predhodnih in naknadnih nadzornih dejavnosti zagotoviti, da ti ponudniki in evropske denarnice za digitalno identiteto, ki jih ti ponudniki zagotavljajo, izpolnjujejo zahteve iz te uredbe;

(b) po potrebi glede ponudnikov evropskih denarnic za digitalno identiteto s sedežem na ozemlju države članice, ki je imenovala zadevni nadzorni organ, na podlagi naknadnih nadzornih dejavnosti sprejeti ukrepe, kadar so obveščeni, da ponudniki ali evropske denarnice za digitalno identiteto, ki jih ti ponudniki zagotavljajo, kršijo to uredbo.

4. Naloge nadzornih organov, imenovanih na podlagi odstavka 1, so zlasti naslednje:

(a) sodelovati z drugimi nadzornimi organi in jim zagotavljati pomoč v skladu s členoma 46c in 46e;

(b) zahtevati informacije, potrebne za spremljanje skladnosti s to uredbo;

(c) ustrezne pristojne organe zadevnih držav članic, imenovane ali ustanovljene na podlagi člena 8(1) Direktive (EU) 2022/2555, obvestiti o vseh resnih kršitvah varnosti ali izgubi celovitosti, s katero se seznanijo pri opravljanju svojih nalog, in v primeru resne kršitve varnosti ali izgube celovitosti, ki zadeva druge države članice, obvestiti enotno kontaktno točko zadevne države članice, imenovano ali vzpostavljeno na podlagi člena 8(3) Direktive (EU) 2022/2555, in enotne kontaktne točke v drugih zadevnih državah članicah, vzpostavljene na podlagi člena 46c(1) te uredbe, ter obvestiti javnost ali zahtevati, da to storijo ponudniki evropske denarnice za digitalno identiteto, kadar nadzorni organ ugotovi, da bi bilo razkritje kršitve varnosti ali izgube celovitosti v javnem interesu;

(d) opravljati inšpekcijske preglede na kraju samem in nadzor na daljavo;

(e) zahtevati, da ponudniki evropskih denarnic za digitalno identiteto odpravijo vsakršno neizpolnjevanje zahtev iz te uredbe;

(f) v primeru nezakonite ali goljufive uporabe evropske denarnice za digitalno identiteto začasno preklicati ali razveljaviti registracijo in vključitev zanašajočih se strank v mehanizem iz člena 5b(7);

(g) sodelovati s pristojnimi nadzornimi organi, ustanovljenimi na podlagi člena 51 Uredbe (EU) 2016/679, zlasti jih v ta namen brez nepotrebnega odlašanja obveščati o domnevnih kršitvah pravil o varstvu osebnih podatkov in o kršitvah varnosti, ki domnevno predstavljajo kršitve varnosti osebnih podatkov;

5. Kadar nadzorni organ, imenovan na podlagi odstavka 1, zahteva, naj ponudnik evropske denarnice za digitalno identiteto odpravi vsakršno neizpolnjevanje zahtev iz te uredbe na podlagi odstavka 4, točka (e), in ta ponudnik ne ukrepa ustrezno in, če je primerno, v roku, ki ga določi ta nadzorni organ, lahko nadzorni organ, imenovan na podlagi odstavka 1, ob upoštevanju zlasti obsega, trajanja in posledic tega neizpolnjevanja odredi, naj ponudnik začasno prekine ali pa ukine zagotavljanje evropske denarnice za digitalno identiteto. Nadzorni organ nadzornim organom drugih držav članic, Komisiji, zanašajočim se strankam in uporabnikom evropske denarnice za digitalno identiteto brez nepotrebnega odlašanja sporoči odločitev, da bo zahteval začasno razveljavitev ali pa ukinitev zagotavljanja evropske denarnice za digitalno identiteto.

6. Vsak nadzorni organ, imenovan na podlagi odstavka 1, vsako leto do 31. marca Komisiji predloži poročilo o svojih glavnih dejavnostih v predhodnem koledarskem letu. Komisija da ta letna poročila na voljo Evropskemu parlamentu in Svetu.

