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

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

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

v skladu z rednim zakonodajnim postopkom ([2]),

ob upoštevanju naslednjega:

(1) Ustvarjanje zaupanja v spletno okolje je ključ do gospodarskega in družbenega razvoja. Zaradi pomanjkanja zaupanja, zlasti občutka, da je pravna varnost pomanjkljiva, potrošniki, podjetja in javni organi oklevajo pri izvajanju elektronskih transakcij in sprejemanju novih storitev.

(2) Namen te uredbe je okrepiti zaupanje v elektronske transakcije na notranjem trgu, tako da se zagotovi skupni temelj za varne elektronske interakcije med državljani, podjetji in javnimi organi, s čimer bi se povečala učinkovitost javnih in zasebnih spletnih storitev, elektronskega poslovanja ter elektronskega trgovanja v Uniji.

(3) Direktiva Evropskega parlamenta in Sveta 1999/93/ES ([3]) je obravnavala elektronske podpise, ni pa zagotovila celovitega čezmejnega in medsektorskega okvira za varne in zaupanja vredne elektronske transakcije, ki bi bile enostavne za uporabo. Ta uredba krepi in razširja področje uporabe navedene direktive.

(4) Komisija je v sporočilu z dne 26. avgusta 2010 z naslovom „Evropska digitalna agenda“ opredelila razdrobljenost digitalnega trga, pomanjkanje interoperabilnosti in naraščanje kibernetske kriminalitete kot glavne ovire za uspešen krog digitalnega gospodarstva. V poročilu o državljanstvu EU iz leta 2010 z naslovom „Odpravljanje ovir za pravice državljanov EU“ je nadalje izpostavila, da je treba odpraviti glavne težave, ki državljanom Unije preprečujejo, da bi koristili ugodnosti enotnega digitalnega trga in čezmejnih digitalnih storitev.

(5) Evropski svet je v svojih sklepih z dne 4. februarja 2011 in 23. oktobra 2011 Komisijo pozval, da do leta 2015 vzpostavi enotni digitalni trg, da bi se zagotovil hiter napredek na ključnih področjih digitalnega gospodarstva in se z lajšanjem čezmejne uporabe spletnih storitev, zlasti omogočanjem varne elektronske identifikacije in avtentikacije, spodbudil popolnoma povezan enotni digitalni trg.

([1]) UL C 351, 15.11.2012, str. 73.
([2]) Stališče Evropskega parlamenta z dne 3. aprila 2014 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 23. julija 2014.
([3]) Direktiva 1999/93/ES Evropskega parlamenta in Sveta z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis (UL L 13, 19.1.2000, str. 12).

(6) V svojih sklepih z dne 27. maja 2011 je Svet Komisijo pozval, da prispeva k enotnemu digitalnemu trgu, tako da oblikuje ustrezne pogoje za čezmejno vzajemno priznavanje ključnih dejavnikov, kot so elektronska identifikacija, elektronski dokumenti, elektronski podpisi in storitve elektronske dostave, ter za interoperabilne storitve e-uprave po vsej Evropski uniji.

(7) Evropski parlament je v svoji resoluciji z dne 21. septembra 2010 o dokončnem oblikovanju notranjega trga za elektronsko poslovanje ([1]) poudaril pomen varnosti elektronskih storitev, zlasti elektronskih podpisov, in potrebo po vzpostavitvi infrastrukture javnih ključev na vseevropski ravni ter pozval Komisijo, da vzpostavi evropski portal za organe potrjevanja, da se zagotovi čezmejna interoperabilnost elektronskih podpisov in izboljša varnost transakcij prek spleta.

(8) V skladu z Direktivo 2006/123/ES Evropskega parlamenta in Sveta ([2]) morajo države članice vzpostaviti „enotne kontaktne točke“, s katerimi zagotovijo, da se vsi postopki in formalnosti v zvezi z dostopom do storitvene dejavnosti in opravljanjem te dejavnosti lahko enostavno zaključijo na daljavo in po elektronski poti prek ustrezne enotne kontaktne točke pri ustreznih pristojnih organih. Številne spletne storitve, dostopne prek enotnih kontaktnih točk, zahtevajo elektronsko identifikacijo, avtentikacijo in podpis.

(9) V večini primerov državljani ne morejo uporabljati svoje elektronske identifikacije za svojo avtentikacijo v drugi državi članici, ker nacionalne sheme elektronske identifikacije iz njihove države niso priznane v drugih državah članicah. Ta elektronska ovira ponudnikom storitev preprečuje, da bi v celoti izkoristili ugodnosti notranjega trga. Vzajemno priznana sredstva elektronske identifikacije bodo poenostavila čezmejno zagotavljanje številnih storitev na notranjem trgu in podjetjem omogočila čezmejno poslovanje brez številnih ovir pri interakciji z javnimi organi.

(10) Direktiva 2011/24/EU Evropskega parlamenta in Sveta ([3]) vzpostavlja mrežo nacionalnih organov, pristojnih za e-zdravje. Da bi se izboljšali varnost in neprekinjenost čezmejnega zdravstvenega varstva, mora mreža pripraviti smernice za čezmejni dostop do elektronskih zdravstvenih podatkov in storitev ter podpreti skupne ukrepe „za identifikacijo in avtentikacijo, na podlagi katerih se olajša prenosljivost podatkov v čezmejnem zdravstvenem varstvu“. Vzajemno priznavanje elektronske identifikacije in avtentikacije je ključno pri uresničevanju čezmejnega zdravstvenega varstva evropskih državljanov. Kadar ljudje potujejo zaradi zdravljenja, morajo biti njihovi zdravstveni podatki dostopni v državi zdravljenja. To zahteva trden in varen okvir za elektronsko identifikacijo, v katerega se zaupa.

(11) To uredbo bi bilo treba uporabljati ob doslednem spoštovanju načel glede varstva osebnih podatkov iz Direktive 95/46/ES Evropskega parlamenta in Sveta ([4]). V zvezi s tem bi morala avtentikacija za spletno storitev, ob upoštevanju načela vzajemnega priznavanja iz te uredbe, zajemati obdelavo le tistih identifikacijskih podatkov, ki so ustrezni in relevantni ter niso pretirani za odobritev dostopa do te spletne storitve. Poleg tega bi morali tudi ponudniki storitev zaupanja in nadzorni organi spoštovati zahteve iz Direktive 95/46/ES v zvezi z zaupnostjo in varnostjo obdelave.

(12) Eden od ciljev te uredbe je odpraviti obstoječe ovire za čezmejno uporabo sredstev elektronske identifikacije, ki se v državah članicah uporabljajo za avtentikacijo, vsaj za javne storitve. Namen te uredbe ni posegati v elektronske sisteme za upravljanje identitete in z njimi povezane infrastrukture, vzpostavljene v državah članicah. Cilj te uredbe je zagotoviti, da je za dostop do čezmejnih spletnih storitev, ki jih zagotavljajo države članice, mogoča varna elektronska identifikacija in avtentikacija.

([1]) UL C 50 E, 21.2.2012, str. 1.
([2]) Direktiva 2006/123/ES Evropskega parlamenta in Sveta z dne 12. decembra 2006 o storitvah na notranjem trgu (UL L 376, 27.12.2006, str. 36).
([3]) Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu (UL L 88, 4.4.2011, str. 45).
([4]) Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

(13) Države članice bi morale imeti možnost, da še naprej prosto uporabljajo ali uvajajo sredstva za namene elektronske identifikacije za dostop do spletnih storitev. Prav tako bi morale imeti možnost, da se same odločijo, ali bodo v zagotavljanje teh sredstev vključile zasebni sektor. Države članice ne bi smele biti zavezane k priglasitvi shem elektronske identifikacije Komisiji. Kar zadeva sheme elektronske identifikacije, ki se na nacionalni ravni uporabljajo za dostop vsaj do javnih spletnih storitev ali posebnih storitev, se lahko države članice same odločijo, ali bodo Komisiji priglasile vse sheme, samo nekatere ali nobene.

(14) V uredbi je treba določiti nekaj pogojev v zvezi s tem, katera sredstva elektronske identifikacije je treba priznati in kako se sheme elektronske identifikacije priglasijo. Ti pogoji bi državam članicam morali pomagati pri krepitvi potrebnega zaupanja v sheme elektronske identifikacije drugih držav članic in vzajemnem priznavanju sredstev elektronske identifikacije, ki spadajo v priglašene sheme. Načelo vzajemnega priznavanja bi se moralo uporabljati, če shema elektronske identifikacije države članice priglasiteljice izpolnjuje pogoje priglasitve, priglasitev pa je bila objavljena v *Uradnem listu Evropske unije*. Načelo vzajemnega priznavanja pa bi se moralo nanašati le na avtentikacijo za spletno storitev. Dostop do teh spletnih storitev in njihova končna dostava prosilcu bi morala biti tesno povezana s pravico do prejema takšnih storitev pod pogoji iz nacionalne zakonodaje.

(15) Obveznost priznavanja sredstev elektronske identifikacije bi morala zadevati le tista sredstva, katerih raven zanesljivosti identitete ustreza ravni, ki je enaka ali višja od zahtevane ravni za zadevno spletno storitev. Poleg tega bi bilo treba to obveznost uporabljati le, kadar zadevni organ javnega sektorja uporablja „srednjo“ ali „visoko“ raven zanesljivosti glede dostopa do te spletne storitve. Države članice bi morale imeti v skladu s pravom Unije možnost, da priznajo sredstva elektronske identifikacije z nižjimi ravnmi zanesljivosti identitete.

(16) Ravni zanesljivosti bi morale označevati stopnjo zaupanja, ki jo sredstvo elektronske identifikacije zagotavlja pri ugotavljanju identitete osebe, s čimer se zagotovi, da je oseba, ki izkazuje določeno identiteto, dejansko oseba, ki ji je bila ta identiteta dodeljena. Raven zanesljivosti je odvisna od stopnje zaupanja v izkazano ali zagotavljano identiteto osebe, ki jo zagotavlja sredstvo elektronske identifikacije, pri čemer se upoštevajo postopki (na primer dokazovanje in preverjanje identitete ter avtentikacija), upravljanje (na primer subjekt, ki izda sredstvo elektronske identifikacije in postopek za izdajo takšnega sredstva) in opravljen tehnični nadzor. Obstajajo različne tehnične opredelitve in opisi ravni zanesljivosti, ki so rezultat vse-evropskih pilotnih projektov, financiranih s sredstvi Unije, standardizacije in mednarodnih dejavnosti. Zlasti vse-evropski pilotni projekt STORK in ISO 29115 se med drugim sklicujeta na ravni 2, 3 in 4, ki bi jih bilo treba v celoti upoštevati pri določanju minimalnih tehničnih zahtev, standardov in postopkov za nizko, srednjo in visoko raven zanesljivosti v smislu te uredbe, pri čemer se zagotavlja skladna uporaba te uredbe, zlasti kar zadeva visoko raven zanesljivosti, povezano z dokazovanjem identitete ob izdaji kvalificiranih potrdil. Opredeljene zahteve bi morale biti tehnološko nevtralne. Dopustiti bi bilo treba možnost, da se potrebne varnostne zahteve izpolnijo z uporabo različnih tehnologij.

(17) Države članice bi morale spodbujati zasebni sektor, da prostovoljno uporablja sredstva elektronske identifikacije v okviru priglašene sheme za namene identifikacije, kadar je to potrebno za spletne storitve ali elektronske transakcije. Možnost uporabe takšnih sredstev elektronske identifikacije bi zasebnemu sektorju omogočila uporabo elektronske identifikacije in avtentikacije, ki se v številnih državah članicah že uporabljata vsaj za javne storitve, podjetja in državljani pa bi tako imeli lažji dostop do čezmejnih spletnih storitev. Da bi zasebnemu sektorju olajšali čezmejno uporabo takšnih sredstev elektronske identifikacije, bi morala biti možnost avtentikacije, ki jo zagotavlja katera koli država članica, na voljo zanašajočim se strankam iz zasebnega sektorja, ki nimajo sedeža na ozemlju te države članice, pod enakimi pogoji, kot veljajo za zanašajoče se stranke iz zasebnega sektorja, ki imajo sedež v tej državi članici. Zato lahko država članica priglasiteljica za zanašajoče se stranke iz zasebnega sektorja določi pogoje za dostop do sredstva avtentikacije. V takšnih pogojih za dostop je lahko navedeno, ali je sredstvo avtentikacije, povezano s priglašeno shemo, trenutno na voljo zanašajočim se strankam iz zasebnega sektorja.

(18) Ta uredba bi morala določati odgovornost države članice priglasiteljice, izdajatelja sredstva elektronske identifikacije, in stranke, ki opravi postopek avtentikacije, v primeru neizpolnjevanja ustreznih obveznosti v skladu s to uredbo. Vendar bi se ta uredba morala uporabljati v skladu z nacionalnimi pravili o odgovornosti. Zato ne vpliva na navedena nacionalna pravila, na primer o opredelitvi škode, ali na ustrezna veljavna postopkovna pravila, tudi o dokaznem bremenu.

(19) Varnost shem elektronske identifikacije je ključna za zaupanja vredno čezmejno vzajemno priznavanje sredstev elektronske identifikacije. V zvezi s tem bi morale države članice sodelovati pri zagotavljanju varnosti in interoperabilnosti shem elektronske identifikacije na ravni Unije. Če bi za sheme elektronske identifikacije potrebovali posebno strojno ali programsko opremo, ki bi jo uporabljale zanašajoče se stranke na nacionalni ravni, te države članice zaradi čezmejne interoperabilnosti ne bi smele naložiti takšnih zahtev in z njimi povezanih stroškov zanašajočim se strankam, ki nimajo sedeža na njihovem ozemlju. V tem primeru bi bilo treba razpravljati o primernih rešitvah in jih razvijati v interoperabilnostnem okviru. Vendar pa se ni mogoče izogniti tehničnim zahtevam, ki izhajajo iz specifikacij nacionalnih sredstev elektronske identifikacije in bi lahko vplivale na imetnike takšnih elektronskih sredstev (npr. pametnih kartic).

