# UREDBA (EU) br. 910/2014 EUROPSKOG PARLAMENTA I VIJEĆA

## od 23. srpnja 2014.

## o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskog gospodarskog i socijalnog odbora ([1]),

u skladu s redovnim zakonodavnim postupkom ([2]),

budući da:

(1) Izgradnja povjerenja u *online* okruženje ključna je za gospodarski i socijalni razvoj. Zbog nedostatka povjerenja, posebno zbog osjećaja pravne nesigurnosti, potrošači, poduzeća i tijela javne vlasti oklijevaju provoditi transakcije elektroničkim putem te koristiti odnosno uvoditi nove usluge.

(2) Ovom Uredbom nastoji se povećati povjerenje u elektroničke transakcije na unutarnjem tržištu pružanjem zajedničkog temelja za sigurnu elektroničku interakciju između građana, poduzećâ i tijela javne vlasti, povećavajući time djelotvornost javnih i privatnih *online* usluga, elektroničkog poslovanja i elektroničke trgovine u Uniji.

(3) Direktivom 1999/93/EZ Europskog parlamenta i Vijeća ([3]) uređeni su elektronički potpisi, no nije utvrđen sveobuhvatan prekogranični i međusektorski okvir za sigurne i vjerodostojne elektroničke transakcije te elektroničke transakcije koje bi bile jednostavne za korištenje. Ovom se Uredbom unapređuje i širi pravna stečevina navedene Direktive.

(4) U Komunikaciji Komisije od 26. kolovoza 2010. pod nazivom „Digitalni program za Europu" rascjepkanost digitalnog tržišta, nedostatak interoperabilnosti i povećanje mrežnog kriminala prepoznati su kao glavne prepreke uspješnom ciklusu digitalnog gospodarstva. U svome Izvješću EU-a o građanstvu iz 2010. pod nazivom „Ukidanje prepreka za prava građana EU-a" Komisija je dodatno istaknula nužnost rješavanja glavnih poteškoća koje građane Unije priječe u korištenju pogodnostima digitalnog jedinstvenog tržišta i prekograničnih digitalnih usluga.

(5) U svojim zaključcima od 4. veljače 2011. i 23. listopada 2011. Europsko vijeće pozvalo je Komisiju da do 2015. uspostavi jedinstveno digitalno tržište radi brzog napretka u ključnim područjima digitalnog gospodarstva i promicanja potpuno integriranog jedinstvenog digitalnog tržišta olakšavanjem prekogranične uporabe *online* usluga, uz pridavanje posebne pozornosti olakšavanju sigurne elektroničke identifikacije i autentikacije.

([1]) SL C 351, 15.11.2012., str. 73.
([2]) Stajalište Europskog parlamenta od 3. travnja 2014. (još nije objavljeno u Službenom listu) i Odluka Vijeća od 23. srpnja 2014.
([3]) Direktiva 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise (SL L 13, 19.1.2000., str. 12.).

(6) Vijeće je u svojim zaključcima od 27. svibnja 2011. pozvalo Komisiju da doprinese jedinstvenom digitalnom tržištu stvaranjem odgovarajućih uvjeta za uzajamno priznavanje ključnih prekograničnih čimbenika, kao što su elektronička identifikacija, elektronički dokumenti, elektronički potpisi i usluge elektroničke dostave, te uvjeta za interoperabilne usluge e-uprave širom Europske unije.

(7) Europski parlament je u svojoj rezoluciji od 21. rujna 2010. o dovršetku formiranja unutarnjeg tržišta za elektroničku trgovinu ([1]) naglasio važnost sigurnosti elektroničkih usluga, naročito elektroničkih potpisa, i potrebu za stvaranjem infrastrukture javnog ključa (Public Key Infrastructure – PKI) na paneuropskoj razini, te je pozvao Komisiju da uspostavi europski portal tijelâ za validaciju radi osiguravanja prekogranične interoperabilnosti elektroničkih potpisa i povećavanja sigurnosti transakcija koje se obavljaju putem interneta.

(8) Direktivom 2006/123/EZ Europskog parlamenta i Vijeća ([2]) od država članica se zahtijeva uspostava „jedinstvenih kontaktnih točaka" („JKT") kako bi se osiguralo da se svi postupci i formalnosti povezani s pristupom uslužnoj djelatnosti i obavljanjem uslužne djelatnosti mogu lako obaviti, na daljinu i elektroničkim putem, preko odgovarajućeg JKT-a ili putem odgovarajućih tijela. Mnoge *online* usluge koje su dostupne putem JKT-a iziskuju elektroničku identifikaciju, autentikaciju i potpis.

(9) U većini slučajeva građani ne mogu koristiti elektroničku identifikaciju u svrhu autentikacije u drugoj državi članici jer nacionalni sustavi elektroničke identifikacije u njihovoj zemlji nisu priznati u drugim državama članicama. Zbog te elektroničke prepreke pružatelji usluga ne mogu koristiti sve pogodnosti unutarnjeg tržišta. Uzajamno priznata sredstva elektroničke identifikacije olakšat će prekogranično pružanje brojnih usluga na unutarnjem tržištu te poduzećima omogućiti prekogranično poslovanje bez suočavanja s brojnim preprekama u interakcijama s tijelima javne vlasti.

(10) Direktivom 2011/24/EU Europskog parlamenta i Vijeća ([3]) uspostavljena je mreža nacionalnih tijela odgovornih za eZdravstvo. Radi veće sigurnosti i kontinuiteta prekogranične zdravstvene zaštite, mreža bi trebala izrađivati smjernice o prekograničnom pristupu elektroničkim podacima i uslugama u području zdravstva, uključujući pružanjem podrške „zajedničkim mjerama za identifikaciju i autentikaciju radi olakšavanja prenosivosti podataka u prekograničnoj zdravstvenoj zaštiti". Uzajamno priznavanje elektroničke identifikacije i autentikacije ključ je ostvarivanja prekogranične zdravstvene zaštite za europske građane. Kada ljudi putuju radi liječenja, njihovi medicinski podaci moraju biti dostupni u zemlji u kojoj se liječe. To iziskuje čvrst, siguran i pouzdan okvir elektroničke identifikacije.

(11) Ova Uredba trebala bi se primjenjivati uz puno poštovanje načela povezanih sa zaštitom osobnih podataka predviđenih u Direktivi 95/46/EZ Europskog parlamenta i Vijeća ([4]). U tom pogledu, s obzirom na načelo uzajamnog priznavanja uspostavljeno ovom Uredbom, autentikacija bi se za *online* uslugu trebala odnositi na obradu samo onih identifikacijskih podataka koji su odgovarajući, relevantni i nisu preopsežni, za odobravanje pristupa toj usluzi *online*. Nadalje, pružatelji usluga povjerenja i nadležna tijela trebali bi poštovati zahtjeve prema Direktivi 95/46/EZ koji se tiču povjerljivosti i sigurnosti obrade.

(12) Jedan od ciljeva ove Uredbe jest uklanjanje postojećih prepreka u prekograničnom korištenju sredstvima elektroničke identifikacije koja se koriste u državama članicama za autentikaciju, barem za javne usluge. Ova Uredba nema za cilj zadirati u elektroničke sustave upravljanja identitetom i s njima povezane infrastrukture uspostavljene u državama članicama. Cilj ove Uredbe jest osigurati da pri pristupu prekograničnim *online* uslugama koje nude države članice postoji mogućnost sigurne elektroničke identifikacije i autentikacije.

([1]) SL C 50, 21.2.2012., str. 1.
([2]) Direktiva 2006/123/EZ Europskog parlamenta i Vijeća od 12. prosinca 2006..o uslugama na unutarnjem tržištu (SL L 376, 27.12.2006., str. 36.).
([3]) Direktiva 2011/24/EU Europskog parlamenta i Vijeća od 9. ožujka 2011. o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi (SL L 88, 4.4.2011., str. 45.).
([4]) Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL L 281, 23.11.1995., str. 31.).

(13) Države članice bi i dalje trebale biti u mogućnosti koristiti se sredstvima za potrebe elektroničke identifikacije radi pristupa *online* uslugama ili uvoditi takva sredstva. Također bi trebale moći odlučiti hoće li uključiti privatni sektor u pružanje tih sredstava. Države članice ne bi trebale biti obvezne Komisiji prijaviti svoje sustave elektroničke identifikacije. Države članice mogu birati hoće li Komisiji prijaviti sve sustave, pojedine sustave ili joj uopće neće prijaviti sustave elektroničke identifikacije koji se koriste na nacionalnoj razini za pristup barem javnim *online* uslugama ili specifičnim uslugama.

(14) U ovoj Uredbi moraju biti određeni izvjesni uvjeti o tome koja sredstva elektroničke identifikacije moraju biti priznata i o načinu na koji bi sustave elektroničke identifikacije trebalo prijaviti. Ti bi uvjeti trebali pomoći državama članicama da izgrade nužno međusobno povjerenje u njihove sustave elektroničke identifikacije i uzajamno priznaju sredstva elektroničke identifikacije koja su obuhvaćena njihovim prijavljenim sustavima. Načelo uzajamnog priznavanja trebalo bi vrijediti ako sustav elektroničke identifikacije države članice koja provodi prijavljivanje ispunjava uvjete prijavljivanja i ako je prijava objavljena u *Službenom listu Europske unije*. Međutim, načelo uzajamnog priznavanja trebalo bi se odnositi samo na autentikaciju na *online* uslugu. Pristup tim *online* uslugama i njihovo konačno pružanje podnositelju trebali bi biti usko povezani s pravom primanja takvih usluga pod uvjetima određenima nacionalnim zakonodavstvom.

(15) Obveza priznavanja sredstava elektroničke identifikacije trebala bi se odnositi samo na ona sredstva čija razina osiguranja identiteta odgovara razini koja je jednaka ili viša od razine koja se zahtijeva za dotičnu *online* uslugu. Pored toga, ta obveza trebala bi se primjenjivati samo kada dotično tijelo javnog sektora koristi razinu sigurnosti koja je „značajna" ili „visoka" u odnosu na pristup toj usluzi *online*. U skladu s pravom Unije, države članice trebale bi i dalje imati slobodu priznavanja sredstava elektroničke identifikacije koja imaju niže razine osiguranja identiteta.