7. Komisija do 21. maja 2025z izvedbenimi akti določi oblike in postopke, ki se nanašajo na poročilo iz odstavka 6 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 46b

Nadzor storitev zaupanja

1. Države članice imenujejo nadzorni organ, ustanovljen na njihovem ozemlju, ali po medsebojnem dogovoru z drugo državo članico imenujejo nadzorni organ s sedežem v tej drugi državi članici. Ta nadzorni organ je pristojen za nadzorne naloge v državi članici, ki ga imenuje, kar zadeva storitve zaupanja.

Nadzorni organi, imenovani na podlagi prvega pododstavka, dobijo potrebna pooblastila in ustrezne vire za opravljanje svojih nalog.

2. Države članice Komisiji uradno sporočijo imena in naslove svojih nadzornih organov, imenovanih na podlagi odstavka 1, ter vse naknadne spremembe v zvezi z njimi. Komisija objavi seznam teh priglašenih nadzornih organov.

3. Vloga nadzornih organov, imenovanih na podlagi odstavka 1, je:

(a) nadzirati ponudnike kvalificiranih storitev zaupanja s sedežem na ozemlju države članice, ki je imenovala zadevni nadzorni organ, ter na podlagi predhodnih in naknadnih nadzornih dejavnosti zagotoviti, da ti ponudniki kvalificiranih storitev zaupanja in kvalificirane storitve zaupanja, ki jih ti zagotavljajo, izpolnjujejo zahteve iz te uredbe;

(b) po potrebi na podlagi naknadnih nadzornih dejavnosti sprejeti ukrepe v zvezi s ponudniki nekvalificiranih storitev zaupanja, ki imajo sedež na ozemlju države članice, ki je imenovala zadevni nadzorni organ, kadar so obveščeni, da navedeni ponudniki nekvalificiranih storitev zaupanja ali kvalificirane storitve zaupanja, ki jih ti zagotavljajo, domnevno ne izpolnjujejo zahtev iz te uredbe.

4. Naloge nadzornega organa, imenovanega na podlagi odstavka 1, so zlasti naslednje:

(a) ustrezne pristojne organe zadevnih držav članic, imenovane ali ustanovljene na podlagi člena 8(1) Direktive (EU) 2022/2555, obvestiti o vseh resnih kršitvah varnosti ali izgubi celovitosti, s katero se seznani pri opravljanju svojih nalog, in v primeru resne kršitve varnosti ali izgube celovitosti, ki zadeva druge države članice, obvestiti enotno kontaktno točko zadevne države članice, imenovano ali vzpostavljeno na podlagi člena 8(3) Direktive (EU) 2022/2555, in enotne kontaktne točke v drugih zadevnih državah članicah, vzpostavljene na podlagi člena 46c(1) te uredbe, ter obvestiti javnost ali zahtevati, da to stori ponudnik storitev zaupanja, kadar nadzorni organ ugotovi, da bi bilo razkritje kršitve varnosti ali izgube celovitosti v javnem interesu;

(b) sodelovati z drugimi nadzornimi organi in jim zagotavljati pomoč v skladu s členoma 46c in 46e;

(c) analizirati poročila o ugotavljanju skladnosti iz člena 20(1) in člena 21(1);

(d) Komisiji poročati o svojih glavnih dejavnostih v skladu z odstavkom 6 tega člena;

(e) izvajati revizije ali zahtevati, da organ za ugotavljanje skladnosti opravi ugotavljanje skladnosti ponudnikov kvalificiranih storitev zaupanja v skladu s členom 20(2);

(f) sodelovati s pristojnimi nadzornimi organi, ustanovljenimi na podlagi člena 51 Uredbe (EU) 2016/679, zlasti jih brez nepotrebnega odlašanja obveščati o domnevnih kršitvah pravil o varstvu osebnih podatkov in o kršitvah varnosti, ki domnevno predstavljajo kršitve varnosti osebnih podatkov;