(20) Sodelovanje držav članic bi moralo olajšati tehnično interoperabilnost priglašenih shem elektronske identifikacije ter tako vzpostaviti visoko raven zaupanja in varnosti, ustrezno stopnji tveganja. K takšnemu sodelovanju bi morala prispevati izmenjava informacij in najboljših praks med državami članicami, da se doseže vzajemno priznavanje.

(21) Ta uredba bi morala določiti tudi splošni pravni okvir za uporabo storitev zaupanja. Ne bi pa smela uvajati splošne obveznosti za njihovo uporabo ali vzpostaviti točke dostopa za vse obstoječe storitve zaupanja. Zlasti ne bi smela urejati zagotavljanja storitev, ki se uporabljajo izključno znotraj zaprtih sistemov med določeno skupino udeležencev, ki ne vplivajo na tretje osebe. Zahteve te uredbe na primer ne bi smele veljati za sisteme, vzpostavljene v podjetjih ali javnih upravah, ki za vodenje notranjih postopkov uporabljajo storitve zaupanja. Zahteve te uredbe bi morale izpolnjevati le storitve zaupanja, ki se zagotavljajo javnosti in vplivajo na tretje osebe. Ta uredba tudi ne bi smela urejati vidikov, povezanih s sklenitvijo in veljavnostjo pogodb ali drugih pravnih obveznosti, če nacionalno pravo ali pravo Unije določa zahteve glede obličnosti. Poleg tega tudi ne bi smela vplivati na nacionalne zahteve glede obličnosti, ki zadevajo javne registre, zlasti trgovinske registre in zemljiške knjige.

(22) Da bi spodbujali njihovo splošno čezmejno uporabo, bi moralo biti mogoče storitve zaupanja uporabljati kot dokaz v pravnih postopkih v vseh državah članicah. Pravne učinke storitev zaupanja se lahko določi v nacionalnem pravu, če v tej uredbi ni določeno drugače.

(23) Če je v tej uredbi določena obveznost priznavanja storitve zaupanja, se lahko takšna storitev zaupanja zavrne le, če je naslovnik obveznosti ne more prebrati ali preveriti zaradi tehničnih razlogov, ki niso pod njegovim neposrednim nadzorom. Kljub temu pa samo na podlagi te obveznosti ne bi smeli od javnega organa zahtevati, da pridobi strojno in programsko opremo, ki je potrebna za tehnično čitljivost vseh obstoječih storitev zaupanja.

(24) Države članice lahko v skladu s pravom Unije ohranijo ali uvedejo nacionalne določbe v zvezi s storitvami zaupanja, če te storitve niso v celoti harmonizirane s to uredbo. Za storitve zaupanja, ki so v skladu s to uredbo, pa bi morali dovoliti prosti pretok na notranjem trgu.

(25) Države članice bi morale še naprej imeti možnost, da same opredelijo druge vrste storitev zaupanja poleg tistih, ki so del zaprtega seznama storitev zaupanja iz te uredbe, da bi jih lahko na nacionalni ravni priznale kot kvalificirane storitve zaupanja.

(26) Zaradi hitrih tehnoloških sprememb bi moral biti s to uredbo sprejet pristop, ki je odprt za inovacije.

(27) Ta uredba bi morala biti tehnološko nevtralna. Pravne učinke, ki jih zagotavlja, bi moralo biti mogoče doseči s katerimi koli tehničnimi sredstvi, če so izpolnjene zahteve iz te uredbe.

(28) Da se okrepi zlasti zaupanje malih in srednjih podjetij ter potrošnikov v notranji trg ter spodbudi uporaba storitev zaupanja in izdelkov, bi bilo treba uvesti pojma kvalificiranih storitev zaupanja in ponudnika kvalificiranih storitev zaupanja ter tako določiti zahteve in obveznosti, ki zagotavljajo visoko raven varnosti vseh kvalificiranih storitev zaupanja in izdelkov, ki se uporabljajo ali zagotavljajo.

(29) V skladu z obveznostmi iz Konvencije Združenih narodov o pravicah invalidov, ki je bila odobrena s Sklepom Sveta 2010/48/ES ([1]), zlasti iz člena 9 navedene konvencije, bi bilo treba invalidom omogočiti dostop do storitev zaupanja in izdelkov za končne uporabnike, ki se uporabljajo pri zagotavljanju teh storitev, v enaki meri kot drugim potrošnikom. Zagotavljane storitve zaupanja in izdelki za končne uporabnike, ki se uporabljajo pri zagotavljanju teh storitev, bi zato morali biti dostopni invalidom, če je to izvedljivo. Pri oceni izvedljivosti bi bilo treba med drugim upoštevati tehnične in ekonomske vidike.

(30) Države članice bi morale imenovati nadzorni organ ali nadzorne organe za izvajanje nadzornih dejavnosti v skladu s to uredbo. Prav tako bi morale imeti možnost, da v dogovoru z drugo državo članico imenujejo nadzorni organ na ozemlju te druge države članice.

(31) Nadzorni organi bi morali sodelovati z organi za varstvo podatkov, na primer z obveščanjem o rezultatih revizij ponudnikov kvalificiranih storitev zaupanja, če se zdi, da so bila kršena pravila o varstvu osebnih podatkov. Sporočanje podatkov bi moralo zajemati zlasti varnostne incidente in kršitve varstva osebnih podatkov.

(32) Vsi ponudniki storitev zaupanja bi morali uporabljati dobro prakso varnosti, ki ustreza tveganjem, povezanim z njihovimi dejavnostmi, da bi okrepili zaupanje uporabnikov v enotni trg.

(33) Določbe o uporabi psevdonimov v potrdilih ne bi smele ovirati držav članic, da zahtevajo identifikacijo oseb v skladu s pravom Unije ali nacionalnim pravom.

(34) Vse države članice bi morale upoštevati skupne bistvene zahteve v zvezi z nadzorom, da se zagotovi primerljiva raven varnosti kvalificiranih storitev zaupanja. Za lažjo dosledno uporabo teh zahtev po vsej Uniji bi morale države članice sprejeti primerljive postopke ter si izmenjevati informacije o nadzornih dejavnostih in najboljših praksah na tem področju.

(35) Zahteve iz te uredbe bi morale veljati za vse ponudnike storitev zaupanja, zlasti zahteve glede varnosti in odgovornosti, da v zvezi s svojimi postopki in storitvami zagotovijo ustrezno skrbnost, preglednost in odgovornost. Vendar je ob upoštevanju vrste storitev, ki jih zagotavljajo ponudniki storitev zaupanja, v zvezi s temi zahtevami ustrezno razlikovati med ponudniki kvalificiranih in ponudniki nekvalificiranih storitev zaupanja.

(36) Vzpostavitev ureditve nadzora za vse ponudnike storitev zaupanja bi morala zagotoviti enake konkurenčne pogoje za varnost in odgovornost v zvezi z njihovimi postopki in storitvami ter s tem prispevati k zaščiti uporabnikov in delovanju notranjega trga. Pri ponudnikih nekvalificiranih storitev zaupanja bi se morale izvajati manj obsežne ter odzivne naknadne nadzorne dejavnosti, ob upoštevanju narave njihovih storitev in postopkov. Nadzorni organ torej ne bi smel imeti splošne obveznosti nadzora ponudnikov nekvalificiranih storitev zaupanja. Ukrepati bi moral le, če je obveščen (na primer s strani ponudnika nekvalificiranih storitev zaupanja samega ali drugega nadzornega organa, z uradnim obvestilom uporabnika ali poslovnega partnerja ali na podlagi svoje lastne preiskave), da ponudnik nekvalificiranih storitev zaupanja ne ravna v skladu z zahtevami iz te uredbe.

([1]) Sklep Sveta 2010/48/ES z dne 26. novembra 2009 o sklenitvi Konvencije Združenih narodov o pravicah invalidov s strani Evropske skupnosti (UL L 23, 27.1.2010, str. 35).

(37) Ta uredba bi morala določiti odgovornost vseh ponudnikov storitev zaupanja. Zlasti vzpostavlja ureditev odgovornosti, v skladu s katero bi morali biti vsi ponudniki storitev zaupanja odgovorni za škodo, ki jo povzročijo fizični ali pravni osebi zaradi neizpolnjevanja obveznosti iz te uredbe. Da bi poenostavili oceno finančnega tveganja, ki bi mu lahko bili izpostavljeni ponudniki storitev zaupanja ali bi moralo biti krito z njihovimi zavarovalnimi policami, ta uredba ponudnikom teh storitev omogoča, da pod določenimi pogoji določijo omejitve glede uporabe storitev, ki jih zagotavljajo, in tako niso odgovorni za škodo zaradi uporabe teh storitev, ki presega takšno omejitev. Potrošniki bi morali biti vnaprej ustrezno obveščeni o omejitvah. Te omejitve bi morale biti prepoznavne za tretje osebe, na primer tako, da se informacije o omejitvah vključijo v splošne pogoje zagotavljane storitve, ali na drug prepoznaven način. Da bi ta načela lahko učinkovala, bi bilo treba to uredbo uporabljati v skladu z nacionalnimi pravili o odgovornosti. Ta uredba tako ne vpliva na navedena nacionalna pravila, na primer o opredelitvi škode, namena (naklepa) in malomarnosti, ali na ustrezna veljavna postopkovna pravila.

(38) Prijave kršitev varnosti in ocene varnostnega tveganja so bistvene, da se lahko ob kršitvi varnosti ali izgubi celovitosti zadevnim stranem zagotovijo ustrezne informacije.

(39) Da bi Komisija in države članice lahko ocenile učinkovitost mehanizma za prijavo kršitev, ki ga uvaja ta uredba, bi morali nadzorni organi Komisiji ter Agenciji Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: agencija ENISA) zagotoviti povzetek informacij.

(40) Da bi Komisija in države članice lahko ocenile učinkovitost mehanizma okrepljenega nadzora, ki ga uvaja ta uredba, bi bilo treba od nadzornih organov zahtevati, da poročajo o svojih dejavnostih. To bi bistveno pripomoglo k boljši izmenjavi dobrih praks med nadzornimi organi ter hkrati zagotovilo preverjanje, da se bistvene zahteve po nadzoru izvajajo dosledno in učinkovito v vseh državah članicah.

(41) Da bi zagotovili vzdržnost in trajnost kvalificiranih storitev zaupanja ter okrepili zaupanje uporabnikov v nepreki-njenost kvalificiranih storitev zaupanja, bi morali nadzorni organi preveriti obstoj in pravilno uporabo določb o načrtih za prenehanje v primerih, ko ponudniki kvalificiranih storitev zaupanja prenehajo opravljati svoje dejavnosti.

(42) Da se olajša nadzor ponudnikov kvalificiranih storitev zaupanja, na primer kadar ponudnik zagotavlja storitve na ozemlju druge države članice in tam ni predmet nadzora ali kadar se računalniki ponudnika nahajajo na ozemlju druge države članice in ne v državi, v kateri ima ponudnik sedež, bi bilo treba vzpostaviti sistem medsebojne pomoči med nadzornimi organi v državah članicah.

(43) Da se zagotovi skladnost ponudnikov kvalificiranih storitev zaupanja in storitev, ki jih ti zagotavljajo, z zahtevami iz te uredbe, bi moral organ za ugotavljanje skladnosti izvajati ugotavljanje skladnosti, njegova poročila o ugotavljanju skladnosti pa bi ponudniki kvalificiranih storitev zaupanja morali predložiti nadzornemu organu. Kadar nadzorni organ od ponudnika kvalificiranih storitev zaupanja zahteva, da predloži poročilo o priložnostnem ugotavljanju skladnosti, bi moral pri tem spoštovati zlasti načela dobrega upravljanja, vključno z obveznostjo utemeljitve svojih odločitev, in načelo sorazmernosti. Zato bi nadzorni organ moral ustrezno utemeljiti svoje odločitve, s katerimi zahteva priložnostno ugotavljanje skladnosti.

(44) Namen te uredbe je zagotoviti skladen okvir, ki bo zagotavljal visoko raven varnosti in pravne varnosti storitev zaupanja. Tozadevno bi morala Komisija pri obravnavi ugotavljanja skladnosti izdelkov in storitev po potrebi iskati sinergije z obstoječimi zadevnimi evropskimi in mednarodnimi sistemi, kot je Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta ([1]), ki določa zahteve za akreditacijo organov za ugotavljanje skladnosti in nadzor trga izdelkov.

([1]) Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30).

(45) Da se omogoči učinkovit postopek za vključitev ponudnikov kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja, ki jih ti zagotavljajo, na zanesljive sezname, bi bilo treba spodbujati predhodno sodelovanje med bodočimi ponudniki kvalificiranih storitev zaupanja in pristojnim nadzornim organom, da se spodbudi ustrezna skrbnost, potrebna za začetek zagotavljanja kvalificiranih storitev zaupanja.

(46) Zanesljivi seznami so bistveni elementi za krepitev zaupanja med udeleženci na trgu, saj je iz njih razvidno, da je imel ponudnik storitev v trenutku nadzora kvalificiran status.

(47) Zaupanje v spletne storitve in njihova uporabnost sta ključna, da bi uporabniki izkoristili vse možnosti elektronskih storitev in se nanje zavestno zanesli. Zato bi bilo treba ustvariti znak zaupanja EU, s katerim bi označili kvalificirane storitve zaupanja, ki jih zagotavljajo ponudniki kvalificiranih storitev zaupanja. Na podlagi takšnega znaka zaupanja EU za kvalificirane storitve zaupanja bi se kvalificirane storitve zaupanja jasno razlikovale od drugih storitev zaupanja, kar bi prispevalo k preglednosti na trgu. Uporaba znaka zaupanja EU s strani ponudnikov kvalificiranih storitev zaupanja bi morala biti prostovoljna in ne bi smela nalagati nobenih drugih zahtev, poleg tistih iz te uredbe.

(48) Čeprav je za zagotavljanje medsebojnega priznavanja elektronskih podpisov potrebna visoka raven varnosti, bi bilo treba v posebnih primerih, denimo v okviru Odločbe Komisije 2009/767/ES ([1]), sprejeti tudi elektronske podpise z nižjo ravnjo varnosti.