(16) Razine osiguranja identiteta trebale bi označivati stupanj pouzdanja u sredstva elektroničke identifikacije pri utvrđivanju identiteta osobe te na taj način osigurati da osoba koja se predstavlja pod određenim identiteom stvarno jest osoba kojoj je taj identitet dodijeljen. Razina sigurnosti ovisi o stupnju pouzdanja koji sredstvo elektroničke identifikacije pruža u odnosu na traženi ili utvrđeni identitet osobe uzimajući u obzir postupke (na primjer dokazivanje identiteta i verifikaciju te autentikaciju), aktivnosti upravljanja (na primjer tijelo koje izdaje sredstva elektroničke identifikacije i postupak izdavanja takvih sredstava) i provedene tehničke kontrole. Postoje različite tehničke definicije i opisi razina sigurnosti koje su posljedica opsežnih pilot-istraživanja financiranih sredstvima Unije, kao i normizacije i međunarodnih aktivnosti. Posebice, opsežni pilot-projekti STORK i ISO 29115 odnose se, između ostalog, na razine 2, 3 i 4, o čemu bi trebalo voditi u najvećoj mogućoj mjeri računa pri određivanju minimalnih tehničkih zahtjeva, normi i postupaka za nisku, značajnu i visoku razinu sigurnosti u smislu ove Uredbe, osiguravajući pritom dosljednu primjenu ove Uredbe, posebno u pogledu visoke razine sigurnosti koja se odnosi na dokazivanje identiteta za izdavanje kvalificiranih certifikata. Utvrđeni zahtjevi trebali bi biti tehnološki neutralni. Neophodne sigurnosne zahtjeve trebalo bi biti moguće ispuniti primjenom različitih tehnologija.

(17) Države članice trebale bi poticati privatni sektor da dobrovoljno koristi sredstva elektroničke identifikacije u okviru prijavljenog sustava u svrhu identifikacije kada je to potrebno za *online* usluge ili elektroničke transakcije. Mogućnost korištenja takvim sredstvima elektroničke identifikacije privatnom bi sektoru omogućila da se pouzda u elektroničku identifikaciju i autentikaciju koje se već uvelike koriste u mnogim državama članicama barem za javne usluge, a poduzećima i građanima olakšala bi pristup prekograničnim *online* uslugama. Kako bi se privatnom sektoru olakšalo korištenje takvim sredstvima prekogranične elektroničke identifikacije, mogućnost autentikacije koju osiguravaju pojedine države članice trebala bi biti dostupna pouzdajućim stranama privatnog sektora s poslovnim nastanom izvan državnog područja te države članice pod istim onim uvjetima koji se primjenjuju na pouzdajuće strane privatnog sektora s poslovnim nastanom unutar te države članice. Shodno tome, u pogledu pouzdajućih strana privatnog sektora, država članica koja provodi prijavljivanje može odrediti uvjete pristupa sredstvima autentikacije. Ti uvjeti pristupa mogu ukazivati na to jesu li sredstva autentikacije koja se odnose na prijavljeni sustav trenutno dostupna pouzdajućim stranama privatnog sektora.

(18) Ova Uredba trebala bi predvidjeti odgovornost države članice koja provodi prijavljivanje, strane koja izdaje sredstva elektroničke identifikacije i strane koja provodi postupak autentikacije za neispunjavanje odgovarajućih obveza prema ovoj Uredbi. Međutim, ova bi se Uredba trebala primjenjivati u skladu s nacionalnim pravilima o odgovornosti. Prema tome, ona ne utječe na nacionalna pravila, primjerice, o definiciji štete ili na pravila o odgovarajućim postupovnim pravilima koja su na snazi, uključujući teret dokaza.

(19) Sigurnost sustava elektroničke identifikacije ključna je za vjerodostojno prekogranično uzajamno priznavanje sredstava elektroničke identifikacije. U vezi s tim, države članice trebale bi surađivati u pogledu sigurnosti i interoperabilnosti sustavâ elektroničke identifikacije na razini Unije. Uvijek kada sustavi elektroničke identifikacije zahtijevaju da pouzdajuće strane na nacionalnoj razini koriste poseban hardver ili softver, prekogranična interoperabilnost traži od tih država članica da pouzdajućim stranama s poslovnim nastanom izvan njihovog državnog područja ne nameće takve zahtjeve i pripadajuće troškove. U tom slučaju trebalo bi razmotriti i razviti odgovarajuća rješenja unutar područja primjene okvira za interoperabilnost. S druge strane, neizbježni su tehnički zahtjevi koji proizlaze iz nužno povezanih specifikacija nacionalnih sredstava elektroničke identifikacije i koji bi mogli utjecati na imatelje takvih elektroničkih sredstava (npr. pametnih kartica).

(20) Suradnja država članica trebala bi olakšati tehničku interoperabilnost prijavljenih sustava elektroničke identifikacije u cilju poticanja visoke razine pouzdanosti i sigurnosti sukladno stupnju rizika. Razmjena informacija i najbolje prakse među državama članicama u cilju njihova uzajamnog priznavanja trebale bi pomoći takvoj suradnji.

(21) Ovom bi se Uredbom također trebao uspostaviti opći pravni okvir za korištenje uslugama povjerenja. Međutim, njome se ne bi trebalo uvesti opću obvezu njihovog korištenja ili uvođenja pristupne točke za sve postojeće usluge povjerenja. Posebice, ona ne bi smjela obuhvaćati pružanje usluga koje se isključivo koriste unutar zatvorenih sustava među utvrđenom skupinom sudionika koji nemaju nikakav utjecaj na treće strane. Primjerice, sustavi uspostavljeni u poduzećima ili upravama javnih tijela radi upravljanja internim postupcima koji koriste usluge povjerenja ne bi trebali biti podložni zahtjevima ove Uredbe. Samo usluge povjerenja koje se pružaju javnosti i koje imaju učinke na treće strane trebale bi ispunjavati zahtjeve utvrđene u Uredbi. Ova Uredba ne bi trebala obuhvaćati ni aspekte koji se odnose na sklapanje i valjanost ugovorâ ili drugih pravnih obveza ako postoje zahtjevi vezani uz oblik utvrđeni nacionalnim pravom ili pravom Unije. Osim toga, ona ne bi trebala utjecati na nacionalne zahtjeve vezane uz oblik koji vrijede za javne registre, a posebno trgovačke registre i zemljišne knjige.

(22) Radi doprinosa njihovom općem prekograničnom korištenju, trebalo bi biti moguće usluge povjerenja koristiti kao dokaze u sudskim postupcima u svim državama članicama. Pravne učinke usluga povjerenja potrebno je odrediti nacionalnim pravom, osim ako je drukčije predviđeno ovom Uredbom.

(23) U mjeri u kojoj se ovom Uredbom stvara obveza priznavanja usluge povjerenja, takva usluga povjerenja može biti odbijena samo ako je osoba na koju se obveza odnosi, zbog tehničkih razloga na koje ona ne može neposredno utjecati, nije u mogućnosti učitati ili verificirati tu uslugu. Međutim, ta obveza sama po sebi ne bi smjela od javnog tijela zahtijevati nabavu hardvera ili softvera potrebnih za tehničku mogućnost učitavanja svih postojećih usluga povjerenja.

(24) Države članice mogu zadržati ili uvesti nacionalne odredbe koje se odnose na usluge povjerenja, u skladu s pravom Unije, ako te usluge nisu u potpunosti usklađene s ovom Uredbom. Međutim, usluge povjerenja koje su u skladu s ovom Uredbom trebale bi slobodno cirkulirati na unutarnjem tržištu.

(25) Države članice trebale bi i dalje moći slobodno određivati druge vrste usluga povjerenja, uz one koje su dio konačnog popisa usluga povjerenja predviđenog ovom Uredbom, u svrhu njihovog priznavanja na nacionalnoj razini kao kvalificiranih usluga povjerenja.

(26) Zbog brzine tehnoloških promjena, ovom Uredbom trebalo bi usvojiti pristup otvoren za inovacije.

(27) Ova Uredba trebala bi biti tehnološki neutralna. Pravni učinci koji se njome osiguravaju trebali bi biti ostvarivi bilo kojim tehničkim sredstvima pod uvjetom da su zahtjevi ove Uredbe ispunjeni.

(28) Kako bi se povećalo povjerenje posebice malih i srednjih poduzeća (MSP-ova) te potrošača u unutarnje tržište i promicalo korištenje uslugama povjerenja i proizvodima povjerenja, trebalo bi uvesti pojmove „kvalificirana usluga povjerenja" i „kvalificirani pružatelj usluga povjerenja" s ciljem naznačivanja zahtjeva i obveza koji osiguravaju visoku razinu sigurnosti svih kvalificiranih usluga povjerenja i proizvoda povjerenja koji se koriste ili pružaju.

(29) U skladu s obvezama prema Konvenciji Ujedinjenih naroda o pravima osoba s invaliditetom, koja je odobrena Odlukom Vijeća 2010/48/EZ ([1]), a posebno člankom 9. Konvencije, osobe s invaliditetom trebale bi moći koristiti usluge povjerenja i proizvode za krajnjeg korisnika koji se koriste pri pružanju tih usluga na ravnopravnoj osnovi s drugim potrošačima. Stoga bi, gdje je to moguće, usluge povjerenja i proizvodi za krajnjeg korisnika koji se koriste pri pružanju tih usluga trebali biti dostupni osobama s invaliditetom. Procjena izvedivosti trebala bi, između ostalog, uključivati tehničke i ekonomske aspekte.

(30) Države članice trebale bi odrediti nadzorno tijelo ili nadzorna tijela za provedbu nadzornih aktivnosti prema ovoj Uredbi. Države članice također bi trebale moći odlučivati, na temelju uzajamnog dogovora s drugom državom članicom, o određivanju nadzornog tijela na državnom području te druge države članice.

(31) Nadzorna tijela trebala bi surađivati s tijelima za zaštitu podataka, primjerice na način da ih obavješćuju o rezultatima revizija kvalificiranih pružatelja usluga povjerenja, u slučaju kada se čini da je došlo do povrede pravila o zaštiti osobnih podataka. Pružanje informacija trebalo bi posebno obuhvaćati sigurnosne incidente te povrede povezane s osobnim podacima.

(32) Svi pružatelji usluga povjerenja trebali bi biti dužni primjenjivati dobru sigurnosnu praksu primjerenu rizicima koji su povezani s njihovim aktivnostima kako bi se ojačalo povjerenje korisnikâ u jedinstveno tržište.

(33) Odredbe o korištenju pseudonimom u certifikatima ne bi trebale sprečavati države članice da zahtijevaju identifikaciju osoba na temelju prava Unije ili nacionalnog prava.

(34) Sve države članice trebale bi poštovati zajedničke osnovne kriterije nadzora radi osiguravanja usporedive sigurnosne razine zaštite kvalificiranih usluga povjerenja. Radi olakšavanja dosljedne primjene tih zahtjeva širom Unije, države članice trebale bi usvojiti usporedive postupke i razmjenjivati informacije o svojim aktivnostima nadzora i najboljoj praksi u tom području.