(g) ponudnikom storitev zaupanja in storitvam, ki jih ti zagotavljajo, dodeliti kvalificirani status ter ga odvzeti v skladu s členoma 20 in 21;

(h) obveščati organ, pristojen za nacionalni zanesljivi seznam iz člena 22(3), o svojih odločitvah glede dodelitve ali odvzema kvalificiranega statusa, razen če je ta organ tudi nadzorni organ, imenovan na podlagi odstavka 1 tega člena;

(i) v primeru, da ponudnik kvalificiranih storitev zaupanja preneha opravljati svoje dejavnosti, preveriti, ali obstajajo določbe o načrtih za prenehanje zagotavljanja storitve in ali se te določbe pravilno uporabljajo, vključno s tem, kako se v skladu s členom 24(2), točka (h), ohrani dostop do informacij;

(j) zahtevati, da ponudniki storitev zaupanja odpravijo vsakršno neizpolnjevanje zahtev iz te uredbe;

(k) preiskovati trditve ponudnikov spletnih brskalnikov na podlagi člena 45a in po potrebi ukrepati.

5. Države članice lahko zahtevajo, da nadzorni organ, imenovan na podlagi odstavka 1, vzpostavi, vzdržuje in posodablja infrastrukturo zaupanja v skladu z nacionalnim pravom.

6. Vsak nadzorni organ, imenovan na podlagi odstavka 1, vsako leto do 31. marca Komisiji predloži poročilo o svojih glavnih dejavnostih v predhodnem koledarskem letu. Komisija da ta letna poročila na voljo Evropskemu parlamentu in Svetu.

7. Komisija do 21. maja 2025 sprejme smernice o izvajanju nalog iz odstavka 4 tega člena s strani nadzornih organov, imenovanih na podlagi odstavka 1 tega člena, ter z izvedbenimi akti določi oblike in postopke, ki se nanašajo na poročilo iz odstavka 6 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 46c

Enotne kontaktne točke

1. Vsaka država članica imenuje enotno kontaktno točko za storitve zaupanja, evropske denarnice za digitalno identiteto in priglašene sheme elektronske identifikacije.

2. Vsaka enotna kontaktna točka opravlja povezovalno funkcijo, da olajša čezmejno sodelovanje med nadzornimi organi za ponudnike storitev zaupanja in med nadzornimi organi za ponudnike evropskih denarnic za digitalno identiteto ter po potrebi s Komisijo in Agencijo Evropske unije za kibernetsko varnost (ENISA) in z drugimi pristojnimi organi v svoji državi članici.

3. Vsaka država članica objavi in Komisiji brez nepotrebnega odlašanja uradno sporoči imena in naslove enotne kontaktne točke, imenovane na podlagi odstavka 1, ter vse naknadne spremembe v zvezi z njimi.

4. Komisija objavi seznam enotnih kontaktnih točk priglašenih na podlagi odstavka 3.

Člen 46d

Medsebojna pomoč

1. Da se olajšata nadzor in izvrševanje obveznosti iz te uredbe, lahko nadzorni organi, imenovani na podlagi člena 46a(1) in člena 46b(1), tudi prek skupine za sodelovanje, ustanovljene na podlagi člena 46e(1), zaprosijo za medsebojno pomoč nadzorne organe druge države članice, v kateri ima ponudnik evropske denarnice za digitalno identiteto ali ponudnik storitev zaupanja sedež ali v kateri se nahajajo njegovi omrežni in informacijski sistemi ali se zagotavljajo njegove storitve.

2. Medsebojna pomoč pomeni vsaj naslednje:

(a) kadar nadzorni organ uporablja nadzorne in izvršilne ukrepe v eni državi članici, o tem obvesti nadzorni organ druge zadevne države članice in se z njim posvetuje;

(b) nadzorni organ lahko od nadzornega organa druge zadevne države članice zahteva, naj sprejme nadzorne ali izvršilne ukrepe, med drugim lahko zahteva, naj opravlja inšpekcijske preglede, ki se nanašajo na poročila o ugotavljanju skladnosti, kot so navedena v členih 20 in 21 v zvezi z zagotavljanjem storitev zaupanja;

(c) nadzorni organi lahko po potrebi opravljajo skupne preiskave z nadzornimi organi drugih držav članic.