(49) Ta uredba bi morala vzpostaviti načelo, da se elektronskemu podpisu ne bi smelo odvzeti pravnega učinka, ker je v elektronski obliki ali ker ne izpolnjuje zahtev za kvalificirani elektronski podpis. Vendar pa se pravni učinek elektronskih podpisov opredeli z nacionalnim pravom, razen kar zadeva zahteve iz te uredbe, v skladu s katerimi bi moral imeti kvalificirani elektronski podpis enakovreden pravni učinek kot lastnoročni podpis.

(50) Ker pristojni organi v državah članicah trenutno uporabljajo različne formate naprednih elektronskih podpisov za elektronsko podpisovanje dokumentov, bi bilo treba zagotoviti, da lahko države članice, ko prejmejo elektronsko podpisane dokumente, tehnično podpirajo vsaj nekaj formatov naprednih elektronskih podpisov. Podobno bi bilo treba v primeru, ko pristojni organi v državah članicah uporabljajo napredne elektronske žige, zagotoviti, da ti podpirajo vsaj nekaj formatov naprednih elektronskih žigov.

(51) Podpisnik bi moral imeti možnost, da naprave za ustvarjanje kvalificiranega elektronskega podpisa zaupa v oskrbo tretji osebi, če se uvedejo ustrezni mehanizmi in postopki, ki zagotavljajo, da ima podpisnik izključni nadzor nad uporabo svojih podatkov za ustvarjanje elektronskega podpisa in da so pri uporabi naprave izpolnjene zahteve za kvalificiran elektronski podpis.

(52) Ustvarjanje elektronskih podpisov na daljavo, pri katerem okolje za ustvarjanje elektronskega podpisa upravlja ponudnik storitev zaupanja v imenu podpisnika, se bo okrepilo, saj prinaša številne gospodarske koristi. Da se zagotovi enako pravno priznavanje takšnih elektronskih podpisov in elektronskih podpisov, ustvarjenih v okolju, ki ga v celoti upravlja uporabnik, pa bi morali ponudniki storitev elektronskih podpisov na daljavo izvajati posebne varnostne postopke pri vodenju in upravljanju ter uporabljati zaupanja vredne sisteme in izdelke, med drugim varne načine elektronske komunikacije, da se zagotovita zanesljivo okolje za ustvarjanje elektronskega podpisa in uporaba tega okolja pod izključnim nadzorom podpisnika. V primeru kvalificiranega elektronskega podpisa, ustvarjenega z napravo za ustvarjanje elektronskega podpisa na daljavo, bi se morale uporabljati zahteve iz te uredbe, ki se uporabljajo za ponudnike kvalificiranih storitev zaupanja.

([1]) Odločba Komisije 2009/767/ES z dne 16. oktobra 2009 o vzpostavitvi ukrepov za pospeševanje uporabe postopkov po elektronski poti s pomočjo „enotnih kontaktnih točk“ po Direktivi 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu (UL L 274, 20.10.2009, str. 36).

(53) Začasna razveljavitev kvalificiranih potrdil je uveljavljena operativna praksa ponudnikov storitev zaupanja v več državah članicah, ki se razlikuje od preklica potrdila in pomeni začasno prenehanje njegove veljavnosti. Zaradi pravne varnosti je potrebno, da je vedno jasno navedeno, da je potrdilo začasno razveljavljeno. Ponudniki storitev zaupanja bi zato morali jasno navesti status potrdila, v primeru njegove začasne razveljavitve pa tudi natančno obdobje, za katero je potrdilo začasno razveljavljeno. Ta uredba ponudnikom storitev zaupanja ali državam članicam ne bi smela nalagati uporabe začasne razveljavitve, morala pa bi zagotavljati pravila o preglednosti, kadar in kjer je taka praksa na voljo.

(54) Čezmejna interoperabilnost in priznavanje kvalificiranih potrdil sta predpogoja za čezmejno priznavanje kvalificiranih elektronskih podpisov. Zato za kvalificirana potrdila ne bi smele veljati nobene obvezne zahteve, ki presegajo zahteve iz te uredbe. Vendar bi bilo treba na nacionalni ravni dovoliti vključitev posebnih lastnosti, kot so enolični identifikatorji, v kvalificirana potrdila, če ne ovirajo čezmejne interoperabilnosti in priznavanja kvalificiranih potrdil in elektronskih podpisov.

(55) Varnostno certificiranje, kar zadeva informacijsko tehnologijo, na podlagi mednarodnih standardov, kot je ISO 15408 ter s tem povezani načini ocenjevanja in ureditve vzajemnega priznavanja, je pomemben način preverjanja varnosti naprav za ustvarjanje kvalificiranega elektronskega podpisa in bi ga bilo treba spodbujati. Vendar so inovativne rešitve in storitve, kot so mobilno podpisovanje in podpisovanje v oblaku, odvisne od tehničnih in organizacijskih rešitev za naprave za ustvarjanje kvalificiranega elektronskega podpisa, za katere varnostni standardi morda še niso na voljo ali za katere prvi postopek varnostnega certificiranja, kar zadeva informacijsko tehnologijo, še ni zaključen. Raven varnosti takšnih naprav za ustvarjanje kvalificiranega elektronskega podpisa bi se lahko ocenila z alternativnimi postopki, samo kadar takšni varnostni standardi še niso na voljo ali kadar prvi postopek varnostnega certificiranja, kar zadeva informacijsko tehnologijo, še ni zaključen. Ti postopki bi morali biti primerljivi s standardi za varnostno certificiranje, kar zadeva informacijsko tehnologijo, če sta njihovi ravni varnosti enakovredni. K tem postopkom bi lahko prispeval medsebojni strokovni pregled.

(56) V tej uredbi bi morale biti določene zahteve za naprave za ustvarjanje kvalificiranega elektronskega podpisa, da se zagotovi funkcionalnost naprednih elektronskih podpisov. Ta uredba ne bi smela zajemati celotnega sistemskega okolja, v katerem takšne naprave delujejo. Zato bi moral biti obseg certificiranja naprav za ustvarjanje kvalificiranega elektronskega podpisa omejen na strojno opremo in sistemsko programsko opremo, ki se uporabljata za upravljanje in varovanje podatkov za ustvarjanje podpisa, ki so ustvarjeni, shranjeni ali obdelani v napravi za ustvarjanje podpisa. Kot je opredeljeno v zadevnih standardih, obveznost certificiranja ne bi smela veljati za aplikacije za ustvarjanje podpisa.

(57) Da se zagotovi pravna varnost glede veljavnosti podpisa, je bistveno opredeliti dele kvalificiranega elektronskega podpisa, ki jih mora zanašajoča se stranka, ki izvaja potrjevanje veljavnosti, oceniti. Poleg tega bi opredelitev zahtev za ponudnike kvalificiranih storitev zaupanja, ki lahko zagotavljajo kvalificirano storitev potrjevanja veljavnosti za zanašajoče se stranke, ki potrjevanja veljavnosti kvalificiranih elektronskih podpisov ne želijo ali ne morejo opravljati same, morala zasebni in javni sektor spodbuditi k naložbam v takšne storitve. Oba elementa bi morala zagotoviti, da je potrjevanje veljavnosti kvalificiranega elektronskega podpisa enostavno in primerno za vse stranke na ravni Unije.

(58) Če transakcija zahteva kvalificirani elektronski žig pravne osebe, bi moral biti enako sprejemljiv tudi kvalificirani elektronski podpis pooblaščenega zastopnika pravne osebe.

(59) Elektronski žigi bi morali služiti kot dokaz, da je elektronski dokument izdala pravna oseba, ter zagotavljati gotovost, kar zadeva izvor in celovitost dokumenta.

(60) Ponudniki storitev zaupanja, ki izdajajo kvalificirana potrdila za elektronski žig, bi morali izvajati potrebne ukrepe, da se omogoči ugotovitev identitete fizične osebe, ki zastopa pravno osebo, ki se ji se izda kvalificirani potrdilo za elektronski žig, če je takšna identifikacija potrebna v okviru sodnega ali upravnega postopka na nacionalni ravni.

(61) Ta uredba bi morala zagotoviti dolgoročno hrambo informacij, da se zagotovi pravna veljavnost elektronskih podpisov in elektronskih žigov v daljšem časovnem obdobju ter da se jih lahko potrdi ne glede na prihodnje tehnološke spremembe.

(62) Da se zagotovi varnost kvalificiranih elektronskih časovnih žigov, bi moralo biti v tej uredbi določena uporaba naprednega elektronskega žiga ali naprednega elektronskega podpisa ali drugih enakovrednih metod. Predvideti je mogoče, da bi se z inovacijami lahko razvile nove tehnologije, ki bi za časovne žige zagotavljale enakovredno raven varnosti. Če se uporabi druga metoda in ne napredni elektronski žig ali napredni elektronski podpis, bi morala biti naloga ponudnika kvalificiranih storitev zaupanja, da v okviru poročila o ugotavljanju skladnosti dokaže, da takšna metoda zagotavlja enakovredno raven varnosti in izpolnjuje zahteve iz te uredbe.

(63) Elektronski dokumenti so pomembni za nadaljnji razvoj čezmejnih elektronskih transakcij na notranjem trgu. Ta uredba bi morala vzpostaviti načelo, da se elektronskemu dokumentu ne bi smelo odvzeti pravnega učinka, ker je v elektronski obliki, s čimer bi se zagotovilo, da elektronska transakcija ne bo zavrnjena le zato, ker je dokument v elektronski obliki.

(64) Komisija bi morala pri obravnavi formatov naprednih elektronskih podpisov in žigov izhajati iz obstoječih praks, standardov in zakonodaje, zlasti Sklepa Komisije 2011/130/EU ([1]).

(65) Poleg avtentikacije dokumenta, ki ga izda pravna oseba, se lahko elektronski žigi uporabijo tudi pri avtentikaciji digitalnih sredstev pravne osebe, kot so programske kode ali strežniki.

(66) Nujno je določiti pravni okvir, da se olajša čezmejno priznavanje storitev elektronske priporočene dostave med obstoječimi nacionalnimi pravnimi sistemi. Ta okvir bi lahko ustvaril tudi nove tržne priložnosti za ponudnike storitev zaupanja iz Unije, ki bi lahko ponujali nove vse-evropske storitve elektronske priporočene dostave.

(67) Storitve za avtentikacijo spletišč obiskovalcu spletišča dajejo zagotovilo, da za tem spletiščem stoji pristen in legitimen subjekt. Te storitve prispevajo h krepitvi zaupanja v poslovanje prek spleta, saj uporabniki zaupajo spletišču, ki je bilo avtenticirano. Zagotavljanje in uporaba storitev za avtentikacijo spletišč sta povsem prostovoljna. Da bi avtentikacija spletišč postala sredstvo za krepitev zaupanja in zagotavljanje boljše izkušnje uporabnikov ter spodbujanje rasti na notranjem trgu, pa bi se moralo s to uredbo določiti minimalne obveznosti glede varnosti in odgovornosti za ponudnike in njihove storitve. V ta namen so bili upoštevani rezultati obstoječih pobud, ki jih je začel zadevni sektor, na primer forum CA/B – Certification Authorities/Browsers Forum. Poleg tega ta uredba ne bi smela ovirati uporabe drugih sredstev ali metod za avtentikacijo spletišč, ki niso zajeti s to uredbo, ponudnikom storitev za avtentikacijo spletišč iz tretjih držav pa ne bi smela preprečevati, da bi svoje storitve zagotavljali strankam v Uniji. Vendar bi se storitve za avtentikacijo spletišč, ki jih zagotavlja ponudnik iz tretje države, morale priznati kot kvalificirane v skladu s to uredbo le, če imata Unija in država sedeža ponudnika sklenjen mednarodni sporazum.

(68) Pojem „pravne osebe“ v skladu z določbami Pogodbe o delovanju Evropske unije (PDEU) o ustanavljanju gospodarskim subjektom omogoča, da svobodno izberejo pravno obliko, za katero menijo, da je primerna za izvajanje njihove dejavnosti. Glede na to pojem „pravne osebe“ v smislu PDEU pomeni vse subjekte, ki so ustanovljeni v skladu s pravom države članice ali zanje velja takšno pravo, ne glede na njihovo pravno obliko.

(69) Institucije, organe, urade in agencije Unije se spodbudi, da priznajo elektronsko identifikacijo in storitve zaupanja, ki jih zajema ta uredba, v okviru upravnega sodelovanja, ki izkorišča zlasti obstoječe dobre prakse in rezultate tekočih projektov na področjih, ki jih zajema ta uredba.

([1]) Sklep Komisije 2011/130/EU z dne 25. februarja 2011 o določitvi minimalnih zahtev glede čezmejne obdelave dokumentov z elektronskim podpisom pristojnih organov v skladu z Direktivo 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu (UL L 53, 26.2.2011, str. 66).

(70) Da bi se nekateri podrobni tehnični vidiki te uredbe lahko prilagodljivo in hitro dopolnili, bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 PDEU sprejme akte v zvezi z merili, ki jih morajo izpolnjevati organi, pristojni za certificiranje naprav za ustvarjanje kvalificiranega elektronskega podpisa. Zlasti je pomembno, da Komisija pri pripravljalnem delu opravi ustrezna posvetovanja, vključno na ravni strokovnjakov. Komisija bi morala pri pripravi in oblikovanju delegiranih aktov zagotoviti, da so ustrezni dokumenti predloženi Evropskemu parlamentu in Svetu istočasno, pravočasno in na ustrezen način.

(71) Za zagotovitev enotnih pogojev izvajanja te uredbe bi bilo treba na Komisijo prenesti izvedbena pooblastila, zlasti za opredelitev referenčnih številk standardov, katerih uporaba bi predstavljala domnevo skladnosti z določenimi zahtevami iz te uredbe. Ta pooblastila bi se morala izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta ([1]).

(72) Komisija bi morala pri sprejemanju delegiranih ali izvedbenih aktov upoštevati standarde in tehnične specifikacije, ki jih pripravijo evropski in mednarodni organi in organizacije za standardizacijo, zlasti Evropski odbor za standardizacijo (CEN), Evropski inštitut za telekomunikacijske standarde (ETSI), Mednarodna organizacija za standardizacijo (ISO) in Mednarodna telekomunikacijska zveza (ITU), da bi zagotovili visoko raven varnosti in interoperabilnosti elektronske identifikacije in storitev zaupanja.