(35) Svi pružatelji usluga povjerenja trebali bi biti podvrgnuti zahtjevima ove Uredbe, posebno onima koji se tiču sigurnosti i odgovornosti kako bi se osigurala odgovarajuća brzina pružanja i transparentnost njihovih djelatnosti i usluga te odgovornost za njihove djelatnosti i usluge. Međutim, uzimajući u obzir vrstu usluga koje pružaju pružatelji usluga povjerenja, potrebno je, u pogledu tih zahtjeva, razlikovati između kvalificiranih i nekvalificiranih pružatelja usluga povjerenja.

(36) Uspostavljanje sustava nadzora za sve pružatelje usluga povjerenja trebalo bi osigurati ravnopravne tržišne uvjete u odnosu na sigurnost i odgovornost njihovih djelatnosti i usluga, doprinoseći na taj način zaštiti korisnikâ i funkcioniranju unutarnjeg tržišta. Nekvalificirani pružatelji usluga povjerenja trebali bi biti podvrgnuti neobvezujućim i reaktivnim naknadnim (*ex post*) nadzornim aktivnostima koje su opravdane zbog prirode njihovih usluga i djelatnosti. Nadzorno tijelo stoga ne bi trebalo imati opću obvezu nadzora nekvalificiranih davatelja usluga. Nadzorno tijelo trebalo bi djelovati samo kada je obaviješteno (primjerice od strane samog nekvalificiranog pružatelja usluga povjerenja, drugog nadzornog tijela, putem prijave korisnika ili poslovnog partnera ili na temelju vlastite istrage) da nekvalificirani pružatelj usluga povjerenja ne ispunjava zahtjeve ove Uredbe.

([1]) Odluka Vijeća 2010/48/EZ od 26. studenoga 2009. o sklapanju Konvencije Ujedinjenih naroda o pravima osoba s invaliditetom od strane Europske zajednice (SL L 23, 27.1.2010., str. 35.).

(37) Ovom bi se Uredbom trebala predvidjeti odgovornost svih pružatelja usluga povjerenja. Njome se posebno uspostavlja sustav odgovornosti prema kojemu bi svi pružatelji usluga povjerenja trebali biti odgovorni za štetu nanesenu svakoj fizičkoj ili pravnoj osobi zbog neispunjavanja obveza u skladu s ovom Uredbom. Kako bi se olakšala procjena financijskog rizika koji bi pružatelji usluga povjerenja mogli snositi ili koji bi trebali pokriti policama osiguranja, ovom se Uredbom dopušta pružateljima usluga povjerenja da odrede ograničenja, pod određenim uvjetima, za korištenje uslugama koje oni pružaju te da ne podliježu odgovornosti za štete povezane s korištenjem uslugama koje prelazi takva ograničenja. Korisnike usluga trebalo bi na odgovarajući način i unaprijed obavješćivati o tim ograničenjima. Ta ograničenja trebala bi biti prepoznatljiva trećim osobama, na primjer, uvrštavanjem informacija o ograničenjima u uvjete poslovanja za pruženu uslugu ili putem drugih dopustivih sredstava. U svrhu provedbe tih načela u praksi, ovu bi Uredbu trebalo primjenjivati u skladu s nacionalnim pravilima o odgovornosti. Ova Uredba stoga ne utječe na nacionalna pravila, primjerice, o definiranju šteta, namjeri, nepažnji ili odgovarajuća postupovna pravila koja su na snazi.

(38) Prijava povreda sigurnosti i procjena sigurnosnog rizika neophodna je radi pružanja odgovarajuće informacije zainteresiranim stranama, u slučaju povrede sigurnosti ili narušavanja cjelovitosti.

(39) Kako bi Komisija i države članice mogle procijeniti djelotvornost mehanizma za prijavu povreda koji se uvodi ovom Uredbom, od nadzornih tijela trebalo bi zatražiti da Komisiji i Agenciji Europske unije za sigurnost mreža i podataka (ENISA) dostave sažete informacije.

(40) Kako bi Komisija i države članice mogle procijeniti djelotvornost mehanizma pojačanog nadzora koji se uvodi ovom Uredbom, od nadzornih tijela trebalo bi zatražiti da izvješćuju o svojim aktivnostima. Time bi se olakšala razmjena dobre prakse između nadzornih tijela i osigurala provjera dosljedne i učinkovite provedbe osnovnih kriterija nadzora u svim državama članicama.

(41) Radi osiguravanja održivosti i trajnosti kvalificiranih usluga povjerenja i jačanja pouzdanja korisnikâ u kontinuitet kvalificiranih usluga povjerenja, nadzorna tijela trebala bi provjeriti postojanje i pravilnu primjenu odredaba o planovima za slučaj prekida pružanja usluga u slučajevima kada kvalificirani pružatelji usluga povjerenja prestanu obavljati svoju djelatnost.

(42) Radi olakšavanja nadzora kvalificiranih pružatelja usluga povjerenja, primjerice kada pružatelj pruža svoje usluge na državnom području druge države članice u kojoj ne podliježe nadzoru, ili kada su računala pružatelja smještena na državnom području države članice koja nije država u kojoj ima poslovni nastan, trebalo bi uspostaviti sustav uzajamne pomoći među nadzornim tijelima u državama članicama.

(43) Kako bi se osigurala usklađenost kvalificiranih pružatelja usluga povjerenja i usluga koje oni pružaju sa zahtjevima određenima u ovoj Uredbi, tijelo za ocjenu sukladnosti trebalo bi provoditi ocjenjivanja sukladnosti, a tako dobivena izvješća o ocjenjivanju sukladnosti kvalificirani pružatelji usluga povjerenja trebali bi podnositi nadzornom tijelu. Uvijek kada nadzorno tijelo od kvalificiranog pružatelja usluga povjerenja zahtijeva podnošenje *ad hoc* izvješća o ocjenjivanju sukladnosti, to nadzorno tijelo trebalo bi posebno poštovati načela dobrog upravljanja, uključujući obvezu obrazlaganja svojih odluka, kao i načelo proporcionalnosti. Stoga bi nadzorno tijelo trebalo na odgovarajući način obrazložiti svoju odluku kojom zahtijeva *ad hoc* ocjenjivanje sukladnosti.

(44) Cilj ove Uredbe jest osiguravanje dosljednog okvira radi pružanja visoke razine sigurnosti i pravne sigurnosti usluga povjerenja. U tom pogledu, kada se govori o ocjenjivanju sukladnosti proizvodâ i usluga, Komisija bi, prema potrebi, trebala težiti sinergijama s postojećim relevantnim europskim i međunarodnim sustavima poput Uredbe (EZ) br. 765/2008 Europskog parlamenta i Vijeća [1] o utvrđivanju zahtjeva za akreditaciju tijela za ocjenjivanje sukladnosti i za nadzor tržišta proizvoda.

[1] Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 (SL L 218, 13.8.2008., str. 30.).

(45) Kako bi se omogućilo učinkovito pokretanje postupka koji bi trebao dovesti do uvrštavanja kvalificiranih pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje oni pružaju na pouzdane popise, trebalo bi poticati prethodno zajedničko djelovanje između potencijalnih pružatelja kvalificiranih usluga povjerenja i nadležnog nadzornog tijela radi olakšavanja dubinske analize koja vodi do pružanja kvalificiranih usluga povjerenja.

(46) Pouzdani popisi bitni su elementi pri izgradnji povjerenja među tržišnim operatorima jer upućuju na kvalificirani status pružatelja usluga u trenutku nadzora.

(47) Pouzdanje u uporabu *online* usluga i jednostavnost njihove uporabe imaju presudno značenje za to da njihovi korisnici mogu u potpunosti iskoristiti prednosti elektroničkih usluga i svjesno se pouzdati u njih. U tu svrhu trebalo bi stvoriti kvalificirani EU znak pouzdanosti kako bi se utvrdile kvalificirane usluge povjerenja koje pružaju kvalificirani pružatelji usluga povjerenja. Takvim EU znakom pouzdanosti za kvalificirane usluge povjerenja jasno bi se razlučile kvalificirane usluge povjerenja od drugih usluga povjerenja čime bi se doprinijelo transparentnosti na tržištu. Korištenje EU znakom pouzdanosti trebalo bi biti dobrovoljno za kvalificirane pružatelje usluga povjerenja te ne bi trebalo stvarati bilo koji drugi zahtjev osim onih koji su već predviđeni ovom Uredbom.

(48) Iako je za osiguravanje uzajamnog priznavanja elektroničkih potpisa potrebna visoka razina sigurnosti, u posebnim slučajevima, kao na primjer u kontekstu Odluke Komisije 2009/767/EZ [1], elektronički potpisi s nižom razinom sigurnosne zaštite također bi trebali biti prihvaćeni.

(49) Ovom bi Uredbom trebalo uspostaviti načelo prema kojem se elektroničkom potpisu ne bi smio uskratiti pravni učinak zbog toga što je on u elektroničkom obliku ili zbog toga što ne ispunjava zahtjeve kvalificiranog elektroničkog potpisa. Međutim, pravne učinke elektroničkih potpisa, osim zahtjeva predviđenih u ovoj Uredbi prema kojima bi kvalificirani elektronički potpis trebao imati jednake pravne učinke kao vlastoručni potpis, potrebno je odrediti nacionalnim pravom.

(50) Budući da nadležna tijela u državama članicama trenutno koriste različite formate naprednih elektroničkih potpisa za elektroničko potpisivanje svojih dokumenata, potrebno je osigurati da države članice mogu tehnički podržati barem određeni broj formata naprednih elektroničkih potpisa kada prime elektronički potpisane dokumente. Slično tomu, kada nadležna tijela u državama članicama koriste napredne elektroničke pečate, bilo bi potrebno osigurati da podržavaju barem određeni broj formata naprednih elektroničkih pečata.

(51) Potpisnik bi trebao moći povjeriti kvalificirana sredstva za izradu elektroničkog potpisa na čuvanje trećoj osobi, pod uvjetom da postoje odgovarajući mehanizmi i postupci kojima se osigurava da potpisnik ima isključivu kontrolu nad korištenjem svojim podacima za izradu elektroničkog potpisa, te da su pri korištenju tim sredstvom ispunjeni zahtjevi za kvalificirani elektronički potpis.

(52) Izradu udaljenih elektroničkih potpisa kada okruženjem za izradu elektroničkog potpisa u ime potpisnika upravlja pružatelj usluga povjerenja trebalo bi povećati s obzirom na s time povezane višestruke gospodarske koristi. Međutim, kako bi se osiguralo da takvi elektronički potpisi budu u pravnom smislu jednako priznati kao i elektronički potpisi koji su u potpunosti izrađeni u okruženju kojim upravlja korisnik, pružatelji usluge udaljenog elektroničkog potpisa trebali bi primjenjivati posebne postupke upravljanja i postupke sigurnosnog administriranja te koristiti vjerodostojne sustave i proizvode, uključujući sigurne elektroničke komunikacijske kanale, kako bi jamčili da je okruženje za izradu elektroničkog potpisa pouzdano i da se koristi pod isključivom kontrolom potpisnika. Kada je kvalificirani elektronički potpis izrađen korištenjem sredstva za izradu udaljenog elektroničkog potpisa, trebali bi se primjenjivati zahtjevi primjenjivi na kvalificirane pružatelje usluge povjerenja određeni ovom Uredbom.