Zadevne države članice se v skladu s svojim nacionalnim pravom dogovorijo o ureditvi in postopkih skupnih ukrepov iz prvega pododstavka in jih tudi vzpostavijo.

3. Nadzorni organ, na katerega se naslovi zahtevek za pomoč, lahko ta zahtevek zavrne iz katerega koli od naslednjih razlogov:

(a) zahtevana pomoč ni sorazmerna z nadzornimi dejavnostmi, ki jih nadzorni organ opravlja v skladu s členoma 46a in 46b;

(b) nadzorni organ ni pristojen za zagotavljanje zahtevane pomoči;

(c) zagotovitev zahtevane pomoči ne bi bila skladna s to uredbo.

4. Skupina za sodelovanje, ustanovljena na podlagi člena 46e(1), do 21. maja 2025 in nato vsaki dve leti izda usmeritve o organizacijskih vidikih in postopkih medsebojne pomoči iz odstavkov 1 in 2 tega člena.

Člen 46e

Skupina za sodelovanje na področju evropske digitalne identitete

1. Da bi podprli in olajšali čezmejno sodelovanje in izmenjavo informacij držav članic na področju storitev zaupanja, evropskih denarnic za digitalno identiteto in priglašenih shem elektronske identifikacije Komisija ustanovi skupino za sodelovanje na področju evropske digitalne identitete (skupina za sodelovanje).

2. Skupino za sodelovanje sestavljajo predstavniki, ki jih imenujejo države članice, in Komisija. Skupini za sodelovanje predseduje Komisija. Komisija skupini za sodelovanje zagotovi tudi sekretariat.

3. Na sestanke skupine za sodelovanje so lahko priložnostno vabljeni predstavniki ustreznih deležnikov, ki lahko sodelujejo pri njenem delu kot opazovalci.

4. ENISA je povabljena, da kot opazovalka sodeluje pri delu skupine za sodelovanje, kadar ta izmenjuje mnenja, najboljše prakse in informacije o pomembnih vidikih kibernetske varnosti, kot je priglasitev kršitev varnosti, ter kadar obravnava uporabo certifikatov kibernetske varnosti ali standardov s področja kibernetske varnosti.

5. Naloge skupine za sodelovanje so:

(a) s Komisijo izmenjavati nasvete in sodelovati glede nastajajočih pobud politike na področju denarnic za digitalno identiteto, sredstev elektronske identifikacije in storitev zaupanja;

(b) po potrebi Komisiji svetovati pri zgodnji pripravi osnutkov izvedbenih in delegiranih aktov, ki se sprejmejo na podlagi te uredbe;

(c) v podporo nadzornim organom pri izvajanju določb te uredbe:

(i) izmenjavati najboljše prakse in informacije glede izvajanja določb te uredbe;

(ii) preučevati ustrezno dogajanje v sektorjih, ki zadevajo denarnice za digitalno identiteto, elektronsko identifikacijo in storitve zaupanja;

(iii) organizirati skupne sestanke z ustreznimi zainteresiranimi stranmi iz vse Unije, da bi razpravljali o dejavnostih skupine za sodelovanje in zbirali prispevke o nastajajočih izzivih politike;

(iv) ob podpori agencije ENISA izmenjavati mnenja, najboljše prakse in informacije o pomembnih vidikih kibernetske varnosti, ki zadevajo evropske denarnice za digitalno identiteto, sheme elektronske identifikacije in storitve zaupanja;

(v) izmenjavati najboljše prakse v zvezi z razvojem in izvajanjem tako politik o obveščanju o kršitvah varnosti kot skupnih ukrepov iz členov 5e in 10;