(73) Zaradi pravne varnosti in jasnosti bi bilo treba Direktivo 1999/93/ES razveljaviti.

(74) Da se udeležencem na trgu, ki že uporabljajo kvalificirana potrdila, izdana fizičnim osebam v skladu z Direktivo 1999/93/ES, zagotovi pravna varnost, je treba omogočiti dovolj dolgo prehodno obdobje. Podobno bi bilo treba prehodne ukrepe določiti tudi za naprave za varno ustvarjanje elektronskega podpisa, katerih skladnost je bila ugotovljena v skladu z Direktivo 1999/93/ES, in overitelje, ki izdajajo kvalificirana potrdila pred 1. julijem 2016. Prav tako je treba Komisiji zagotoviti, da lahko sprejme izvedbene in delegirane akte pred tem datumom.

(75) Datumi začetka uporabe iz te uredbe ne vplivajo na obstoječe obveznosti držav članic na podlagi prava Unije, zlasti Direktive 2006/123/ES.

(76) Ker države članice ne morejo zadovoljivo doseči ciljev te uredbe, temveč se zaradi obsega predlaganega ukrepa lažje dosežejo 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) V skladu s členom 28(2) Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta ([2]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je podal mnenje dne 27. septembra 2012 ([3]) –

([1]) Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13).

([2]) Uredba (ES) št. 45/2001 Evropskega parlamenta in Svet z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12,1,2001, str. 1).

([3]) UL C 28, 30.1.2013, str. 6.

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

1. Da se zagotovi pravilno delovanje notranjega trga in doseže ustrezna raven varnosti sredstev elektronske identifikacije in storitev zaupanja, ta uredba:

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

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

(c) določa pravni okvir za elektronske podpise, elektronske žige, elektronske časovne žige, elektronske dokumente, storitve elektronske priporočene dostave in storitve v zvezi s potrdili za avtentikacijo spletišč.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za sheme elektronske identifikacije, ki jih priglasi država članica, in za ponudnike storitev zaupanja s sedežem v Uniji.

2. Ta uredba se ne uporablja za zagotavljanje storitev zaupanja, ki se uporabljajo izključno znotraj zaprtih sistemov, ki obstajajo na podlagi nacionalnega prava ali dogovorov med določeno skupino udeležencev.

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

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

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 pravno osebo;

2. „sredstvo elektronske identifikacije“ pomeni materialno in/ali nematerialno enoto, ki vsebuje identifikacijske podatke osebe in se uporablja za avtentikacijo pri spletnih storitvah;

3. „identifikacijski podatki osebe“ pomeni niz podatkov, ki omogočajo, da se določi identiteta fizične ali pravne osebe ali fizične osebe, ki zastopa pravno osebo;

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

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

6. „zanašajoča se stranka“ pomeni fizično ali pravno osebo, ki se zanaša na elektronsko identifikacijo ali storitev zaupanja;

7. „organ javnega sektorja“ pomeni državni, regionalni ali lokalni organ, osebo javnega prava ali združenje, ki jo/ga ustanovi eden ali več takšnih organov ali ena ali več takšnih oseb javnega prava, ali zasebni subjekt, ki ga je vsaj eden od teh organov, oseb ali združenj pooblastil za zagotavljanje javnih storitev, kadar deluje v okviru tega pooblastila;

8. „oseba javnega prava“, pomeni osebo, opredeljeno v točki 4 člena 2(1) Direktive 2014/24/EU Evropskega parlamenta in Sveta ([1]);

9. „podpisnik“ pomeni fizično osebo, ki ustvari elektronski podpis;

10. „elektronski podpis“ pomeni niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani in jih podpisnik uporablja za podpisovanje;

11. „napredni elektronski podpis“ pomeni elektronski podpis, ki izpolnjuje zahteve iz člena 26;

12. „kvalificirani elektronski podpis“ pomeni napredni elektronski podpis, ki se ustvari z napravo za ustvarjanje kvalificiranega elektronskega podpisa in temelji na kvalificiranem potrdilu za elektronske podpise;

13. „podatki za ustvarjanje elektronskega podpisa“ pomeni enolične podatke, ki jih podpisnik uporablja za ustvarjanje elektronskega podpisa;

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

15. „kvalificirano potrdilo za elektronski podpis“ pomeni potrdilo za elektronske podpise, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge I;

16. „storitev zaupanja“ pomeni elektronsko storitev, ki se praviloma opravlja za plačilo in vključuje:

    (a) ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami, ali

    (b) ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali

    (c) hrambo elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami;

17. „kvalificirana storitev zaupanja“ pomeni storitev zaupanja, ki izpolnjuje zadevne zahteve iz te uredbe;

([1]) Direktiva 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES (UL L 94, 28.3.2014, str. 65).

18. „organ za ugotavljanje skladnosti“ pomeni organ, opredeljen v točki 13 člena 2 Uredbe (ES) št. 765/2008, ki je akreditiran v skladu z navedeno uredbo in je pristojen za ugotavljanje skladnosti ponudnika kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja, ki jih ta zagotavlja;

19. „ponudnik storitev zaupanja“ pomeni fizično ali pravno osebo, ki zagotavlja eno ali več storitev zaupanja, kot ponudnik kvalificiranih ali nekvalificiranih storitev zaupanja;

20. „ponudnik kvalificiranih storitev zaupanja“ pomeni ponudnika storitev zaupanja, ki zagotavlja eno ali več kvalificiranih storitev zaupanja in mu nadzorni organ dodeli kvalificirani status;

21. „izdelek“ pomeni strojno ali programsko opremo ali ustrezne sestavne dele strojne ali programske opreme, katerih uporaba je namenjena zagotavljanju storitev zaupanja;

22. „naprava za ustvarjanje elektronskega podpisa“ pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega podpisa;

23. „naprava za ustvarjanje kvalificiranega elektronskega podpisa“ pomeni napravo za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II;

24. „ustvarjalec žiga“ pomeni pravno osebo, ki ustvari elektronski žig;

25. „elektronski žig“ pomeni niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani, da se zagotovita izvor in celovitost povezanih podatkov;

26. „napredni elektronski žig“ pomeni elektronski žig, ki izpolnjuje zahteve iz člena 36;

27. „kvalificirani elektronski žig“ pomeni napredni elektronski žig, ki se ustvari z napravo za ustvarjanje kvalificiranega elektronskega žiga in temelji na kvalificiranem potrdilu za elektronski žig;

28. „podatki za ustvarjanje elektronskega žiga“ pomenijo enolične podatke, ki jih ustvarjalec elektronskega žiga uporabi za ustvarjanje elektronskega žiga;

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

30. „kvalificirano potrdilo za elektronski žig“ pomeni potrdilo za elektronski žig, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge III;

31. „naprava za ustvarjanje elektronskega žiga“ pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega žiga;

32. „naprava za ustvarjanje kvalificiranega elektronskega žiga“ pomeni napravo za ustvarjanje elektronskega žiga, ki smiselno izpolnjuje zahteve iz Priloge II;

33. „elektronski časovni žig“ pomeni podatke v elektronski obliki, ki druge podatke v elektronski obliki povezujejo z določenim trenutkom in tako zagotavljajo dokaz, da so slednji podatki v tistem trenutku obstajali;

34. „kvalificirani elektronski časovni žig“ pomeni elektronski časovni žig, ki izpolnjuje zahteve iz člena 42;

35. „elektronski dokument“ pomeni kakršno koli vsebino, shranjeno v elektronski obliki, zlasti besedilo ali zvočni, vizualni ali avdiovizualni zapis;

36. „storitev elektronske priporočene dostave“ pomeni storitev, ki omogoča prenos podatkov med tretjimi stranmi z elektronskimi sredstvi, zagotavlja dokaze o ravnanju s prenesenimi podatki, vključno z dokazilom o oddaji in prejemu podatkov, ter prenesene podatke varuje pred izgubo, krajo, poškodbo ali kakršno koli nepooblaščeno spremembo;

37. „kvalificirana storitev elektronske priporočene dostave“ pomeni storitev elektronske priporočene dostave, ki izpolnjuje zahteve iz člena 44;

38. „potrdilo za avtentikacijo spletišč“ pomeni potrdilo, ki omogoča avtentikacijo spletišča in spletišče povezuje s fizično ali pravno osebo, ki se ji izda potrdilo;

39. „kvalificirano potrdilo za avtentikacijo spletišč“ pomeni potrdilo za avtentikacijo spletišč, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge IV;

40. „podatki za potrjevanje veljavnosti“ pomeni podatke, ki se uporabljajo za potrjevanje veljavnosti elektronskega podpisa ali elektronskega žiga;

41. „potrjevanje veljavnosti“ pomeni postopek preverjanja in potrditve, da je elektronski podpis ali žig veljaven.

Člen 4

Načelo notranjega trga

1. Za zagotavljanje storitev zaupanja, ki jih na ozemlju države članice zagotavlja ponudnik storitev zaupanja s sedežem v drugi državi članici, ne veljajo nobene omejitve iz razlogov, ki spadajo na področje uporabe te uredbe.

2. Za izdelke in storitve zaupanja, ki so skladni s to uredbo, se dovoli prosti pretok na notranjem trgu.

Člen 5

Obdelava in varstvo podatkov

1. Obdelava osebnih podatkov se izvaja v skladu z Direktivo 95/46/ES.

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

POGLAVJE II

ELEKTRONSKA IDENTIFIKACIJA

Člen 6

Vzajemno priznavanje

1. Če nacionalno pravo ali upravna praksa za dostop do storitve, ki jo prek spleta zagotavlja organ javnega sektorja v eni državi članici, predpisuje elektronsko identifikacijo z uporabo sredstva elektronske identifikacije in avtentikacije, se sredstvo elektronske identifikacije, izdano v drugi državi članici, prizna v prvi državi članici za namene čezmejne avtentikacije za to spletno storitev, če so izpolnjeni naslednji pogoji:

(a) sredstvo elektronske identifikacije je izdano v okviru sheme elektronske identifikacije, navedene na seznamu, ki ga Komisija objavi v skladu s členom 9;

(b) raven zanesljivosti takšnega sredstva elektronske identifikacije ustreza ravni zanesljivosti, ki je enaka ali višja od ravni zanesljivosti, ki jo zahteva zadevni organ javnega sektorja pri dostopu do spletne storitve v prvi državi članici, pod pogojem, da raven zanesljivosti takšnega sredstva elektronske identifikacije ustreza srednji ali visoki ravni zanesljivosti;

(c) zadevni organ javnega sektorja uporablja srednjo ali visoko raven zanesljivosti v zvezi z dostopom do te spletne storitve.

Takšno priznanje se opravi najpozneje 12 mesecev po tem, ko Komisija objavi seznam iz točke (a) prvega pododstavka.

2. Organi javnega sektorja lahko za namene čezmejne avtentikacije za storitve, ki jih zagotavljajo prek spleta, priznajo sredstvo elektronske identifikacije, ki se izda v okviru sheme elektronske identifikacije, navedene na seznamu, ki ga Komisija objavi v skladu s členom 9, in ustreza nizki ravni zanesljivosti.

Člen 7

Upravičenost do priglasitve shem elektronske identifikacije

Shema elektronske identifikacije je upravičena do priglasitve v skladu s členom 9(1), če so izpolnjeni vsi naslednji pogoji:

(a) sredstva elektronske identifikacije v okviru sheme elektronske identifikacije se izdajo:

(i) s strani države članice priglasiteljice;

(ii) po pooblastilu države članice priglasiteljice, ali

(iii) neodvisno od države članice priglasiteljice, vendar jih ta država članica priznava;

(b) sredstva elektronske identifikacije v okviru sheme elektronske identifikacije se lahko uporabljajo za dostop do vsaj ene storitve, ki jo zagotavlja organ javnega sektorja in za katero se v državi članici priglasiteljici zahteva elektronska identifikacija;

(c) shema elektronske identifikacije in sredstva elektronske identifikacije, izdana v okviru te sheme, izpolnjujejo zahteve vsaj ene od ravni zanesljivosti, določenih v izvedbenem aktu iz člena 8(3);

(d) država članica priglasiteljica zagotovi, da se identifikacijski podatki osebe, ki enolično predstavljajo zadevno osebo, dodelijo fizični ali pravni osebi iz točke 1 člena 3 v skladu s tehničnimi specifikacijami, standardi in postopki za ustrezno raven zanesljivosti, določenimi v izvedbenem aktu iz člena 8(3), ob izdaji sredstva elektronske identifikacije v okviru navedene sheme;

(e) izdajatelj sredstva elektronske identifikacije v okviru navedene sheme, zagotovi, da se sredstvo elektronske identifikacije dodeli osebi iz točke (d) tega člena v skladu s tehničnimi specifikacijami, standardi in postopki za ustrezno raven zanesljivosti, določenimi v izvedbenem aktu iz člena 8(3);

(f) država članica priglasiteljica zagotovi, da je avtentikacija na voljo prek spleta, tako da lahko vsaka zanašajoča se stranka s sedežem na ozemlju druge države članice potrdi identifikacijske podatke osebe, prejete v elektronski obliki.

Za zanašajoče se stranke, ki niso organi javnega sektorja, lahko država članica priglasiteljica določi pogoje dostopa do navedene avtentikacije. Čezmejna avtentikacija je brezplačna, če se opravi v povezavi s spletno storitvijo, ki jo zagotavlja organ javnega sektorja.

Države članice ne uvedejo nobenih posebnih nesorazmernih tehničnih zahtev za zanašajoče se stranke, ki nameravajo opraviti tako avtentikacijo, če takšne zahteve preprečujejo ali znatno ovirajo interoperabilnost priglašenih shem elektronske identifikacije;

(g) vsaj šest mesecev pred priglasitvijo v skladu s členom 9(1) država članica priglasiteljica zagotovi drugim državam članicam v skladu z obveznostjo iz člena 12(5) opis te sheme v skladu s postopkovno ureditvijo, določeno z izvedbenim aktom iz člena 12(7);

(h) shema elektronske identifikacije izpolnjuje zahteve izvedbenega akta iz člena 12(8).