[1] Odluka Komisije 2009/767/EZ od 16. listopada 2009. o utvrđivanju mjera kojima se olakšava uporaba postupaka elektroničkim putem preko „jedinstvenih kontaktnih točaka" u skladu s Direktivom 2006/123/EZ Europskog parlamenta i Vijeća o uslugama na unutarnjem tržištu (SL L 274, 20.10.2009., str. 36.).

(53) Suspenzija kvalificiranih certifikata ustaljena je praksa postupanja pružatelja usluga povjerenja u nizu država članica, a razlikuje se od opoziva te podrazumijeva privremeni gubitak valjanosti certifikata. Zbog razloga pravne sigurnosti suspenzija certifikata uvijek mora biti jasno naznačena. U tu bi svrhu pružatelji usluga povjerenja trebali biti odgovorni za jasno naznačavanje statusa certifikata i, ako je certifikat suspendiran, točnog razdoblja suspenzije. Ovom se Uredbom pružateljima usluga povjerenja ili državama članicama ne bi trebala nametati primjena suspenzije, već bi trebalo predvidjeti pravila o transparentnosti kada i ako je takva praksa dostupna.

(54) Prekogranična interoperabilnost i priznavanje kvalificiranih certifikata preduvjet je za prekograničnо priznavanje kvalificiranih elektroničkih potpisa. Kvalificirani certifikati stoga ne bi trebali podlijegati obveznim zahtjevima koji prelaze zahtjeve utvrđene u ovoj Uredbi. Međutim, na nacionalnoj bi razini trebalo dopustiti uvrštavanje posebnih značajki, poput jedinstvenih identifikatora, u kvalificirane certifikate, pod uvjetom da takve posebne značajke ne ometaju prekograničnu interoperabilnost i priznavanje kvalificiranih certifikata i elektroničkih potpisa.

(55) Certificiranje sigurnosti informacijske tehnologije na temelju međunarodnih normi, kao što su ISO 15408 i povezani načini evaluacije i dogovori o uzajamnom priznavanju, važan je alat za verifikaciju sigurnosti kvalificiranih sredstava za izradu elektroničkih potpisa i trebalo bi ga promicati. Međutim, inovativna rješenja i usluge, kao što su potpisivanje pomoću mobilnih uređaja i potpisivanje pomoću tehnologije oblaka (*cloud signing*) oslanjaju se na tehnička i organizacijska rješenja za kvalificirana sredstva za izradu elektroničkih potpisa za koje sigurnosne norme možda još nisu dostupne ili za koje je prvo certificiranje sigurnosti informacijske tehnologije još uvijek u tijeku. Razinu sigurnosti takvih kvalificiranih sredstava za izradu elektroničkih potpisa moglo bi se ocjenjivati primjenom alternativnih postupaka samo ako takve sigurnosne norme nisu dostupne ili ako je prvo certificiranje sigurnosti informacijske tehnologije još uvijek u tijeku. Ti bi postupci trebali biti usporedivi s normama za certificiranje sigurnosti informacijske tehnologije ako su njihove razine sigurnosti jednakovrijedne. Stručna revizija mogla bi olakšati te postupke.

(56) Ovom Uredbom trebalo bi utvrditi zahtjeve za kvalificirana sredstva za izradu elektroničkih potpisa kako bi se osigurala funkcionalnost naprednih elektroničkih potpisa. Ova Uredba ne bi trebala obuhvaćati cjelokupno okruženje sustava u kojemu se takva sredstva primjenjuju. Stoga bi se opseg certificiranja kvalificiranih sredstava za izradu elektroničkih potpisa trebao ograničiti na hardver i softver sustava koji se koristi za upravljanje i zaštitu podataka za izradu potpisa koji su izrađeni, pohranjeni ili obrađeni u sredstvu za izradu potpisa. Kao što je navedeno u relevantnim normama, područje primjene obveze certificiranja ne bi trebalo uključivati aplikacije za izradu potpisa.

(57) Radi osiguravanja pravne sigurnosti u pogledu valjanosti potpisa, nužno je utvrditi komponente kvalificiranog elektroničkog potpisa koje bi trebala procijeniti pouzdajuća strana koja obavlja validaciju. Osim toga, utvrđivanjem zahtjeva za kvalificirane pružatelje usluga povjerenja koji mogu pružiti kvalificiranu uslugu validacije pouzdajućim stranama koje ne žele ili ne mogu same obaviti validaciju kvalificiranih elektroničkih potpisa, trebali bi potaknuti privatni i javni sektor na ulaganja u takve usluge. Oba elementa trebala bi za sve aktere na razini Unije omogućiti jednostavnu i praktičnu validaciju kvalificiranog elektroničkog potpisa.

(58) Kada je za transakciju potreban kvalificirani elektronički pečat pravne osobe, kvalificirani elektronički potpis ovlaštenog predstavnika pravne osobe trebao bi biti jednako prihvatljiv.

(59) Elektronički pečati trebali bi služiti kao dokaz da je elektronički dokument izdala pravna osoba, jamčeći na taj način izvornost i cjelovitost dokumenta.

(60) Pružatelji usluga povjerenja koji izdaju kvalificirane certifikate za elektroničke pečate trebali bi primjenjivati neophodne mjere kako bi bili u mogućnosti utvrditi identitet fizičke osobe koja zastupa pravnu osobu kojoj je izdan kvalificirani certifikat za elektronički pečat, ako je takva identifikacija potrebna na nacionalnoj razini u kontekstu sudskog ili upravnog postupka.

(61) Ovom bi Uredbom trebalo osigurati dugoročno čuvanje informacija kako bi se osigurala pravna valjanost elektroničkih potpisa i elektroničkih pečata tijekom duljih razdoblja, čime bi se zajamčila mogućnost njihove validacije neovisno o budućim tehnološkim promjenama.

(62) Kako bi se osigurala sigurnost kvalificiranih elektroničkih vremenskih žigova, ovom bi se Uredbom trebalo zahtijevati korištenje naprednim elektroničkim pečatom ili naprednim elektroničkim potpisom ili drugim jednakovrijednim metodama. Pretpostavlja se da inovacije mogu dovesti do novih tehnologija kojima se može osigurati jednaka razina sigurnosti za vremenske žigove. Kad god se umjesto naprednog elektroničkog pečata ili naprednog elektroničkog potpisa koristi neka druga metoda, kvalificirani pružatelj usluga povjerenja trebao bi dokazati, u skladu s izvješćem o ocjenjivanju sukladnosti, da takva metoda osigurava jednakovrijednu razinu sigurnosti i da ispunjava obveze određene u ovoj Uredbi.

(63) Elektronički dokumenti važni su za daljnji razvoj prekograničnih elektroničkih transakcija na unutarnjem tržištu. Ovom bi Uredbom trebalo uspostaviti načelo prema kojem se elektroničkom dokumentu ne bi smio uskratiti pravni učinak zbog toga što je on u elektroničkom obliku, a kako bi se osiguralo da elektronička transakcija ne bude odbijena samo zbog toga što je određeni dokument u elektroničkom obliku.

(64) Komisija bi se pri razmatranju formata naprednih elektroničkih potpisa i pečata trebala osloniti na postojeću praksu, norme i zakonodavstvo, a posebno na Odluku Komisije 2011/130/EU ([1]).

(65) Osim autentikacije dokumenta koji je izdala pravna osoba, elektronički pečati mogu se koristiti i za autentikaciju bilo koje digitalne imovine pravne osobe, kao što su softverski kod ili poslužitelji.

(66) Bitno je osigurati pravni okvir kako bi se olakšalo prekogranično priznavanje među postojećim nacionalnim pravnim sustavima u odnosu na usluge elektroničke preporučene dostave. Tim bi se okvirom mogle otvoriti i nove tržišne mogućnosti za Unijine pružatelje usluga povjerenja jer će oni na paneuropskoj razini moći ponuditi nove usluge elektroničke preporučene dostave.

(67) Usluge autentikacije mrežnih stranica osiguravaju sredstva pomoću kojih posjetitelj mrežnih stranica može biti siguran da iza tih mrežnih stranica stoji vjerodostojan i zakoniti subjekt. Te usluge doprinose izgradnji povjerenja i pouzdanja u vođenje poslovanja *online* jer će korisnici imati pouzdanja u mrežne stranice koje su autenticirane. Pružanje i korištenje uslugama autentikacije mrežnih stranica u cijelosti su dobrovoljni. Međutim, kako bi autentikacija mrežnih stranica postala sredstvo jačanja povjerenja, pružanja boljeg iskustva za korisnika i unapređivanja rasta na unutarnjem tržištu, ovom bi Uredbom trebalo utvrditi minimalne obveze u odnosu na sigurnost i odgovornost pružateljâ usluga i usluga koje oni pružaju. U tu svrhu, u obzir su uzeti rezultati postojećih industrijskih inicijativa, na primjer, Tijela za certificiranje/Forum preglednikâ – Forum CA/B. Osim toga, ova Uredba ne bi trebala ograničavati korištenje drugim sredstvima ili metodama autentikacije mrežnih stranica koji nisu obuhvaćeni ovom Uredbom niti bi trebala sprečavati pružatelje usluga autentikacije mrežnih stranica iz trećih zemalja da svoje usluge pružaju korisnicima u Uniji. Međutim, usluge autentikacije mrežnih stranica pružatelja usluga iz treće zemlje trebale bi se priznavati kao kvalificirane, u skladu s ovom Uredbom, samo ako je sklopljen međunarodni sporazum između Unije i zemlje u kojoj taj pružatelj usluge ima poslovni nastan.

(68) U skladu s odredbama o poslovnom nastanu iz Ugovora o funkcioniranju Europske unije (UFEU), pojam „pravne osobe" gospodarskim subjektima ostavlja mogućnost da odaberu pravni oblik koji smatraju prikladnim za obavljanje svoje djelatnosti. Sukladno tomu, „pravne osobe", u smislu UFEU-a, znači svi subjekti koji su osnovani prema pravu države članice ili uređeni pravom države članice, bez obzira na njihov pravni oblik.

(69) Institucije, tijela, urede i agencije Unije potiče se da priznaju elektroničku identifikaciju i usluge povjerenja obuhvaćene ovom Uredbom u svrhu kapitalizacije administrativne suradnje, posebno u vezi s postojećom dobrom praksom i rezultatima projekata koji su u tijeku u područjima obuhvaćenima ovom Uredbom.