(vi) organizirati skupne sestanke s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, ustanovljeno na podlagi člena 14(1) Direktive (EU) 2022/2555, da bi izmenjali pomembne informacije o kibernetskih grožnjah, incidentih, ranljivostih, pobudah za ozaveščanje, usposabljanjih, vajah in spretnostih, krepitvi zmogljivosti, zmogljivosti za razvoj standardov in tehničnih specifikacij, pa tudi standardih in tehničnih specifikacijah, povezanih s storitvami zaupanja in elektronsko identifikacijo;

(vii) na zahtevo nadzornega organa razpravljati o specifičnih zahtevkih za medsebojno pomoč iz člena 46d;

(viii) z zagotavljanjem usmeritev o organizacijskih vidikih in postopkih medsebojne pomoči iz člena 46d olajšati izmenjavo informacij med nadzornimi organi;

(d) organizirati medsebojne strokovne preglede shem elektronske identifikacije, ki jih je treba priglasiti na podlagi te uredbe.

6. Države članice zagotovijo, da njihovi imenovani predstavniki v skupini za sodelovanje učinkovito in uspešno sodelujejo.

7. Komisija do 21. maja 2025 z izvedbenimi akti določi potrebno postopkovno ureditev za lažje sodelovanje med državami članicami iz odstavka 5, točka (d), tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).“;

(48) člen 47 se spremeni:

(a) odstavka 2 in 3 se nadomestita z naslednjim:

„2. Pooblastilo za sprejemanje delegiranih aktov iz člena 5c(7), člena 24(4b) in člena 30(4) se prenese na Komisijo za nedoločen čas od 17. septembra 2014.

3. Prenos pooblastila iz člena 5c(7), člena 24(4b) in člena 30(4) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.“;

(b) odstavek 5 se nadomesti z naslednjim:

„5. Delegirani akt, sprejet na podlagi člena 5c(7), člena 24(4b) ali člena 30(4), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.“;

(49) v poglavje VI se vstavi naslednji člen:

„Člen 48a

Zahteve glede poročanja

1. Države članice zagotovijo zbiranje statističnih podatkov v zvezi z delovanjem evropskih denarnic za digitalno identiteto in kvalificiranih storitev zaupanja, ki se zagotavljajo 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 dopuščajo uporabo evropske denarnice za digitalno identiteto;

(c) število pritožb uporabnikov in incidentov na področju varstva potrošnikov ali varstva podatkov v zvezi z zanašajočimi se strankami in kvalificiranimi storitvami zaupanja;

(d) zbirno poročilo s podatki o incidentih, ki so onemogočili uporabo evropske denarnice za digitalno identiteto;

(e) povzetek pomembnih varnostnih incidentov, kršitev varstva podatkov in prizadetih uporabnikov evropskih denarnic za digitalno identiteto ali kvalificiranih storitev zaupanja.

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

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

(50) člen 49 se nadomesti z naslednjim:

„*Člen 49*

Pregled

1. Komisija do 21. maja 2026 pregleda uporabo te uredbe ter Evropskemu parlamentu in Svetu predloži poročilo. Komisija v tem poročilu oceni zlasti, ali bi bilo ustrezno spremeniti področje uporabe te uredbe ali njene posebne določbe, med drugim zlasti določbe iz člena 5c(5), pri tem pa upošteva izkušnje, pridobljene pri uporabi te uredbe, pa tudi tehnološke, tržne in pravne spremembe. Po potrebi temu poročilu priloži predlog za spremembo te uredbe.

2. Poročilo iz odstavka 1 vključuje oceno razpoložljivosti, varnosti in uporabnosti priglašenih sredstev elektronske identifikacije in evropskih denarnic za digitalno identiteto, ki spadajo na področje uporabe te uredbe, ter oceno o tem, ali naj so vsi zasebni ponudniki spletnih storitev, ki avtentikacijo uporabnikov opravljajo prek storitev elektronske identifikacije tretjih oseb, obvezani sprejeti uporabo priglašenih sredstev elektronske identifikacije in evropske denarnice za digitalno identiteto.