Člen 8

Ravni zanesljivosti shem elektronske identifikacije

1. Shema elektronske identifikacije, priglašena v skladu s členom 9(1), določa nizko, srednjo in/ali visoko raven zanesljivosti, dodeljeno sredstvom elektronske identifikacije, izdanim v okviru te sheme.

2. Nizka, srednja in visoka raven zanesljivosti izpolnjujejo naslednja merila:

(a) nizka raven zanesljivosti se nanaša na sredstvo elektronske identifikacije v okviru sheme elektronske identifikacije, ki zagotavlja omejeno stopnjo zaupanja v izkazano ali zagotavljano identiteto osebe in za katero je značilno sklicevanje na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je zmanjšati nevarnost zlorabe ali spreminjanja identitete;

(b) srednja raven zanesljivosti se nanaša na sredstvo elektronske identifikacije v okviru sheme elektronske identifikacije, ki zagotavlja srednjo stopnjo zaupanja v izkazano ali zagotavljano identiteto osebe in za katero je značilno sklicevanje na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je znatno zmanjšati nevarnost zlorabe ali spreminjanja identitete;

(c) visoka raven zanesljivosti se nanaša na sredstvo elektronske identifikacije v okviru sheme elektronske identifikacije, ki zagotavlja višjo stopnjo zaupanja v izkazano ali zagotavljano identiteto osebe kot sredstva elektronske identifikacije srednje ravni zanesljivosti in za katero je značilno sklicevanje na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je preprečiti nevarnost zlorabe ali spreminjanja identitete.

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 za namene odstavka 1.

Te minimalne tehnične specifikacije, standardi in postopki se določijo ob sklicevanju na zanesljivost in kakovost naslednjih elementov:

(a) postopka za dokazovanje in preverjanje identitete fizičnih ali pravnih oseb, ki zaprosijo za izdajo sredstva elektronske identifikacije;

(b) postopka za izdajo zahtevanega sredstva elektronske identifikacije;

(c) mehanizma avtentikacije, prek katerega fizična ali pravna oseba uporablja sredstvo elektronske identifikacije, da odvisni stranki potrdi svojo identiteto;

(d) izdajatelja sredstva elektronske identifikacije;

(e) katerega koli drugega organa, vključenega v postopek izdaje sredstva elektronske identifikacije, ter

(f) tehničnih in varnostnih specifikacij izdanega sredstva elektronske identifikacije.

Komisija izvedbene akte sprejme v skladu s postopkom pregleda iz člena 48(2).

Člen 9

Priglasitev

1. Država članica priglasiteljica priglasi Komisiji naslednje informacije, brez nepotrebnega odlašanja pa tudi vse njihove naknadne spremembe:

(a) opis sheme elektronske identifikacije, vključno z njenimi ravnmi zanesljivosti in izdajateljem oziroma izdajatelji sredstva elektronske identifikacije v okviru sheme;

(b) veljavno ureditev nadzora in informacije o ureditvi odgovornosti v zvezi s/z:

(i) izdajateljem sredstva elektronske identifikacije, in

(ii) stranko, ki opravi postopek avtentikacije;

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

(d) informacije o subjektu ali subjektih, ki urejajo registracijo enoličnih identifikacijskih podatkov osebe;

(e) opis, kako se izpolnjujejo zahteve, določene v izvedbenih aktih iz člena 12(8);

(f) opis avtentikacije iz točke (f) člena 7;

(g) ureditev začasne razveljavitve ali preklica priglašene elektronske identifikacijske sheme, avtentikacije ali zadevnih ogroženih delov.

2. Eno leto po začetku uporabe izvedbenih aktov iz členov 8(3) in 12(8) Komisija v *Uradnem listu Evropske unije* objavi seznam shem elektronske identifikacije, priglašenih v skladu z odstavkom 1 tega člena, in osnovne informacije o njih.

3. Če Komisija prejme priglasitev po izteku obdobja iz odstavka 2, v *Uradnem listu Evropske unije* objavi spremembe seznama iz odstavka 2 v dveh mesecih po datumu prejema priglasitve.

4. Država članica lahko Komisiji predloži zahtevek, da se s seznama iz odstavka 2 umakne shema elektronske identifikacije, ki jo je ta država članica priglasila. Komisija objavi ustrezne spremembe seznama članice v *Uradnem listu Evropske unije* v enem mesecu po datumu prejema zahtevka države članice.

5. Komisija lahko z izvedbenimi akti določi okoliščine, formate in postopke priglasitve iz odstavka 1. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 10

Kršitev varnosti

1. Ob kršitvi ali delnem ogrožanju bodisi sheme elektronske identifikacije, priglašene v skladu s členom 9(1), ali avtentikacije iz točke (f) člena 7 na način, ki vpliva na zanesljivost čezmejne avtentikacije te sheme, država članica priglasiteljica brez odlašanja začasno razveljavi ali prekliče to čezmejno avtentikacijo ali zadevne ogrožene dele ter o tem obvesti druge države članice in Komisijo.

2. Ko je kršitev ali ogrožanje iz odstavka 1 odpravljeno, država članica priglasiteljica ponovno vzpostavi čezmejno avtentikacijo in o tem brez nepotrebnega odlašanja obvesti druge države članice in Komisijo.

3. Če se kršitev ali ogrožanje iz odstavka 1 ne odpravi v treh mesecih po začasni razveljavitvi ali preklicu, država članica priglasiteljica uradno obvesti druge države članice in Komisijo o umiku sheme elektronske identifikacije.

Komisija v *Uradnem listu Evropske unije* objavi ustrezne spremembe seznama iz člena 9(2) brez nepotrebnega odlašanja.

Člen 11

Odgovornost

1. Država članica priglasiteljica je odgovorna za škodo, ki je namenoma ali iz malomarnosti povzročena fizični ali pravni osebi zaradi neizpolnjevanja obveznosti iz točk (d) in (f) člena 7 pri opravljanju čezmejne transakcije.

2. Izdajatelj sredstva elektronske identifikacije je odgovoren za škodo, ki jo namenoma ali iz malomarnosti povzroči fizični ali pravni osebi zaradi neizpolnjevanja obveznosti iz točke (e) člena 7 pri opravljanju čezmejne transakcije.

3. Stranka, ki opravi postopek avtentikacije, je odgovorna za škodo, ki jo namenoma ali iz malomarnosti povzroči kateri koli fizični ali pravni osebi, če pri opravljanju čezmejne transakcije ne zagotovi pravilnega delovanja avtentikacije iz točke (f) člena 7.

4. Odstavki 1, 2 in 3 se uporabljajo v skladu z nacionalnimi pravili o odgovornosti.

5. Odstavki 1, 2 in 3 ne posegajo v odgovornost, ki jo imajo v skladu z nacionalnim pravom stranke transakcije, pri kateri se uporabljajo sredstva elektronske identifikacije, ki so del sheme elektronske identifikacije, priglašene v skladu s členom 9(1).

Člen 12

Sodelovanje in interoperabilnost

1. Nacionalne sheme elektronske identifikacije, priglašene v skladu s členom 9(1), so interoperabilne.

2. Za namene odstavka 1 se vzpostavi interoperabilnostni okvir.

3. Interoperabilnostni okvir izpolnjuje naslednja merila:

(a) prizadeva si biti tehnološko nevtralen in ne diskriminira med posebnimi nacionalnimi tehničnimi rešitvami za elektronsko identifikacijo znotraj države članice;

(b) upošteva evropske in mednarodne standarde, kadar je mogoče;

(c) lajša izvajanje načela vgrajene zasebnosti, in

(d) zagotavlja, da so osebni podatki obdelani v skladu z Direktivo 95/46/ES.

4. Interoperabilnostni okvir sestavljajo:

(a) sklicevanje na minimalne tehnične zahteve, povezane z ravnmi zanesljivosti iz člena 8;

(b) določitev nacionalnih ravni zanesljivosti priglašenih shem elektronske identifikacije glede na ravni zanesljivosti iz člena 8;

(c) sklicevanje na minimalne tehnične zahteve glede interoperabilnosti;

(d) sklicevanje na minimalni niz identifikacijskih podatkov osebe, ki enolično predstavljajo fizično ali pravno osebo in so dostopni v okviru shem elektronske identifikacije;

(e) poslovnik;

(f) ureditev za reševanje sporov, in

(g) skupni varnostni standardi delovanja.

5. Države članice sodelujejo na naslednjih področjih:

(a) interoperabilnost shem elektronske identifikacije, priglašenih v skladu s členom 9(1), in shem elektronske identifikacije, ki jih države članice nameravajo priglasiti, ter

(b) varnost shem elektronske identifikacije.

6. Sodelovanje med državami članicami vključuje:

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

(b) izmenjavo informacij, izkušenj in dobrih praks v zvezi z delom z ravnmi zanesljivosti za sheme elektronske identifikacije iz člena 8;

(c) medsebojni strokovni pregled shem elektronske identifikacije, zajetih s to uredbo, in

(d) preverjanje zadevnega razvoja v sektorju elektronske identifikacije.

7. Komisija do 18. marca 2015 z izvedbenimi akti določi potrebno postopkovno ureditev za lažje sodelovanje med državami članicami, določeno v odstavkih 5 in 6, da se spodbudi visoka raven zaupanja in varnosti, ki ustreza stopnji nevarnosti.

8. Komisija do 18. septembra 2015 za določitev enotnih pogojev izvajanja zahteve iz odstavka 1 sprejme izvedbene akte o interoperabilnostnem okviru, opredeljenem v odstavku 4, pri tem pa upošteva merila iz odstavka 3 in rezultate sodelovanja med državami članicami.

9. Izvedbeni akti iz odstavkov 7 in 8 tega člena se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

POGLAVJE IIII

STORITVE ZAUPANJA

ODDELEK 1

Splošne določbe

Člen 13

Odgovornost in dokazno breme

1. Brez poseganja v odstavek 2 so ponudniki storitev zaupanja odgovorni za škodo, ki je namenoma ali iz malomarnosti povzročena fizični ali pravni osebi zaradi neizpolnjevanja obveznosti po tej uredbi.

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

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

2. Kadar ponudniki storitev zaupanja svoje stranke ustrezno vnaprej obvestijo o omejitvah uporabe storitev, ki jih zagotavljajo, in kadar tretja stranka te omejitve lahko prepozna, ponudniki storitev zaupanja niso odgovorni za škodo, ki izhaja iz uporabe storitev, ki presega navedene omejitve.

3. Odstavka 1 in 2 se uporabljata v skladu z nacionalnimi pravili o odgovornosti.

Člen 14

Mednarodni vidiki

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

2. Sporazumi iz odstavka 1 zagotavljajo zlasti, da:

(a) ponudniki storitev zaupanja v tretji državi ali mednarodnih organizacijah, s katerimi je sklenjen sporazum, in storitve zaupanja, ki jih zagotavljajo, izpolnjujejo zahteve, ki veljajo za ponudnike kvalificiranih storitev zaupanja s sedežem v Uniji in za kvalificirane storitve zaupanja, ki jih zagotavljajo;

(b) 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 mednarodni organizaciji, s katero je sklenjen sporazum.

Člen 15

Dostopnost za invalide

Če je izvedljivo, so ponujene storitve zaupanja in izdelki za končne uporabnike, ki se uporabljajo pri zagotavljanju teh storitev, dostopni invalidom.

Člen 16

Kazni

Države članice določijo pravila o kaznih, ki se uporabljajo za kršitve te uredbe. Kazni so učinkovite, sorazmerne in odvračilne.

ODDELEK 2

Nadzor

Člen 17

Nadzorni organ

1. Države članice imenujejo nadzorni organ s sedežem na njihovem ozemlju ali – po medsebojnem dogovoru z drugo državo članico – nadzorni organ s sedežem v tej drugi državi članici. Ta organ je odgovoren za nadzorne naloge v državi članici, ki organ imenuje.

Nadzorni organi imajo potrebna pooblastila in ustrezne vire za opravljanje svojih nalog.

2. Države članice Komisijo uradno obvestijo o imenu in naslovu svojih imenovanih nadzornih organov.

3. Vloga nadzornega organa je:

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

(b) po potrebi sprejeti ukrepe v zvezi s ponudniki nekvalificiranih storitev zaupanja s sedežem na ozemlju države članice, ki organ imenuje, na podlagi naknadnega nadzora, kadar je obveščen, da ti ponudniki ali storitve zaupanja, ki jih zagotavljajo, domnevno ne izpolnjujejo zahtev iz te uredbe.

4. Za namene odstavka 3 in ob upoštevanju omejitev iz navedenega odstavka naloge nadzornega organa vključujejo zlasti:

(a) sodelovanje z drugimi nadzornimi organi in zagotavljanje pomoči tem organom v skladu s členom 18;

(b) analizo poročil o ugotavljanju skladnosti iz členov 20(1) in 21(1);

(c) obveščanje drugih nadzornih organov in javnosti o kršitvah varnosti ali izgubi celovitosti v skladu s členom 19(2);

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

(e) izvajanje revizij ali izdajanje zahtevkov organu za ugotavljanje skladnosti, da opravi ugotavljanje skladnosti ponudnikov kvalificiranih storitev zaupanja v skladu s členom 20(2);

(f) sodelovanje z organi za varstvo podatkov, zlasti obveščanje teh organov o rezultatih revizij ponudnikov kvalificiranih storitev zaupanja brez nepotrebnega odlašanja, če se zdi, da so bila kršena pravila o varstvu osebnih podatkov;

(g) odobritev kvalificiranega statusa ponudnikom storitev zaupanja in storitvam, ki jih zagotavljajo, ter odvzem takšnega statusa v skladu s členoma 20 in 21;

(h) obveščanje organa, odgovornega za nacionalni zanesljiv seznam iz člena 22(3), o odločitvah glede odobritve ali odvzema kvalificiranega statusa, razen v primeru, ko je ta organ tudi nadzorni organ;

(i) preverjanje obstoja in pravilne uporabe določb o načrtih za prenehanje zagotavljanja storitve v primerih, ko ponudnik kvalificiranih storitev zaupanja preneha opravljati svoje dejavnosti, vključno z načinom, kako so te informacije dostopne v skladu s točko (h) člena 24(2);

(j) izdajanje zahtevkov ponudnikom storitev zaupanja, da odpravijo morebitno neizpolnjevanje zahtev iz te uredbe.