([1]) Odluka Komisije 2011/130/EU od 25. veljače 2011. o uspostavljanju minimalnih zahtjeva za prekograničnu obradu dokumenata koje elektronički potpisuju nadležna tijela prema Direktivi 2006/123/EZ Europskog parlamenta i Vijeća o uslugama na unutarnjem tržištu (SL L 53, 26.2.2011., str. 66.).

(70) Kako bi se određeni podrobni tehnički aspekti ove Uredbe dopunili na fleksibilan i brz način, Komisiji bi, u pogledu kriterija koje trebaju ispuniti tijela odgovorna za certificiranje kvalificiranih sredstava za izradu elektroničkih potpisa, trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a. Posebno je važno da Komisija tijekom svog pripremnog rada provede odgovarajuća savjetovanja, uključujući i ona na razini stručnjaka. Prilikom pripreme i izrade delegiranih akata, Komisija bi trebala osigurati da se relevantni dokumenti Europskom parlamentu i Vijeću šalju istodobno, na vrijeme i na primjeren način.

(71) Kako bi se osiguravali jedinstveni uvjeti za provedbu ove Uredbe, posebno uvjeti za utvrđivanje referentnih brojeva normi čije bi korištenje predmnijevalo ispunjavanje određenih zahtjeva koji su utvrđeni u ovoj Uredbi, provedbene ovlasti trebalo bi dodijeliti Komisiji. Te bi se ovlasti trebale izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća ([1]).

(72) Komisija bi pri donošenju delegiranih ili provedbenih akata trebala posebno uzeti u obzir norme i tehničke specifikacije koje su izradile europske i međunarodne normizacijske organizacije i normizacijska tijela, posebno Europski odbor za normizaciju (CEN), Europski institut za telekomunikacijske norme (ETSI), Međunarodna organizacija za normizaciju (ISO) i Međunarodna telekomunikacijska unija (ITU), s ciljem osiguravanja visoke razine sigurnosti i interoperabilnosti elektroničke identifikacije i usluga povjerenja.

(73) Zbog razloga pravne sigurnosti i jasnoće, Direktivu 1999/93/EZ trebalo bi staviti izvan snage.

(74) Radi osiguravanja pravne sigurnosti za tržišne operatore koji već koriste kvalificirane certifikate izdane fizičkim osobama u skladu s Direktivom 1999/93/EZ, potrebno je osigurati dovoljno dugo prijelazno razdoblje. Slično tome, trebalo bi uspostaviti prijelazne mjere za sredstva za sigurnu izradu potpisa, čija je sukladnost utvrđena u skladu s Direktivom 1999/93/EZ, kao i za pružatelje usluga certificiranja koji su izdali kvalificirane certifikate prije 1. srpnja 2016. Naposljetku, također je potrebno Komisiji osigurati sredstva za donošenje provedbenih akata i delegiranih akata prije tog datuma.

(75) Datumi primjene određeni u ovoj Uredbi ne utječu na postojeće obveze država članica prema pravu Unije, posebno prema Direktivi 2006/123/EZ.

(76) S obzirom na to da ciljeve ove Uredbe ne mogu dostatno ostvariti države članice, nego se zbog opsega djelovanja oni na bolji način mogu ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. Ugovora o Europskoj uniji. U skladu s načelnom proporcionalnosti utvrđenim u tom članku, ova Uredba ne prelazi ono što je potrebno za ostvarivanje tih ciljeva.

(77) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 28. stavkom 2. Uredbe (EZ) br. 45/2001 Europskog parlamenta i Vijeća ([2]) koji je dao mišljenje 27. rujna 2012. ([3]),

([1]) Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13.).

([2]) Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL L 8, 12.1.2001.,str. 1.).

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

DONIJELI SU OVU UREDBU:

POGLAVLJE I.

**OPĆE ODREDBE**

*Članak 1.*

**Predmet**

S ciljem osiguravanja ispravnog funkcioniranja unutarnjeg tržišta, istodobno težeći primjerenoj razini sigurnosti sredstava elektroničke identifikacije i usluga povjerenja, ovom se Uredbom:

(a) utvrđuju uvjeti pod kojima države članice priznaju sredstva elektroničke identifikacije fizičkih i pravnih osoba koja su obuhvaćena prijavljenim sustavom elektroničke identifikacije druge države članice;

(b) utvrđuju pravila za usluge povjerenja, posebno za elektroničke transakcije; i

(c) uspostavlja pravni okvir za elektroničke potpise, elektroničke pečate, elektroničke vremenske žigove, elektroničke dokumente, usluge elektroničke preporučene dostave i usluge certificiranja za autentikaciju mrežnih stranica.

*Članak 2.*

**Područje primjene**

1. Ova se Uredba primjenjuje na sustave elektroničke identifikacije koje je prijavila država članica, kao i na pružatelje usluga povjerenja koji imaju poslovni nastan u Uniji.

2. Ova se Uredba ne primjenjuje na pružanje usluga povjerenja koje se isključivo koriste unutar zatvorenih sustava koji proizlaze iz nacionalnog prava ili iz sporazumâ među utvrđenom skupinom sudionika.

3. Ova Uredba ne utječe na nacionalno pravo ili pravo Unije koje se odnosi na sklapanje i valjanost ugovorâ ili drugih pravnih ili postupovnih obveza u pogledu forme.

*Članak 3.*

**Definicije**

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „elektronička identifikacija” znači postupak korištenja osobnim identifikacijskim podacima u elektroničkom obliku koji na nedvojben način predstavljaju bilo fizičku ili pravnu osobu ili fizičku osobu koja predstavlja pravnu osobu;

2. „sredstvo elektroničke identifikacije” znači materijalna i/ili nematerijalna jedinica koja sadrži osobne identifikacijske podatke i koja se koristi za autentikaciju na *online* uslugu;

3. „osobni identifikacijski podaci” znači skup podataka koji omogućavaju da se utvrdi identitet fizičke ili pravne osobe ili fizičke osobe koja predstavlja pravnu osobu;

4. „sustav elektroničke identifikacije” znači sustav za elektroničku identifikaciju u okviru kojega se izdaju sredstva elektroničke identifikacije fizičkim ili pravnim osobama ili fizičkim osobama koje predstavljaju pravne osobe;

5. „autentikacija” znači elektronički postupak koji omogućava da elektronička identifikacija fizičke ili pravne osobe ili izvornost i cjelovitost podataka u elektroničkom obliku budu potvrđeni;

6. „pouzdajuća strana” znači fizička ili pravna osoba koja se oslanja na elektroničku identifikaciju ili uslugu povjerenja;

7. „tijelo javnog sektora” znači državno, regionalno ili lokalno tijelo, javnopravno tijelo ili udruženje koje se sastoji od jednog ili nekoliko takvih tijela ili jednog ili nekoliko takvih javnopravnih tijela ili privatni subjekt koji je ovlastilo barem jedno od tih vlasti, tijela ili udruženja za pružanje javnih usluga kada djeluju u okviru takve ovlasti;

8. „javnopravno tijelo” znači tijelo definirano u članku 2. stavku 1. točki 4. Direktive 2014/24/EU Europskog parlamenta i Vijeća ([1]);

9. „potpisnik” znači fizička osoba koja izrađuje elektronički potpis;

10. „elektronički potpis” znači podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje;

11. „napredan elektronički potpis” znači elektronički potpis koji ispunjava zahtjeve navedene u članku 26.;

12. „kvalificirani elektronički potpis” znači napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise;

13. „podaci za izradu elektroničkog potpisa” znači jedinstveni podaci koje potpisnik koristi za izradu elektroničkog potpisa;

14. „certifikat za elektronički potpis” znači elektronička potvrda koja povezuje podatke za validaciju elektroničkog potpisa s fizičkom osobom i potvrđuje barem ime ili pseudonim te osobe;

15. „kvalificirani certifikat za elektronički potpis” znači certifikat za elektroničke potpise koji izdaje kvalificirani pružatelj usluga povjerenja i koji ispunjava zahtjeve utvrđene u Prilogu I.;

16. „usluga povjerenja” znači elektronička usluga koja se u pravilu pruža uz naknadu i koja se sastoji od:

   (a) izrade, verifikacije i validacije elektroničkih potpisa, elektroničkih pečata ili elektroničkih vremenskih žigova, usluge elektroničke preporučene dostave i certifikata koji se odnose na te usluge; ili

   (b) izrade, verifikacije i validacije certifikata za autentikaciju mrežnih stranica; ili

   (c) čuvanja elektroničkih potpisa, pečata ili certifikata koji se odnose na te usluge;

17. „kvalificirana usluga povjerenja” znači usluga povjerenja koja ispunjava odgovarajuće zahtjeve utvrđene u ovoj Uredbi;

([1]) Direktiva 2014/24/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/18/EZ (SL L 94, 28.3.2014., str. 65.).

18. „tijelo za ocjenjivanje sukladnosti” znači tijelo u smislu članka 2. točke 13. Uredbe (EZ) br. 765/2008 koje je u skladu s tom Uredbom ovlašteno kao nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža;

19. „pružatelj usluga povjerenja” znači fizička ili pravna osoba koja pruža jednu ili više usluga povjerenja bilo kao kvalificirani ili nekvalificirani pružatelj usluga povjerenja;

20. „kvalificirani pružatelj usluga povjerenja” znači pružatelj usluga povjerenja koji pruža jednu ili više kvalificiranih usluga povjerenja i kojemu je nadzorno tijelo odobrilo kvalificirani status;

21. „proizvod” znači hardver ili softver ili odgovarajuće komponente hardvera ili softvera koji su namijenjeni za korištenje u svrhu pružanja usluga povjerenja;

22. „sredstvo za izradu elektroničkog potpisa” znači konfigurirani softver ili hardver koji se koristi za izradu elektroničkog potpisa;

23. „kvalificirano sredstvo za izradu elektroničkog potpisa” znači sredstvo za izradu elektroničkog potpisa koje ispunjava zahtjeve utvrđene u Prilogu II.;

24. „autor pečata” znači pravna osoba koja izrađuje elektronički pečat;

25. „elektronički pečat” znači podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka;

26. „napredan elektronički pečat” znači elektronički pečat koji ispunjava zahtjeve navedene u članku 36.;

27. „kvalificirani elektronički pečat” znači napredan elektronički pečat koji je izrađen pomoću kvalificiranog sredstva za izradu elektroničkog pečata i koji se temelji na kvalificiranom certifikatu za elektronički pečat;

28. „podaci za izradu elektroničkog pečata” znači jedinstveni podaci koje autor elektroničkog pečata koristi za izradu elektroničkog pečata;