3. Komisija do 21. maja 2030 in nato vsaka štiri leta Evropskemu parlamentu in Svetu predloži poročilo o napredku pri doseganju ciljev te uredbe.“;

(51) 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 do 21. maja 2027 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 do 21. maja 2026 še naprej štejejo za kvalificirana potrdila za elektronske podpise v skladu s to uredbo.

3. 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 do 21. maja 2026 lahko opravlja ne da bi bilo treba za zagotavljanje teh storitev upravljanja pridobiti kvalificirani status.

4. Ponudniki kvalificiranih storitev zaupanja, ki jim je bil kvalificirani status na podlagi te uredbe dodeljen pred 20. majem 2024, nadzornemu organu čim prej, najpozneje pa do 21. maja 2026, predložijo poročilo o ugotavljanju skladnosti, ki dokazuje skladnost s členom 24(1), (1a) in 1(b).“;

(52) priloge I do IV se spremenijo v skladu s prilogami I do IV k tej uredbi;

(53) dodajo se nove priloge V, VI in VII, kakor so določene v prilogah V, VI in VII k tej uredbi.

Člen 2

Začetek veljavnosti

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

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

V Bruslju, 11. aprila 2024

Za Evropski parlament	*Za Svet*
predsednica	*predsednica*
R. METSOLA	H. LAHBIB

PRILOGA I

V Prilogi I k Uredbi (EU) št. 910/2014 se točka (i) nadomesti z naslednjim:

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

PRILOGA II

V Prilogi II k Uredbi (EU) št. 910/2014 se točki 3 in 4 črtata.

PRILOGA III

V Prilogi III k Uredbi (EU) št. 910/2014 se točka (i) nadomesti z naslednjim:

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

PRILOGA IV

Priloga IV k Uredbi (EU) št. 910/2014 se spremeni:

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

„(c) za fizične osebe: vsaj ime osebe, za katero se izdaja potrdilo, ali psevdonim in, če je uporabljen psevdonim, se to jasno navede;

(ca) za pravne osebe: enoličen nabor podatkov, ki nedvoumno predstavljajo pravno osebo, za katero se izdaja potrdilo, pri čemer je vključeno vsaj ime pravne osebe, za katero se izdaja potrdilo, in po potrebi registrska številka, kot sta navedena v uradnih evidencah;“;

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

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

PRILOGA V

„PRILOGA V

ZAHTEVE V ZVEZI S KVALIFICIRANIM ELEKTRONSKIM POTRDILOM O ATRIBUTIH

Kvalificirana elektronska potrdila o atributih vsebujejo:

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

(b) 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:

(i) za pravne osebe: ime in po potrebi registrsko številko, kot sta navedena v uradnih evidencah,

(ii) za fizične osebe: ime osebe;

(c) nabor podatkov, ki nedvoumno predstavlja subjekt, na katerega se nanašajo potrjeni atributi, in, 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 ponudnika kvalificiranih storitev zaupanja, in, če je primerno, navedbo sheme potrdil, med katere spada potrdilo o atributih;

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

(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, s katerimi je mogoče preveriti veljavnost kvalificiranega potrdila, ali lokacijo teh storitev.“.

PRILOGA VI

„PRILOGA VI

MINIMALNI SEZNAM ATRIBUTOV

Države članice na podlagi člena 45e zagotovijo, da se sprejmejo ukrepi, s katerimi lahko ponudniki kvalificiranih storitev zaupanja, ki izdajajo kvalificirana elektronska potrdila o atributih elektronsko 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 pravom Unije ali nacionalnim pravom, 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;
7. izobrazba, nazivi in licence;
8. poklicne kvalifikacije, nazivi in licence;
9. pooblastila in mandati za zastopanje fizičnih ali pravnih oseb;
10. javna dovoljenja in licence;
11. za pravne osebe: finančni podatki in podatki o družbah.“.

PRILOGA VII

„PRILOGA VII

ZAHTEVE V ZVEZI Z ELEKTRONSKIM POTRDILOM O ATRIBUTIH, IZDANIM 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, s katerimi je mogoče preveriti veljavnost potrdila, ali lokacijo teh storitev.“.