5. Države članice lahko zahtevajo, da nadzorni organ vzpostavi, vzdržuje in posodablja infrastrukturo zaupanja v skladu s pogoji iz nacionalnega prava.

6. Vsako leto do 31. marca vsak nadzorni organ Komisiji predloži poročilo o svojih glavnih dejavnostih v predhodnem koledarskem letu, skupaj s povzetkom uradnih obvestil o kršitvah, ki jih je prejel od ponudnikov storitev zaupanja v skladu s členom 19(2).

7. Komisija zagotovi, da je letno poročilo iz odstavka 6 na voljo državam članicam.

8. Komisija lahko z izvedbenimi akti opredeli oblike in postopke, ki se nanašajo na poročilo iz odstavka 6. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 18

Medsebojna pomoč

1. Nadzorni organi sodelujejo z namenom izmenjave dobre prakse.

Nadzorni organ na podlagi prejema utemeljenega zahtevka drugega nadzornega organa temu organu zagotovi pomoč, da se lahko dejavnosti nadzornih organov opravijo na skladen način. Medsebojna pomoč lahko vključuje zlasti zahtevke za informacije in nadzorne ukrepe, kot so zahtevki za opravljanje inšpekcijskih pregledov, ki se nanašajo na poročila o ugotavljanju skladnosti iz členov 20 in 21.

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

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

(b) zahtevana pomoč ni sorazmerna z nadzornimi dejavnostmi nadzornega organa, ki jih opravlja v skladu s členom 17;

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

3. Države članice lahko svojim nadzornim organom po potrebi dovolijo, da opravljajo skupne preiskave, v katerih sodeluje osebje nadzornih organov drugih držav članic. Zadevne države članice se v skladu s svojim nacionalnim pravom dogovorijo o ureditvi in postopkih takšnih skupnih ukrepov in jih tudi vzpostavijo.

Člen 19

Varnostne zahteve za ponudnike storitev zaupanja

1. Ponudniki kvalificiranih in nekvalificiranih storitev zaupanja sprejmejo ustrezne tehnične in organizacijske ukrepe za obvladovanje nevarnosti, povezanih z varnostjo storitev zaupanja, ki jih zagotavljajo. Ti ukrepi ob upoštevanju najnovejših tehnoloških dosežkov zagotavljajo, da je raven varnosti sorazmerna s stopnjo nevarnosti. Sprejmejo se zlasti zato, da bi preprečili in čim bolj zmanjšali vpliv varnostnih incidentov ter deležnike obvestili o škodljivih učinkih takih incidentov.

2. Ponudniki kvalificiranih in nekvalificiranih storitev zaupanja o vsaki kršitvi varnosti ali izgubi celovitosti, ki znatno vpliva na zagotovljeno storitev zaupanja ali na osebne podatke, vsebovane v njej, brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po ugotovitvi, uradno obvestijo nadzorni organ, po potrebi pa tudi druge pristojne organe, kot je pristojni nacionalni organ za varnost informacij ali organ za varstvo podatkov.

Kadar je verjetno, da bo kršitev varnosti ali izguba celovitosti negativno vplivala na fizično ali pravno osebo, ki ji je bila zagotovljena storitev zaupanja, ponudnik storitev zaupanja o kršitvi varnosti ali izgubi celovitosti brez nepotrebnega odlašanja uradno obvesti tudi fizično ali pravno osebo.

Uradno obveščeni nadzorni organ po potrebi obvesti nadzorne organe drugih zadevnih držav članic in agencijo ENISA, zlasti če kršitev varnosti ali izguba celovitosti zadeva dve ali več držav članic.

Uradno obveščeni nadzorni organ o tem obvesti javnost ali to zahteva od ponudnika storitev zaupanja, kadar ugotovi, da je razkritje kršitve varnosti ali izgube celovitosti v javnem interesu.

3. Nadzorni organ agenciji ENISA enkrat na leto predloži povzetek uradnih obvestil o kršitvi varnosti in izgubi celovitosti, ki jih je prejel od ponudnikov storitev zaupanja.

4. Komisija lahko z izvedbenimi akti:

(a) dodatno opredeli ukrepe iz odstavka 1 ter

(b) določi oblike in postopke, vključno z roki, ki se uporabljajo za namene odstavka 2.

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

ODDELEK 3

Kvalificirane storitve zaupanja

Člen 20

Nadzor ponudnikov kvalificiranih storitev zaupanja

1. Ponudnike kvalificiranih storitev zaupanja na njihove lastne stroške vsaj vsakih 24 mesecev revidira organ za ugotavljanje skladnosti. Namen revizije je potrditi, ali ponudniki kvalificiranih storitev zaupanja in kvalificirane storitve zaupanja, ki jih zagotavljajo, izpolnjujejo zahteve iz te uredbe. Ponudniki kvalificiranih storitev zaupanja zadevno poročilo o ugotavljanju skladnosti predložijo nadzornemu organu v treh delovnih dneh po njegovem prejemu.

2. Brez poseganja v odstavek 1 lahko nadzorni organ – na stroške teh 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, da so bila pravila o varstvu osebnih podatkov kršena, nadzorni organ obvesti organe za varstvo podatkov o rezultatih svojih revizij.

3. Kadar nadzorni organ zahteva, da ponudnik kvalificiranih storitev zaupanja odpravi vsakršno neizpolnjevanje zahtev iz te uredbe, ta ponudnik pa ne sprejme ustreznih ukrepov – po potrebi v roku, ki ga določi nadzorni organ – lahko nadzorni organ ob upoštevanju zlasti obsega, trajanja in posledic takšnega neizpolnjevanja temu ponudniku ali zadevnim storitvam, ki jih ponudnik zagotavlja, odvzame kvalificirani status ter o tem obvesti organ iz člena 22(3), da se posodobijo zanesljivi seznami iz člena 22(1). Nadzorni organ obvesti ponudnika kvalificiranih storitev zaupanja o odvzemu kvalificiranega statusa temu ponudniku ali zadevnim storitvam.

4. Komisija lahko z izvedbenimi akti določi referenčne številke naslednjih standardov:

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

(b) pravila o reviziji, na podlagi katerih bodo organi za ugotavljanje skladnosti opravili ugotavljanje skladnosti ponudnikov kvalificiranih storitev zaupanja iz odstavka 1.

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

Člen 21

Začetek zagotavljanja kvalificirane storitve zaupanja

1. Kadar nameravajo ponudniki storitev zaupanja brez kvalificiranega statusa začeti zagotavljati kvalificirane storitve zaupanja, svojo namero priglasijo nadzornemu organu ter mu predložijo poročilo o ugotavljanju skladnosti, ki ga izda organ za ugotavljanje skladnosti.

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.

Če nadzorni organ ugotovi, da ponudnik storitev zaupanja in storitve zaupanja, ki jih ti zagotavljajo, izpolnjuje zahteve iz prvega pododstavka, 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).

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.

3. Ponudniki kvalificiranih storitev zaupanja lahko začnejo zagotavljati kvalificirane storitve zaupanja, potem ko je kvalificirani status naveden na zanesljivem seznamu iz člena 22(1).

4. Komisija lahko z izvedbenimi akti določi oblike in postopke za namene odstavkov 1 in 2. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 22

Zanesljivi seznami

1. Vsaka država članica sestavi, vodi in objavi zanesljive sezname, vključno z informacijami o ponudnikih kvalificiranih storitev zaupanja, za katere je odgovorna, skupaj z informacijami o kvalificiranih storitvah zaupanja, ki jih ti ponudniki zagotavljajo.

2. Države članice v obliki, primerni za avtomatizirano obdelavo, na varen način sestavijo, vodijo in objavijo elektronsko podpisane ali ožigosane zanesljive sezname ponudnikov storitev zaupanja iz odstavka 1.

3. Države članice Komisijo brez nepotrebnega odlašanja uradno obvestijo o vseh informacijah o organu, ki je pristojen za sestavljanje, vodenje in objavljanje nacionalnih zanesljivih seznamov, ter podrobnosti o tem, kje so taki seznami objavljeni, o potrdilih, uporabljenih za podpisovanje ali ožigosanje zanesljivih seznamov, ter o vseh njihovih spremembah.

4. Komisija na varen način in v elektronsko podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo, da informacije iz odstavka 3 na voljo javnosti.

5. Komisija do 18. septembra 2015 z izvedbenimi akti določi informacije iz odstavka 1 ter opredeli tehnične specifikacije in oblike za zanesljive sezname, ki se uporabljajo za namene odstavkov 1 do 4. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 23

Znak zaupanja EU za kvalificirane storitve zaupanja

1. Potem ko je na zanesljivem seznamu iz člena 22(1) naveden kvalificirani status iz drugega pododstavka člena 21(2), lahko ponudnik kvalificiranih storitev zaupanja uporabi znak zaupanja EU in tako na preprost, prepoznaven in jasen način označi kvalificirane storitve zaupanja, ki jih zagotavlja.

2. Ponudnik kvalificiranih storitev zaupanja pri uporabi znaka zaupanja EU za kvalificirane storitve zaupanja iz odstavka 1 zagotovi, da je na njegovem spletišču navedena povezava do ustreznega zanesljivega seznama.

3. Komisija do 1. julija 2015 z izvedbenimi akti določi specifikacije glede oblike in zlasti predstavitve, sestave, velikosti in zasnove znaka zaupanja EU za kvalificirane storitve zaupanja. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 24

Zahteve za ponudnike kvalificiranih storitev zaupanja

1. Ob izdaji kvalificiranega potrdila za storitev zaupanja ponudnik kvalificiranih storitev zaupanja z ustreznimi sredstvi in v skladu z nacionalnim pravom preveri identiteto in po potrebi druge posebne lastnosti fizične ali pravne osebe, za katero se izdaja kvalificirano potrdilo.

Ponudnik kvalificiranih storitev zaupanja podatke iz prvega pododstavka preveri bodisi neposredno ali prek tretje osebe v skladu z nacionalnim pravom:

(a) s fizično prisotnostjo fizične osebe ali pooblaščenega predstavnika pravne osebe ali

(b) na daljavo, s pomočjo sredstev elektronske identifikacije, v zvezi s katerimi je bila pred izdajo kvalificiranega potrdila zagotovljena fizična prisotnost fizične osebe ali pooblaščenega predstavnika pravne osebe in ki izpolnjujejo zahteve iz člena 8 v zvezi s „srednjo“ ali „visoko“ ravnjo zanesljivosti, ali

(c) s potrdilom kvalificiranega elektronskega podpisa ali kvalificiranega elektronskega žiga, izdanega v skladu s točko (a) ali (b), ali

(d) s pomočjo drugih načinov identifikacije, ki so priznani na nacionalni ravni in zagotavljajo enakovredno zanesljivost kakor fizična prisotnost. Enakovredno zanesljivost potrdi organ za ugotavljanje skladnosti.

2. Ponudnik kvalificiranih storitev zaupanja, ki zagotavlja kvalificirane storitve zaupanja:

(a) obvesti nadzorni organ o vsaki spremembi pri zagotavljanju svojih kvalificiranih storitev zaupanja ter o nameri o prenehanju opravljanja teh dejavnosti;

(b) zaposluje osebje in po potrebi podizvajalce, ki imajo potrebno strokovno znanje, izkušnje in kvalifikacije ter so zanesljivi in ki so se udeležili ustreznega usposabljanja v zvezi z varnostjo in pravili o varstvu osebnih podatkov ter uporabljajo upravne in upravljavske postopke, ki so v skladu z evropskimi ali mednarodnimi standardi;

(c) kar zadeva tveganje odškodninske odgovornosti v skladu s členom 13, ohranja zadostna finančna sredstva in/ali pridobi ustrezno zavarovanje odgovornosti v skladu z nacionalnim pravom;

(d) pred vstopom v pogodbeno razmerje vsako osebo, ki želi uporabljati kvalificirano storitev zaupanja, jasno in razumljivo 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;

(f) uporablja zaupanja vredne sisteme za shranjevanje podatkov, ki jih prejme, v preverljivi obliki, tako da:

(i) so ti javno dostopni samo, če je bila pridobljena privolitev osebe, na katero se podatki nanašajo,

(ii) lahko le pooblaščene osebe vnašajo podatke in spreminjajo shranjene podatke,

(iii) se lahko preveri avtentičnost podatkov;

(g) sprejme ustrezne ukrepe proti ponarejanju in kraji podatkov;

(h) v ustreznem časovnem obdobju, tudi potem, ko je ponudnik kvalificiranih storitev zaupanja prenehal opravljati dejavnosti, beleži vse pomembne informacije o podatkih, ki jih je izdal in prejel ponudnik kvalificiranih storitev zaupanja, in ohranja dostop do njih, zlasti da se zagotovijo dokazi v pravnih postopkih in neprekinjenost storitve. Beleženje je lahko elektronsko;

(i) ima posodobljen načrt za prenehanje zagotavljanja storitve, da se zagotovi neprekinjenost storitve v skladu z določbami, ki jih preveri nadzorni organ v skladu s točko (i) člena 17(4);

(j) zagotovi zakonito obdelavo osebnih podatkov v skladu z Direktivo 95/46/ES;

(k) v primeru ponudnikov kvalificiranih storitev zaupanja, ki izdajajo kvalificirana potrdila, vzpostavi in posodablja podatkovno zbirko potrdil.

3. Če ponudnik kvalificiranih storitev zaupanja, ki izdaja kvalificirana potrdila, sklene, da se potrdilo prekliče, tak preklic zabeleži v svoji podatkovni zbirki potrdil in pravočasno, v vsakem primeru pa v 24 urah po prejetju zahtevka, objavi, da je potrdilo preklicano. Preklic začne učinkovati takoj po objavi.