29. „certifikat za elektronički pečat” znači elektronička potvrda koja povezuje podatke za validaciju elektroničkog pečata s pravnom osobom i potvrđuje naziv te osobe;

30. „kvalificirani certifikat za elektronički pečat” znači certifikat za elektronički pečat koji izdaje kvalificirani pružatelj usluge povjerenja i koji ispunjava zahtjeve određene u Prilogu III.;

31. „sredstvo za izradu elektroničkog pečata” znači konfigurirani softver ili hardver koji se koristi za izradu elektroničkog pečata;

32. „sredstvo za izradu kvalificiranog elektroničkog pečata” znači sredstvo za izradu elektroničkog pečata koje *mutatis mutandis* ispunjava zahtjeve određene u Prilogu II.;

33. „elektronički vremenski žig” znači podaci u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme;

34. „kvalificirani elektronički vremenski žig” znači elektronički vremenski žig koji ispunjava zahtjeve navedene u članku 42.;

35. „elektronički dokument” znači svaki sadržaj koji je pohranjen u elektroničkom obliku, a posebno kao tekstualni ili zvučni, vizualni ili audiovizualni zapis;

36. „usluga elektroničke preporučene dostave” znači usluga koja omogućava prijenos podataka među trećim stranama pomoću elektroničkih sredstava i pruža dokaz o postupanju s prenesenim podacima, uključujući dokaz o slanju i primanju podataka, čime se preneseni podaci štite od rizika gubitka, krađe, oštećenja ili bilo kakvih neovlaštenih preinaka;

37. „kvalificirana usluga elektroničke preporučene dostave” znači usluga elektroničke preporučene dostave koja ispunjava zahtjeve utvrđene u članku 44.;

38. „certifikat za autentikaciju mrežnih stranica” znači potvrda pomoću koje je moguće izvršiti autentikaciju mrežnih stranica te kojom se mrežne stranice povezuju s fizičkom ili pravnom osobom kojoj je izdan certifikat;

39. „kvalificirani certifikat za autentikaciju mrežnih stranica” znači certifikat za autentikaciju mrežnih stranica koji izdaje kvalificirani pružatelj usluga povjerenja i koji ispunjava zahtjeve utvrđene u Prilogu IV.;

40. „podaci za validaciju” znači podaci koji se koriste za validaciju elektroničkog potpisa ili elektroničkog pečata;

41. „validacija” znači postupak verifikacije i potvrđivanja da su elektronički potpis ili pečat valjani.

*Članak 4.*

**Načelo unutarnjeg tržišta**

1. Pružanje usluga povjerenja na državnom području države članice od strane pružatelja usluge povjerenja s poslovnim nastanom u drugoj državi članici ne ograničava se zbog razloga koji ulaze u područje primjene ove Uredbe.

2. Proizvodima i uslugama povjerenja koji su u skladu s ovom Uredbom dopušta se slobodno cirkulirati na unutarnjem tržištu.

*Članak 5.*

**Obrada i zaštita podataka**

1. Obrada osobnih podataka provodi se u skladu s Direktivom 95/46/EZ.

2. Ne dovodeći u pitanje pravne učinke koje pseudonimi imaju prema nacionalnom pravu, korištenje pseudonimom u elektroničkim transakcijama nije zabranjeno.

POGLAVLJE II.

**ELEKTRONIČKA IDENTIFIKACIJA**

*Članak 6.*

**Uzajamno priznavanje**

1. Kada se prema nacionalnom pravu ili nacionalnom administrativnom praksom zahtijeva elektronička identifikacija pomoću sredstva elektroničke identifikacije i autentikacije radi pristupa usluzi koju tijelo javnog sektora pruža *online* u jednoj državi članici, sredstvo elektroničke identifikacije izdano u drugoj državi članici priznaje se u prvoj državi članici za potrebe prekogranične autentikacije na tu uslugu *online*, pod uvjetom da su ispunjeni sljedeći uvjeti:

(a) sredstvo elektroničke identifikacije izdano je u okviru sustava elektroničke identifikacije koji je uvršten na popis koji je objavila Komisija na temelju članka 9.;

(b) razina sigurnosti tih sredstava elektroničke identifikacije odgovara razini sigurnosti koja je jednaka ili viša od razine sigurnosti koju zahtijeva nadležno tijelo javnog sektora radi pristupa toj usluzi *online* u prvoj državi članici ili viša od te razine, pod uvjetom da razina sigurnosti tih sredstava elektroničke identifikacije odgovara značajnoj ili visokoj razini sigurnosti;

(c) odgovarajuće tijelo javnog sektora primjenjuje značajnu ili visoku razinu sigurnosti u odnosu na pristupanje toj usluzi *online*.

Takvo priznavanje mora uslijediti najkasnije 12 mjeseci nakon što Komisija objavi popis iz prvog podstavka točke (a).

2. Sredstvo elektroničke identifikacije koje se izdaje u okviru sustava elektroničke identifikacije uvrštenog na popis koji je objavila Komisija na temelju članka 9. i koji odgovara niskoj razini sigurnosti, tijela javnog sektora mogu priznati za potrebe prekogranične autentikacije na uslugu koju ta tijela pružaju *online*.

*Članak 7.*

**Prihvatljivost sustava elektroničke identifikacije za prijavu**

Sustav elektroničke identifikacije prihvatljiv je za prijavu na temelju članka 9. stavka 1. pod uvjetom da budu ispunjeni svi sljedeći uvjeti:

(a) sredstva elektroničke identifikacije u okviru sustava elektroničke identifikacije izdana su:

i. od strane države članice koja provodi prijavljivanje;

ii. u okviru mandata države članice koja provodi prijavljivanje; ili

iii. neovisno o državi članici koja provodi prijavljivanje, a priznata su od strane te države članice;

(b) sredstva elektroničke identifikacije u okviru sustava elektroničke identifikacije mogu se koristiti za pristup barem jednoj usluzi koju pruža tijelo javnog sektora i koja zahtijeva elektroničku identifikaciju u državi članici koja provodi prijavljivanje;

(c) sustav elektroničke identifikacije i sredstva elektroničke identifikacije izdana u okviru tog sustava ispunjavaju zahtjeve barem jedne od razina sigurnosti određenih u provedbenom aktu iz članka 8. stavka 3.;

(d) država članica koja provodi prijavljivanje osigurava da se osobni identifikacijski podaci koji nedvojbeno predstavljaju osobu o kojoj je riječ, u skladu s tehničkim specifikacijama, normama i postupcima za odgovarajuću razinu sigurnosti određenu u provedbenom aktu iz članka 8. stavka 3., pripisuju fizičkoj ili pravnoj osobi iz članka 3. točke 1. u vrijeme kada su sredstva elektroničke identifikacije izdana u okviru tog sustava;

(e) strana koja izdaje sredstva elektroničke identifikacije u okviru tog sustava osigurava da se sredstva elektroničke identifikacije pripisuju osobi iz točke (d) ovog članka u skladu s tehničkim specifikacijama, normama i postupcima za odgovarajuću razinu sigurnosti određenu u provedbenom aktu iz članka 8. stavka 3.;

(f) država članica koja provodi prijavljivanje osigurava dostupnost autentikacije *online*, tako da svaka pouzdajuća strana s poslovnim nastanom na državnom području druge države članice može potvrditi osobne identifikacijske podatke zaprimljene u elektroničkom obliku.

Za pouzdajuće strane koje nisu tijela javnog sektora, država članica koja provodi prijavljivanje može odrediti uvjete pristupa toj autentikaciji. Prekogranična autentikacija pruža se bez naknade kada se provodi *online* u vezi s uslugom koju pruža tijelo javnog sektora.

Države članice ne nameću bilo kakve posebne nerazmjerne tehničke zahtjeve pouzdajućim stranama koje namjeravaju provesti takvu autentikaciju ako takvi zahtjevi sprečavaju ili znatno ograničavaju interoperabilnost prijavljenih sustava elektroničke identifikacije;

(g) najmanje šest mjeseci prije prijave na temelju članka 9. stavka 1., za potrebe obveze prema članku 12. stavku 5., država članica koja provodi prijavljivanje drugoj državi članici dostavlja opis tog sustava u skladu s postupovnim aranžmanima koji su utvrđeni provedbenim aktima iz članka 12. stavka 7.;

(h) sustav elektroničke identifikacije ispunjava zahtjeve određene u provedbenom aktu iz članka 12. stavka 8.

*Članak 8.*

**Razine sigurnosti sustava elektroničke identifikacije**

1. Sustav elektroničke identifikacije koji je prijavljen na temelju članka 9. stavka 1. određuje nisku, značajnu i/ili visoku razinu sigurnosti koja se pripisuje sredstvima elektroničke identifikacije koja su izdana u okviru tog sustava.

2. Niska, značajna odnosno visoka razina sigurnosti moraju ispunjavati sljedeće kriterije:

(a) niska razina sigurnosti odnosi se na sredstva elektroničke identifikacije u kontekstu sustava elektroničke identifikacije, koja pruža ograničen stupanj pouzdanja u odnosu na traženi ili utvrđeni identitet osobe te je karakterizirana upućivanjem na tehničke specifikacije, norme i s njima povezane postupke, uključujući tehničke kontrole čija je svrha smanjenje rizika zlouporabe ili promjene identiteta;

(b) značajna razina sigurnosti odnosi se na sredstva elektroničke identifikacije u kontekstu sustava elektroničke identifikacije, koja pruža značajan stupanj pouzdanja u odnosu na traženi ili utvrđeni identitet osobe te je karakterizirana upućivanjem na tehničke specifikacije, norme i s njima povezane postupke, uključujući tehničke kontrole čija je svrha značajno smanjenje rizika zlouporabe ili promjene identiteta;

(c) visoka razina sigurnosti odnosi se na sredstva elektroničke identifikacije u kontekstu sustava elektroničke identifikacije, koja pruža viši stupanj pouzdanja u odnosu na traženi ili utvrđeni identitet osobe od sredstava elektroničke identifikacije sa značajnom razinom sigurnosti te je karakterizirana upućivanjem na tehničke specifikacije, norme i s njima povezane postupke, uključujući tehničke kontrole čija je svrha značajno smanjenje rizika zlouporabe ili promjene identiteta.

3. Komisija, uzimajući u obzir odgovarajuće međunarodne norme i podložno stavku 2., provedbenim aktima do 18. rujna 2015. određuje minimalne tehničke specifikacije, norme i postupke u odnosu na koje se za sredstva elektroničke identifikacije u smislu stavka 1. utvrđuju niska, značajna i visoka razina sigurnosti.

Te minimalne tehničke specifikacije, norme i postupci određuju se upućivanjem na pouzdanost i kvalitetu sljedećih elemenata:

(a) postupka radi dokazivanja i verifikacije identiteta fizičke ili pravne osobe koja podnosi zahtjev za izdavanje sredstava elektroničke identifikacije;

(b) postupka za izdavanje traženih sredstava elektroničke identifikacije;

(c) mehanizma autentikacije putem kojeg fizička ili pravna osoba koristi sredstva elektroničke identifikacije za potvrđivanje svoga identiteta pouzdajućoj strani;

(d) tijela koje izdaje sredstvo elektroničke identifikacije;

(e) svakog drugog tijela uključenog u podnošenje zahtjeva za izdavanje sredstava elektroničke identifikacije; i

(f) tehničkih i sigurnosnih specifikacija izdanih sredstava elektroničke identifikacije.

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 9.*

**Prijavljivanje**

1. Država članica koja provodi prijavljivanje Komisiji prijavljuje sljedeće informacije i, bez odgađanja, sve njihove naknadne izmjene:

(a) opis sustava elektroničke identifikacije, uključujući njegove razine sigurnosti i izdavatelja ili izdavatelje sredstava elektroničke identifikacije u okviru sustava;

(b) primjenjivi sustav nadzora i informacije o pravilima o odgovornosti s obzirom na sljedeće:

i. stranu koja izdaje sredstvo elektroničke identifikacije; i

ii. stranu koja provodi postupak autentikacije;

(c) tijelo ili tijela odgovorno (odgovorna) za sustav elektroničke identifikacije;

(d) informacije o subjektu ili subjektima koji upravljaju registracijom jedinstvenih osobnih identifikacijskih podataka;

(e) opis načina ispunjavanja zahtjeva određenih u provedbenim aktima iz članka 12. stavka 8.;

(f) opis autentikacije iz članka 7. točke (f);

(g) dogovori za suspenziju ili opoziv bilo prijavljenog sustava elektroničke identifikacije ili autentikacije ili ugroženih dijelova o kojima je riječ.

2. Godinu dana od dana primjene provedbenih akata iz članka 8. stavka 3. i članka 12. stavka 8., Komisija u *Službenom listu Europske unije* objavljuje popis sustavâ elektroničke identifikacije koji su prijavljeni na temelju stavka 1. ovog članka i osnovne informacije o njima.

3. Ako Komisija primi prijavu nakon isteka razdoblja iz stavka 2., ona u *Službenom listu Europske unije* objavljuje izmjene popisa iz stavka 2., u roku od dva mjeseca od datuma primitka te prijave.

4. Država članica može Komisiji podnijeti zahtjev za uklanjanje sustava elektroničke identifikacije koji je prijavila ta država članica s popisa iz stavka 2. Komisija objavljuje odgovarajuće izmjene popisa u *Službenom listu Europske unije* u roku od mjeseca dana od datuma primitka zahtjeva države članice.

5. Komisija može provedbenim aktima utvrditi okolnosti, oblike i postupke prijava prema stavku 1. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 10.*

**Povreda sigurnosti**

1. U slučaju povrede ili djelomičnog ugrožavanja bilo sustava elektroničke identifikacije koji je prijavljen na temelju članka 9. stavka 1. ili autentikacije iz članka 7. točke (f) na način koji utječe na pouzdanost prekogranične autentikacije tog sustava, država članica koja provodi prijavljivanje bez odgađanja suspendira ili opoziva tu prekograničnu autentikaciju ili ugrožene dijelove o kojima je riječ i obavješćuje ostale države članice i Komisiju.

2. Kada je povreda ili ugrožavanje iz stavka 1. otklonjeno, država članica koja provodi prijavljivanje ponovno uspostavlja prekograničnu autentikaciju i bez odgađanja obavješćuje ostale države članice i Komisiju.

3. Ako povreda ili ugrožavanje iz stavka 1. nije otklonjeno u roku od 3 mjeseca od suspenzije ili opoziva, država članica koja provodi prijavljivanje obavješćuje druge države članice i Komisiju o povlačenju sustava elektroničke identifikacije.

Komisija u *Službenom listu Europske unije* bez odgađanja objavljuje odgovarajuće izmjene popisa iz članka 9. stavka 2.

*Članak 11.*

**Odgovornost**

1. Država članica koja provodi prijavljivanje odgovorna je za štetu koja je namjerno ili nepažnjom prouzročena svakoj fizičkoj ili pravnoj osobi nepoštovanjem obveza pri prekograničnoj transakciji prema članku 7. točkama (d) i (f).

2. Strana koja izdaje sredstva elektroničke identifikacije odgovara za štetu koja je namjerno ili nepažnjom prouzročena svakoj fizičkoj ili pravnoj osobi nepoštovanjem obveza pri prekograničnoj transakciji iz članka 7. točke (e).

3. Strana koja provodi postupak autentikacije odgovorna je za štetu koja je namjerno ili nepažnjom prouzročena svakoj fizičkoj ili pravnoj osobi nepoštovanjem obveze osiguravanja ispravne provedbe autentikacije iz članka 7. točke (f) pri prekograničnoj transakciji.

4. Stavci 1., 2. i 3. primjenjuju se u skladu s nacionalnim pravilima o odgovornosti.

5. Stavci 1., 2. i 3. ne dovode u pitanje odgovornost prema nacionalnom pravu stranaka transakcije u kojoj se koriste sredstva elektroničke identifikacije obuhvaćena sustavom elektroničke identifikacije prijavljenim na temelju članka 9. stavka 1.

*Članak 12.*

**Suradnja i interoperabilnost**

1. Nacionalni sustavi elektroničke identifikacije prijavljeni na temelju članka 9. stavka 1. moraju biti interoperabilni.

2. Za potrebe stavka 1., uspostavlja se okvir za interoperabilnost.

3. Okvir za interoperabilnost mora ispunjavati sljedeće kriterije:

(a) za cilj ima tehnološku neutralnost i ne pravi razliku između bilo kojih posebnih nacionalnih tehničkih rješenja za elektroničku identifikaciju unutar određene države članice;

(b) pridržava se europskih i međunarodnih normi, kada je to moguće;

(c) olakšava provedbu načela „ugrađene zaštite privatnosti”; i

(d) osigurava obradu osobnih podataka u skladu s Direktivom 95/46/EZ.

4. Okvir za interoperabilnost sastoji se od:

(a) upućivanja na minimalne tehničke zahtjeve koji se odnose na razine sigurnosti prema članku 8.;

(b) raspoređivanja nacionalnih razina sigurnosti prijavljenih sustava elektroničke identifikacije na razine sigurnosti prema članku 8.;

(c) upućivanja na minimalne tehničke zahtjeve za interoperabilnost;

(d) upućivanja na najmanji skup osobnih identifikacijskih podataka koji na nedvojben način predstavljaju fizičku ili pravnu osobu i kojim raspolažu sustavi elektroničke identifikacije;

(e) poslovnika;

(f) dogovorâ za rješavanje sporova; i

(g) zajedničkih operativnih sigurnosnih normi.

5. Države članice surađuju u pogledu sljedećeg:

(a) interoperabilnosti sustava elektroničke identifikacije koji su prijavljeni na temelju članka 9. stavka 1. i sustava elektroničke identifikacije koje države članice namjeravaju prijaviti; i

(b) sigurnosti sustavâ elektroničke identifikacije.

6. Suradnja među državama članicama sastoji se od:

(a) razmjene informacija, iskustva i dobre prakse u vezi sa sustavima elektroničke identifikacije i posebno u vezi s tehničkim zahtjevima koji se odnose na interoperabilnost i razine sigurnosti;

(b) razmjene informacija, iskustva i dobre prakse u vezi s radom s razinama sigurnosti sustavâ elektroničke identifikacije u skladu s člankom 8.;

(c) stručnog pregleda sustava elektroničke identifikacije obuhvaćenih ovom Uredbom; i

(d) pregleda odgovarajućih kretanja u sektoru elektroničke identifikacije.

7. Komisija provedbenim aktima do 18. ožujka 2015. uspostavlja potrebne postupovne aranžmane kako bi olakšala suradnju među državama članicama iz stavaka 5. i 6., s ciljem poticanja visoke razine povjerenja i sigurnosti koja je primjerena stupnju rizika.

8. Komisija u svrhu određivanja jednakih uvjeta za provedbu zahtjeva prema stavku 1. do 18. rujna 2015. donosi provedbene akte o okviru za interoperabilnost kako je određeno u stavku 4., podložno kriterijima određenima u stavku 3. te uzimajući u obzir rezultate suradnje među državama članicama.

9. Provedbeni akti iz stavaka 7. i 8. ovog članka donose se u skladu s postupkom ispitivanja iz članka 48. stavka 2.

POGLAVLJE III.

## USLUGE POVJERENJA

*ODJELJAK 1.*

### *Opće odredbe*

*Članak 13.*

### Odgovornost i teret dokaza

1. Ne dovodeći u pitanje stavak 2., pružatelji usluga povjerenja odgovorni su za štetu koja je namjerno ili nepažnjom prouzročena svakoj fizičkoj ili pravnoj osobi zbog nepoštovanja obveza prema ovoj Uredbi.

Teret dokazivanja namjere ili nepažnje nekvalificiranog pružatelja usluga povjerenja je na fizičkoj ili pravnoj osobi koja zahtijeva naknadu štete iz prvog podstavka.

Namjera ili nepažnja kvalificiranog pružatelja usluga povjerenja pretpostavlja se, osim ako kvalificirani pružatelj usluga povjerenja dokaže da je šteta iz prvog podstavka nastala bez namjere ili nepažnje tog kvalificiranog pružatelja usluga povjerenja.

2. U slučaju kada pružatelji usluga povjerenja propisno i unaprijed obavijeste svoje korisnike o ograničenjima pri korištenju uslugama koje pružaju i kada su ta ograničenja prepoznatljiva za treće strane, pružatelji usluga povjerenja ne odgovaraju za štete koje nastanu zbog korištenja uslugama kojim se prekoračuju naznačena ograničenja.

3. Stavci 1. i 2. primjenjuju se u skladu s nacionalnim pravilima o odgovornosti.

*Članak 14.*

### Međunarodni aspekti

1. Usluge povjerenja koje pružaju pružatelji usluga povjerenja s poslovnim nastanom u trećoj zemlji priznaju se kao pravno jednake kvalificiranim uslugama povjerenja koje pružaju kvalificirani pružatelji usluga povjerenja s poslovnim nastanom u Uniji kada su usluge povjerenja iz treće zemlje priznate u okviru sporazuma sklopljenog između Unije i treće zemlje o kojoj je riječi ili određene međunarodne organizacije u skladu s člankom 218. UFEU-a.