4. V zvezi z odstavkom 3 ponudniki kvalificiranih storitev zaupanja, ki izdajajo kvalificirana potrdila, vsaki zanašajoči se stranki zagotovijo informacije o veljavnosti ali preklicu kvalificiranih potrdil, ki so jih izdali. Te informacije so vsaj za posamezna potrdila na voljo kadar koli in tudi po izteku veljavnosti potrdila, in sicer na zanesljiv, brezplačen in učinkovit avtomatiziran način.

5. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za zaupanja vredne sisteme in izdelke, ki izpolnjujejo zahteve iz točk (e) in (f) odstavka 2 tega člena. Zahteve iz tega člena veljajo za izpolnjene, kadar zaupanja vredni sistemi in izdelki izpolnjujejo te standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

ODDELEK 4

Elektronski podpisi

Člen 25

Pravni učinki elektronskih podpisov

1. Elektronskemu podpisu se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker je v elektronski obliki ali ker ne izpolnjuje zahtev za kvalificirani elektronski podpis.

2. Kvalificirani elektronski podpis ima enakovreden pravni učinek kot lastnoročni podpis.

3. Kvalificirani elektronski podpis, ki temelji na kvalificiranem potrdilu, izdanem v eni državi članici, se prizna kot kvalificirani elektronski podpis v vseh drugih državah članicah.

Člen 26

Zahteve za napredne elektronske podpise

Napredni elektronski podpis izpolnjuje naslednje zahteve:

(a) enolično je povezan s podpisnikom;

(b) z njim je mogoče identificirati podpisnika;

(c) ustvari se na podlagi podatkov za ustvarjanje elektronskega podpisa, ki jih podpisnik z visoko stopnjo zaupanja lahko uporablja izključno pod svojim nadzorom, in

(d) s podatki, ki so na ta način podpisani, je povezan tako, da je opazna vsaka naknadna sprememba podatkov.

Člen 27

Elektronski podpisi pri javnih storitvah

1. Če država članica za uporabo spletne storit ve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu, zahteva napredni elektronski podpis, ta država članica prizna napredne elektronske podpise, napredne elektronske podpise, ki temeljijo na kvalificiranem potrdilu za elektronske podpise, in kvalificirane elektronske podpise, ki so vsaj v formatih ali uporabljajo metode, ki so opredeljeni v izvedbenih aktih iz odstavka 5.

2. Če država članica za uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu, zahteva napredni elektronski podpis, ki temelji na kvalificiranem potrdilu, ta država članica prizna napredne elektronske podpise, ki temeljijo na kvalificiranem potrdilu, in kvalificirane elektronske podpise, ki so vsaj v formatih ali uporabljajo metode, ki so opredeljeni v izvedbenih aktih iz odstavka 5.

3. Države članice za čezmejno uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja, ne zahtevajo elektronskega podpisa z višjo ravnjo varnosti, kot jo ima kvalificirani elektronski podpis.

4. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za napredne elektronske podpise. Zahteve za napredne elektronske podpise iz odstavkov 1 in 2 tega člena ter iz člena 26 veljajo za izpolnjene, če napredni elektronski podpis izpolnjuje te standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

5. Komisija do 18. septembra 2015 in ob upoštevanju obstoječih praks, standardov in pravnih aktov Unije z izvedbenimi akti opredeli referenčne formate naprednih elektronskih podpisov ali referenčne metode, če se uporabijo alternativne oblike. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 28

Kvalificirana potrdila za elektronske podpise

1. Kvalificirana potrdila za elektronske podpise morajo izpolnjevati zahteve iz Priloge I.

2. Za kvalificirana potrdila za elektronski podpise ne veljajo nobene obvezne zahteve, ki presegajo zahteve iz Priloge I.

3. Kvalificirana potrdila za elektronske podpise lahko vključujejo neobvezne dodatne posebne lastnosti. Te lastnosti ne vplivajo na interoperabilnost in priznanje kvalificiranih elektronskih podpisov.

4. Če je bilo kvalificirano potrdilo za elektronski podpis po prvotnem aktiviranju preklicano, preneha veljati v trenutku njegovega preklica, status pa se mu v nobenem primeru ne povrne v prejšnje stanje.

5. Države članice lahko določijo nacionalna pravila o začasni razveljavitvi kvalificiranega potrdila za elektronski podpis, pri čemer morata biti izpolnjena naslednja pogoja:

(a) če je kvalificirano potrdilo za elektronski podpis začasno razveljavljeno, to potrdilo za obdobje začasne razveljavitve preneha veljati,

(b) obdobje začasne razveljavitve se jasno navede v podatkovni zbirki potrdil, v tem obdobju pa mora biti iz storitve, ki zagotavlja informacije o statusu potrdila, razvidno, da je kvalificirano potrdilo začasno razveljavljeno.

6. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirana potrdila za elektronski podpis. Zahteve iz Priloge I veljajo za izpolnjene, če kvalificirano potrdilo za elektronski podpis izpolnjuje navedene standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 29

Zahteve za naprave za ustvarjanje kvalificiranega elektronskega podpisa

1. Naprave za ustvarjanje kvalificiranega elektronskega podpisa morajo izpolnjevati zahteve iz Priloge II.

2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za naprave za ustvarjanje kvalificiranega elektronskega podpisa. Zahteve iz Priloge II veljajo za izpolnjene, če naprava za ustvarjanje kvalificiranega elektronskega podpisa izpolnjuje navedene standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 30

Certificiranje naprav za ustvarjanje kvalificiranega elektronskega podpisa

1. Skladnost naprav za ustvarjanje kvalificiranega elektronskega podpisa z zahtevami iz Priloge II certificirajo ustrezni javni ali zasebni organi, ki jih imenujejo države članice.

2. Države članice Komisijo uradno obvestijo o imenih in naslovih javnega ali zasebnega organa iz odstavka 1. Komisija da te informacije na voljo državam članicam.

3. Certificiranje iz odstavka 1 se izvede na podlagi:

(a) postopka varnostne ocene, izvedenega v skladu z enim od standardov za ocenjevanje varnosti izdelkov informacijske tehnologije s seznama, vzpostavljenega v skladu z drugim pododstavkom, ali

(b) postopka, ki ni postopek iz točke (a), če uporablja primerljive ravni varnosti ter če javni ali zasebni organ iz odstavka 1 o njem uradno obvesti Komisijo. Ta postopek se lahko uporabi le, če standardov iz točke (a) ni ali če postopek varnostne ocene iz točke (a) še poteka.

Komisija z izvedbenimi akti vzpostavi seznam standardov za oceno varnosti izdelkov informacijske tehnologije iz točke (a). Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

4. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 47, v zvezi z določitvijo posebnih meril, ki jih morajo izpolnjevati imenovani organi iz odstavka 1 tega člena.

Člen 31

Objava seznama certificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa

1. Države članice Komisijo brez nepotrebnega odlašanja, najpozneje pa en mesec po zaključku postopka certificiranja, uradno obvestijo o informacijah o napravah za ustvarjanje kvalificiranega elektronskega podpisa, ki so jih certificirali organi iz člena 30(1). Komisijo brez nepotrebnega odlašanja, najpozneje pa en mesec po razveljavitvi certificiranja, uradno obvestijo tudi o informacijah o napravah za ustvarjanje elektronskega podpisa, ki niso več certificirane.

2. Komisija na podlagi prejetih informacij pripravi, objavi in vodi seznam certificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa.

3. Komisija lahko z izvedbenimi akti določi formate in postopke, ki se uporabljajo za namene odstavka 1. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 32

Zahteve za potrjevanje veljavnosti kvalificiranih elektronskih podpisov

1. S postopkom potrjevanja veljavnosti kvalificiranega elektronskega podpisa se potrdi veljavnost kvalificiranega elektronskega podpisa 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 bil veljaven v času podpisa;

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

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

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

(f) je bil elektronski podpis ustvarjen z napravo za ustvarjanje kvalificiranega elektronskega podpisa;

(g) celovitost podpisanih podatkov ni ogrožena;

(h) so bile v času podpisa izpolnjene zahteve iz člena 26.

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

3. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za potrjevanje veljavnosti kvalificiranih elektronskih podpisov. Zahteve iz odstavka 1 veljajo za izpolnjene, če so pri potrjevanju veljavnosti kvalificiranih elektronskih podpisov izpolnjeni ti standardi. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 33

Kvalificirana storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov

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

(a) potrjevanje veljavnosti opravi v skladu s členom 32(1) in

(b) zanašajočim se strankam omogoči, da prejmejo rezultat postopka potrjevanja veljavnosti na zanesljiv in učinkovit avtomatiziran način, ki je označen z naprednim elektronskim podpisom ali naprednim elektronskim žigom ponudnika kvalificiranih storitev potrjevanja veljavnosti.

2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirano storitev potrjevanja veljavnosti iz odstavka 1. Zahteve iz odstavka 1 veljajo za izpolnjene, če storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov izpolnjuje te standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 34

Kvalificirana storitev hrambe kvalificiranih elektronskih podpisov

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

2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirano storitev hrambe kvalificiranih elektronskih podpisov. Zahteve iz odstavka 1 veljajo za izpolnjene, če ureditve za kvalificirano storitev hrambe kvalificiranih elektronskih podpisov izpolnjujejo te standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

ODDELEK 5

Elektronski žigi

Člen 35

Pravni učinki elektronskih žigov

1. Elektronskemu žigu se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker je v elektronski obliki ali ne izpolnjuje zahtev za kvalificirane elektronske žige.

2. V zvezi s kvalificiranim elektronskim žigom se domneva celovitost podatkov in pravilnost izvora teh podatkov, s katerimi je kvalificirani elektronski žig povezan.

3. Kvalificirani elektronski žig, ki temelji na kvalificiranem potrdilu, izdanem v eni državi članici, se prizna kot kvalificirani elektronski žig v vseh drugih državah članicah.

Člen 36

Zahteve za napredne elektronske žige

Napredni elektronski žig izpolnjuje naslednje zahteve:

(a) enolično je povezan z ustvarjalcem žiga;

(b) z njim je mogoče identificirati ustvarjalca žiga;

(c) ustvari se na podlagi podatkov za ustvarjanje elektronskega žiga, ki jih ustvarjalec žiga z visoko stopnjo zaupanja in pod svojim nadzorom lahko uporablja za ustvarjanje elektronskega žiga, in

(d) povezan je s podatki, na katere se nanaša, in sicer tako, da je mogoče zaslediti vsako naknadno spremembo teh podatkov.

Člen 37

Elektronski žigi pri javnih storitvah

1. Če država članica za uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu, zahteva napredni elektronski žig, ta država članica prizna napredne elektronske žige, napredne elektronske žige, ki temeljijo na kvalificiranem potrdilu za elektronske žige, in kvalificirane elektronske žige, ki so vsaj v formatih ali uporabljajo metode, ki so opredeljeni v izvedbenih aktih iz odstavka 5.

2. Če država članica za uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu, zahteva napredni elektronski žig, ki temelji na kvalificiranem potrdilu, ta država članica prizna napredne elektronske žige, ki temeljijo na kvalificiranem potrdilu, in kvalificirane elektronske žige, ki so vsaj v formatih ali uporabljajo metode, ki so opredeljeni v izvedbenih aktih iz odstavka 5.

3. Države članice za čezmejni dostop do spletne storitve, ki jo zagotavlja organ javnega sektorja, ne zahtevajo elektronskega žiga z višjo ravnjo varnosti, kot jo ima kvalificirani elektronski žig.

4. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za napredne elektronske žige. Zahteve za napredne elektronske žige iz odstavkov 1 in 2 tega člena ter iz člena 36 veljajo za izpolnjene, če napredni elektronski žig izpolnjuje te standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

5. Komisija do 18. septembra 2015 in ob upoštevanju obstoječih praks, standardov in pravnih aktov Unije z izvedbenimi akti določi referenčne formate naprednih elektronskih žigov ali referenčne metode, če so uporabljene alternativne oblike. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 38

Kvalificirana potrdila za elektronske žige

1. Kvalificirana potrdila za elektronske žige morajo izpolnjevati zahteve iz Priloge III.

2. Za kvalificirana potrdila za elektronske žige ne veljajo nobene obvezne zahteve, ki presegajo zahteve iz Priloge III.

3. Kvalificirana potrdila za elektronske žige lahko vključujejo neobvezne dodatne posebne lastnosti. Te lastnosti ne vplivajo na interoperabilnost in priznanje kvalificiranih elektronskih žigov.

4. Če je bilo kvalificirano potrdilo za elektronski žig po prvotnem aktiviranju preklicano, preneha veljati v trenutku njegovega preklica, status pa se mu v nobenem primeru ne povrne v prejšnje stanje.

5. Države članice lahko določijo nacionalna pravila o začasni razveljavitvi kvalificiranih potrdil za elektronske žige, pri čemer morata biti izpolnjena naslednja pogoja:

(a) če je kvalificirano potrdilo za elektronski žig začasno razveljavljeno, ta potrdilo v obdobju začasne razveljavitve preneha veljati;

(b) obdobje začasne razveljavitve se jasno navede v podatkovni zbirki potrdil, v tem obdobju pa mora biti iz storitve, ki zagotavlja informacije o statusu potrdila, razvidno, da je kvalificirano potrdilo začasno razveljavljeno.

6. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirana potrdila za elektronske žige. Zahteve iz Priloge III veljajo za izpolnjene, če kvalificirano potrdilo za elektronski žig izpolnjuje navedene standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

Člen 39

Naprave za ustvarjanje kvalificiranega elektronskega žiga

1. Člen 29 se smiselno uporablja za zahteve za naprave za ustvarjanje kvalificiranega elektronskega žiga.

2. Člen 30 se smiselno uporablja za certificiranje naprav za ustvarjanje kvalificiranega elektronskega žiga.

3. Člen 31 se smiselno uporablja za objavo seznama certificiranih naprav za ustvarjanje kvalificiranega elektronskega žiga.

Člen 40

Potrjevanje veljavnosti in hramba kvalificiranih elektronskih žigov

Členi 32, 33 in 34 se smiselno uporabljajo za potrjevanje veljavnosti in hrambo kvalificiranih elektronskih žigov.

ODDELEK 6

Elektronski časovni žig

Člen 41

Pravni učinek elektronskih časovnih žigov

1. Elektronskemu časovnemu žigu se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker je v elektronski obliki ali ne izpolnjuje zahtev za kvalificirani elektronski časovni žig.

2. V zvezi s kvalificiranim elektronskim časovnim žigom se domneva pravilnost navedenega datuma in časa ter celovitost podatkov, s katerimi sta datum in čas povezana.

3. Kvalificirani elektronski časovni žig, izdan v eni državi članici, se prizna kot kvalificirani elektronski časovni žig v vseh državah članicah.

Člen 42

Zahteve za kvalificirane elektronske časovne žige

1. Kvalificirani elektronski časovni žig izpolnjuje naslednje zahteve:

(a) datum in čas povezuje s podatki tako, da je mogoče razumno izključiti možnost spremembe podatkov, ne da bi bila ta sprememba zaznana;

(b) temelji na točnem časovnem viru, povezanem z univerzalnim koordiniranim časom;

(c) podpisan je z naprednim elektronskim podpisom ali ožigosan z naprednim elektronskim žigom ponudnika kvalificiranih storitev zaupanja ali z drugo enakovredno metodo.

2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za povezovanje datuma in časa s podatki in za točne časovne vire. Skladnost z zahtevami iz odstavka 1 velja za izpolnjeno, če povezava datuma in časa s podatki in točen časovni vir izpolnjujeta navedene standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

ODDELEK 7

Storitev elektronske priporočene dostave

Člen 43

Pravni učinek storitve elektronske priporočene dostave

1. Podatkom, poslanim in prejetim s storitvijo elektronske priporočene dostave, se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker so v elektronski obliki ali ne izpolnjujejo zahtev za kvalificirano storitev elektronske priporočene dostave.

2. V zvezi s podatki, poslanimi in prejetimi s storitvijo kvalificirane elektronske priporočene dostave, se domneva, da so podatki celoviti, da jih je poslal njihov pošiljatelj in prejel njihov naslovnik, katerih identiteta je ugotovljena, ter da so točni glede datuma in časa oddaje in prejema podatkov, navedenih v okviru kvalificirane storitve elektronske priporočene dostave.

Člen 44

Zahteve za kvalificirane storitve elektronske priporočene dostave

1. Kvalificirane storitve elektronske priporočene dostave izpolnjujejo naslednje zahteve:

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

(b) z visoko stopnjo zaupanja zagotavljajo identifikacijo pošiljatelja;

(c) zagotavljajo identifikacijo naslovnika pred dostavo podatkov;

(d) oddaja in prejem podatkov je zavarovano z naprednim elektronskim podpisom ali naprednim elektronskim žigom ponudnika kvalificiranih storitev zaupanja, tako da je izključena možnost spremembe podatkov, ne da bi bila ta sprememba zaznana;

(e) vsaka sprememba podatkov, potrebna za pošiljanje ali prejem podatkov, se jasno sporoči pošiljatelju in naslovniku podatkov;

(f) s kvalificiranim elektronskim časovnim žigom se navedeta datum in čas oddaje, prejema in vseh sprememb podatkov;

Pri prenašanju podatkov med dvema ali več ponudniki kvalificiranih storitev zaupanja veljajo zahteve iz točk (a) do (f) za vse ponudnike kvalificiranih storitev zaupanja.

2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za postopke pošiljanja in prejemanja podatkov. Zahteve iz odstavka 1 veljajo za izpolnjene, če postopek pošiljanja in prejemanja podatkov izpolnjuje navedene standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

ODDELEK 8

Avtentikacija spletišč

Člen 45

Zahteve za kvalificirana potrdila za avtentikacijo spletišč

1. Kvalificirana potrdila za avtentikacijo spletišč izpolnjujejo zahteve iz Priloge IV.

2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirana potrdila za avtentikacijo spletišč. Zahteve iz Priloge IV se štejejo za izpolnjene, če kvalificirano potrdilo za avtentikacijo spletišč izpolnjuje navedene standarde. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 48(2).

POGLAVJE IV

ELEKTRONSKI DOKUMENTI

Člen 46

Pravni učinki elektronskih dokumentov

Elektronskemu dokumentu se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker je v elektronski obliki.

POGLAVJE V

PRENOS POOBLASTILA IN IZVEDBENE DOLOČBE

Člen 47

Izvajanje pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.

2. Pooblastilo za sprejemanje delegiranih aktov iz člena 30(4) se prenese na Komisijo za nedoločen čas od 17. septembra 2014.

3. Pooblastilo iz člena 30(4) lahko kadar koli prekliče Evropski parlament ali Svet. Z odločitvijo o preklicu preneha veljati prenos pooblastila, naveden v tej odločitvi. Odločitev začne učinkovati dan po njeni objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je v njej določen. Odločitev ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Takoj ko Komisija sprejme delegirani akt, o tem istočasno uradno obvesti Evropski parlament in Svet.

5. Delegirani akt, sprejet v skladu s členom 30(4), začne veljati le, če niti Evropski parlament niti Svet ne nasprotuje delegiranemu aktu v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če sta pred iztekom tega roka tako Evropski parlament kot Svet obvestila Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.

Člen 48

Postopek v odboru

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.

2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

POGLAVJE VI

KONČNE DOLOČBE

Člen 49

Pregled

Komisija pregleda uporabo te uredbe in poroča Evropskemu parlamentu in Svetu najpozneje 1. julija 2020. Komisija oceni zlasti, ali bi bilo ustrezno spremeniti področje uporabe te uredbe ali njene posebne določbe, vključno s členi 6, točko (f) člena 7 in členi 34, 43, 44 in 45, pri tem pa upošteva izkušnje, pridobljene pri uporabi te uredbe, pa tudi tehnološke, tržne in pravne spremembe.

Poročilu iz prvega odstavka se po potrebi priložijo zakonodajni predlogi.

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

Člen 50

Razveljavitev

1. Direktiva 1999/93/ES se razveljavi z učinkom od 1. julija 2016.

2. Sklicevanje na razveljavljeno direktivo se razume kot sklicevanje na to uredbo.

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 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 štejejo za kvalificirana potrdila za elektronske podpise po tej uredbi do izteka njihove veljavnosti.

3. Overitelj, ki izdaja kvalificirana potrdila na podlagi Direktive 1999/93/ES, nadzornemu organu čim prej oziroma najpozneje do 1. julija 2017 predloži poročilo o ugotavljanju skladnosti. Dokler overitelj ne predloži zadevnega poročila o ugotavljanju skladnosti in nadzorni organ ne zaključi ocene skladnosti, se ta overitelj šteje za ponudnika kvalificiranih storitev zaupanja na podlagi te uredbe.

4. Če overitelj, ki izdaja kvalificirana potrdila na podlagi Direktive 1999/93/ES, nadzornemu organu v roku iz odstavka 3 ne predloži poročila o ugotavljanju skladnosti, se ta overitelj od 2. julija 2017 ne šteje za ponudnika kvalificiranih storitev zaupanja na podlagi te uredbe.

Člen 52

Začetek veljavnosti

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

2. Ta uredba se uporablja od 1. julija 2016, z naslednjimi izjemami:

(a) členi 8(3), 9(5), 12(2) do (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) in (5), 28(6), 29(2), 30(3) in (4), 31(3), 32(3), 33(2), 34(2), 37(4) in (5), 38(6), 42(2), 44(2), 45(2), ter člena 47 in 48 se uporabljajo od 17. septembra 2014;

(b) člen 7, člen 8(1) in (2), členi 9, 10, 11 ter člen 12(1) se uporabljajo od datuma začetka uporabe izvedbenih aktov iz členov 8(3) in 12(8);

(c) člen 6 se začne uporabljati tri leta po datumu začetka uporabe izvedbenih aktov iz členov 8(3) in 12(8).

3. Če se priglašena shema elektronske identifikacije navede na seznamu, ki ga Komisija objavi v skladu s členom 9, pred datumom iz točke (c) odstavka 2 tega člena, se sredstva elektronske identifikacije v okviru te sheme priznajo na podlagi člena 6 najpozneje 12 mesecev po objavi te sheme, vendar ne pred datumom iz točke (c) odstavka 2 tega člena.

4. Ne glede na točko (c) odstavka 2 tega člena lahko država članica sklene, da se sredstva elektronske identifikacije v okviru sheme elektronske identifikacije, ki jo na podlagi člena 9(1) priglasi druga država članica, priznajo v prvi državi članici od datuma začetka uporabe izvedbenih aktov iz členov 8(3) in 12(8). Zadevne države članice obvestijo Komisijo. Komisija te informacije objavi.

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

V Bruslju, 23. julija 2014

Za Parlament	*Za Svet*
Predsednik	*Predsednik*
M. SCHULZ	S. GOZI

PRILOGA I

ZAHTEVE V ZVEZI S KVALIFICIRANIMI POTRDILI ZA ELEKTRONSKE PODPISE

Kvalificirana potrdila za elektronske podpise vsebujejo:

(a) navedbo, vsaj v formatu, primernem za avtomatizirano obdelavo, da je bilo potrdilo izdano kot kvalificirano potrdilo za elektronski podpis;

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

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

— za fizične osebe: ime osebe;

(c) vsaj ime podpisnika ali psevdonim; če je uporabljen psevdonim, se to jasno navede;

(d) podatke za potrjevanje veljavnosti elektronskega podpisa, ki ustrezajo podatkom za ustvarjanje elektronskega podpisa;

(e) podrobnosti o začetku in koncu veljavnosti potrdila;

(f) identifikacijsko šifro potrdila, ki je enolična za ponudnika kvalificiranih storitev zaupanja;

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

(h) lokacijo, kjer je potrdilo, ki podpira napredni elektronski podpis ali napredni elektronski žig iz točke (g), na voljo brezplačno;

(i) lokacijo storitev, s katerimi je mogoče preveriti veljavnost kvalificiranega potrdila;

(j) če se podatki za ustvarjanje elektronskega podpisa, povezani s podatki za potrjevanje veljavnosti elektronskega podpisa, nahajajo v napravi za ustvarjanje kvalificiranega elektronskega podpisa, se to ustrezno navede vsaj v formatu, primernem za avtomatizirano obdelavo.

PRILOGA II

ZAHTEVE V ZVEZI Z NAPRAVAMI ZA USTVARJANJE KVALIFICIRANEGA ELEKTRONSKEGA PODPISA

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

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

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

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

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

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

3. Podatke za ustvarjanje elektronskega podpisa lahko v imenu podpisnika pridobiva ali upravlja le ponudnik kvalificiranih storitev zaupanja.

4. Ponudniki kvalificiranih storitev zaupanja, ki v imenu podpisnika upravljajo podatke za ustvarjanje elektronskega podpisa, lahko brez poseganja v točko (d) točke 1 podatke za ustvarjanje elektronskega podpisa podvajajo le za namene varnostne kopije, pod pogojem, da sta izpolnjeni naslednji zahtevi:

   (a) varnost podvojenih naborov podatkov je enaka ravni, ki jo ima varnost prvotnih naborov podatkov;

   (b) število podvojenih naborov podatkov ni večje, kot je to nujno potrebno, da se zagotovi neprekinjenost storitve.

PRILOGA III

ZAHTEVE V ZVEZI S KVALIFICIRANIMI POTRDILI ZA ELEKTRONSKE ŽIGE

Kvalificirana potrdila za elektronske žige vsebujejo:

(a) navedbo, vsaj v formatu, primernem za avtomatizirano obdelavo, da je bilo potrdilo izdano kot kvalificirano potrdilo za elektronski žig;

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

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

— za fizične osebe: ime osebe;

(c) vsaj ime ustvarjalca žiga in po potrebi registrsko številko, kot sta navedena v uradnih evidencah;

(d) podatke za potrjevanje veljavnosti elektronskega žiga, ki ustrezajo podatkom za ustvarjanje elektronskega žiga;

(e) podrobnosti o začetku in koncu veljavnosti potrdila;

(f) identifikacijsko šifro potrdila, ki je enolična za ponudnika kvalificiranih storitev zaupanja;

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

(h) lokacijo, kjer je potrdilo, ki podpira napredni elektronski podpis ali napredni elektronski žig iz točke (g), na voljo brezplačno;

(i) lokacijo storitev, s katerimi je mogoče preveriti veljavnost kvalificiranega potrdila;

(j) če se podatki za ustvarjanje elektronskega žiga, povezani s podatki za potrjevanje elektronskega žiga, nahajajo v napravi za ustvarjanje kvalificiranega elektronskega žiga, se to ustrezno navede vsaj v formatu, primernem za avtomatizirano obdelavo.

PRILOGA IV

ZAHTEVE ZA KVALIFICIRANA POTRDILA ZA AVTENTIKACIJO SPLETIŠČ

Kvalificirana potrdila za avtentikacijo spletišč vsebujejo:

(a) navedbo, vsaj v formatu, primernem za avtomatizirano obdelavo, da je bilo potrdilo izdano kot kvalificirano potrdilo za avtentikacijo spletišč;

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

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

— za fizične osebe: ime osebe;

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

za pravne osebe: vsaj ime pravne osebe, za katero se izdaja potrdilo, in po potrebi registrsko številko, kot sta navedena v uradnih evidencah;

(d) elemente naslova fizične ali pravne osebe, za katero se izdaja potrdilo, vključno vsaj s krajem in državo, po potrebi, kot so navedeni v uradnih evidencah;

(e) ime/imena domene, ki jo upravlja fizična ali pravna oseba, za katero se izdaja potrdilo;

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

(g) identifikacijsko šifro potrdila, ki je enolična za ponudnika kvalificiranih storitev zaupanja;

(h) napredni elektronski podpis ali napredni elektronski žig ponudnika kvalificiranih storitev zaupanja, ki izdaja potrdilo;

(i) lokacijo, na kateri je potrdilo, ki podpira napredni elektronski podpis ali napredni elektronski žig iz točke (h), na voljo brezplačno;

(j) lokacijo storitev za preverjanje veljavnosti potrdila, s katerimi je mogoče preveriti veljavnost kvalificiranega potrdila.