2. Sporazumima iz stavka 1. posebno se osigurava da:

(a) pružatelji usluga povjerenja u trećoj zemlji ili međunarodne organizacije s kojima je sklopljen sporazum i usluge povjerenja koje oni pružaju ispunjavaju zahtjeve koji se primjenjuju na kvalificirane pružatelje usluga povjerenja s poslovnim nastanom u Uniji i na kvalificirane usluge povjerenja koje oni pružaju;

(b) kvalificirane usluge povjerenja koje pružaju kvalificirani pružatelji usluga povjerenja s poslovnim nastanom u Uniji budu priznate kao pravno jednake uslugama povjerenja koje pružaju pružatelji usluga povjerenja u trećoj zemlji ili koje pružaju međunarodne organizacije s kojima je sklopljen sporazum.

*Članak 15.*

**Dostupnost za osobe s invaliditetom**

Kada je to moguće, usluge povjerenja i proizvodi za krajnje korisnike korišteni pri pružanju tih usluga dostupni su osobama s invaliditetom.

*Članak 16.*

**Sankcije**

Države članice utvrđuju pravila o sankcijama koje se primjenjuju na povrede ove Uredbe. Te sankcije moraju biti djelotvorne, razmjerne i odvraćajuće.

*ODJELJAK 2.*

***Nadzor***

*Članak 17.*

**Nadzorno tijelo**

1. Države članice određuju nadzorno tijelo s poslovnim nastanom na njihovom državnom području ili, prema uzajamnom dogovoru s drugom državom članicom, nadzorno tijelo s poslovnim nastanom u toj drugoj državi članici. To tijelo je odgovorno za zadaće nadzora u državi članici koja ga određuje.

Nadzornim se tijelima dodjeljuju potrebne ovlasti i odgovarajuća sredstva za obavljanje njihovih zadaća.

2. Države članice obavješćuju Komisiju i druge države članice o nazivima i adresama svojih nadzornih tijela koja su odredile.

3. Uloga nadzornog tijela jest sljedeća:

(a) da nadzire kvalificirane pružatelje usluga povjerenja s poslovnim nastanom na državnom području države članice koja ga određuje kako bi se osiguralo, putem prethodnih (*ex ante*) i naknadnih (*ex post*) aktivnosti nadzora, da ti kvalificirani pružatelji usluga povjerenja i kvalificirane usluge povjerenja koje oni pružaju ispunjavaju zahtjeve utvrđene u ovoj Uredbi;

(b) da, prema potrebi, poduzima mjere u odnosu na nekvalificirane pružatelje usluga povjerenja s poslovnim nastanom na državnom području države članice koja ga određuje, putem naknadnih (*ex post*) aktivnosti nadzora, kada primi obavijest da ti nekvalificirani pružatelji usluga povjerenja ili usluge povjerenja koje oni pružaju navodno ne ispunjavaju zahtjeve utvrđene u ovoj Uredbi.

4. Za potrebe stavka 3. i podložno u njemu predviđenim ograničenjima, zadaće nadzornog tijela posebno uključuju:

(a) suradnju s drugim nadzornim tijelima i pružanje pomoći tim tijelima u skladu s člankom 18.;

(b) analiziranje izvješćâ o ocjenjivanju sukladnosti iz članka 20. stavka 1. i članka 21. stavka 1.;

(c) obavješćivanje drugih nadzornih tijela i javnosti o povredama sigurnosti ili gubitku cjelovitosti u skladu s člankom 19. stavkom 2.;

(d) izvješćivanje Komisije o svojim glavnim aktivnostima u skladu sa stavkom 6. ovog članka;

(e) obavljanje revizija ili zahtijevanje od tijela za ocjenjivanje sukladnosti da provede ocjenjivanje sukladnosti kvalificiranih pružatelja usluga povjerenja u skladu s člankom 20. stavkom 2.;

(f) suradnju s tijelima za zaštitu podataka, a posebice obavješćujući ih, bez odgađanja, o rezultatima revizija kvalificiranih pružatelja usluga povjerenja, u slučaju kada se čini da je došlo do povrede pravila o zaštiti osobnih podataka;

(g) dodjeljivanje kvalificiranog statusa pružateljima usluga povjerenja i uslugama koje oni pružaju i ukidanje tog statusa u skladu s člancima 20. i 21.;

(h) obavješćivanje tijela odgovornog za nacionalni pouzdani popis iz članka 22. stavka 3. o odlukama o dodjeljivanju ili ukidanju kvalificiranog statusa, osim ako je to tijelo ujedno i nadzorno tijelo;

(i) provjeravanje postojanja i pravilne primjene odredaba o planovima prekida u slučajevima kada kvalificirani pružatelj usluga povjerenja prekine svoje aktivnosti, uključujući način na koji se održava dostupnost informacija u skladu s člankom 24. stavkom 2. točkom (h);

(j) zahtijevanje od pružatelja usluga povjerenja da otklone svako nepoštovanje zahtjeva utvrđenih u ovoj Uredbi.

5. Države članice mogu od nadzornog tijela zahtijevati da uspostavi, održava i ažurira infrastrukturu povjerenja u skladu s uvjetima prema nacionalnom pravu.

6. Svako nadzorno tijelo Komisiji do 31. ožujka svake godine dostavlja izvješće o svojim glavnim aktivnostima u prethodnoj kalendarskoj godini, zajedno sa sažetkom obavijesti o povredama koje je primilo od pružatelja usluga povjerenja u skladu s člankom 19. stavkom 2.

7. Komisija stavlja na raspolaganje državama članicama godišnje izvješće iz stavka 6.

8. Komisija može provedbenim aktima utvrditi oblike i postupke izvješća iz stavka 6. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 18.*

**Uzajamna pomoć**

1. Nadzorna tijela surađuju s ciljem razmjenjivanja dobre prakse.

Nadzorno tijelo, po primitku obrazloženog zahtjeva drugog nadzornog tijela, tom tijelu pruža pomoć kako bi se aktivnosti nadzornih tijela mogle provoditi na dosljedan način. Uzajamna pomoć može posebno obuhvaćati zahtjeve za informacijama i nadzorne mjere, kao što su zahtjevi za provođenje kontrola koje se odnose na izvješća o ocjenjivanju sukladnosti, kako je navedeno u člancima 20. i 21.

2. Nadzorno tijelo kojemu je upućen zahtjev za pomoć može odbiti taj zahtjev zbog bilo kojeg od sljedećih razloga:

(a) nadzorno tijelo nije nadležno za pružanje tražene pomoći;

(b) tražena pomoć nije razmjerna aktivnostima nadzora nadzornog tijela koje se provode u skladu s člankom 17.;

(c) pružanje tražene pomoći ne bi bilo u skladu s ovom Uredbom.

3. Prema potrebi, države članice mogu ovlastiti svoja nadzorna tijela da provode zajedničke istrage u kojima sudjeluje osoblje nadzornih tijela iz drugih država članica. Dogovore i postupke za takva zajednička djelovanja dogovaraju i uspostavljaju dotične države članice u skladu sa svojim nacionalnim pravima.

*Članak 19.*

**Sigurnosni zahtjevi primjenjivi na pružatelje usluga povjerenja**

1. Kvalificirani i nekvalificirani pružatelji usluga povjerenja poduzimaju odgovarajuće tehničke i organizacijske mjere za upravljanje rizicima koji prijete sigurnosti usluga povjerenja koje oni pružaju. Uzimajući u obzir najnovija tehnološka rješenja, tim se mjerama osigurava da razina sigurnosti odgovara stupnju rizika. Posebno se poduzimaju mjere za sprečavanje i smanjivanje utjecaja sigurnosnih incidenata te za obavješćivanje dionika o neželjenim učincima bilo kakvih incidenata te vrste.

2. Kvalificirani i nekvalificirani pružatelji usluga povjerenja obavješćuju, bez odgađanja, ali u svakom slučaju u roku od 24 sata od saznanja za iste, nadzorno tijelo i, prema potrebi, druga odgovarajuća tijela, kao što je nadležno nacionalno tijelo za sigurnost informacija ili tijelo za zaštitu podataka, o svakoj povredi sigurnosti ili gubitku cjelovitosti koji imaju značajan utjecaj na pruženu uslugu povjerenja ili u njoj sadržane osobne podatke.

Ako je izgledno da bi povreda sigurnosti ili gubitak cjelovitosti mogli nepovoljno utjecati na fizičku ili pravnu osobu kojoj su pružene usluge povjerenja, pružatelj usluga povjerenja o povredi ili gubitku cjelovitosti bez odgađanja obavješćuje i tu fizičku ili pravnu osobu.

Prema potrebi, posebno ako se povreda sigurnosti ili gubitak cjelovitosti odnosi na dvije države članice ili više njih, prijavljeno nadzorno tijelo obavješćuje nadzorna tijela u drugim državama članicama na koje se to odnosi i ENISA-u.

Prijavljeno nadzorno tijelo obavješćuje javnost ili zahtijeva od pružatelja usluga povjerenja da to učini ako utvrdi da je otkrivanje povrede sigurnosti ili gubitka cjelovitosti u javnom interesu.

3. Nadzorno tijelo jednom godišnje dostavlja ENISA-i sažetak obavijesti o povredi sigurnosti i gubitku cjelovitosti koje je primilo od pružateljâ usluga povjerenja.

4. Komisija može provedbenim aktima:

(a) podrobnije odrediti mjere iz stavka 1.; i

(b) odrediti oblike i postupke, uključujući rokove, primjenjive za potrebe stavka 2.

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*ODJELJAK 3.*

***Kvalificirane usluge povjerenja***

*Članak 20.*

**Nadzor kvalificiranih pružatelja usluga povjerenja**

1. Tijelo za ocjenjivanje sukladnosti obavlja reviziju pružatelja kvalificiranih usluga povjerenja o njihovu trošku i najmanje svaka 24 mjeseca. Svrha revizija sastoji se u potvrđivanju da kvalificirani pružatelji usluga povjerenja i kvalificirane usluge povjerenja koje oni pružaju ispunjavaju zahtjeve utvrđene u ovoj Uredbi. Kvalificirani pružatelji usluga povjerenja nadzornom tijelu podnose izvješće o ocjenjivanju sukladnosti u roku od tri radna dana od njegova primitka.

2. Ne dovodeći u pitanje stavak 1., nadzorno tijelo može u bilo kojem trenutku obaviti reviziju ili zahtijevati od tijela za ocjenjivanje sukladnosti da obavi ocjenjivanje sukladnosti pružatelja kvalificiranih usluga povjerenja, o trošku tih pružatelja usluga povjerenja, kako bi potvrdilo da pružatelji usluga povjerenja i kvalificirane usluge povjerenja koje oni pružaju ispunjavaju zahtjeve utvrđene u ovoj Uredbi. U slučaju kada se čini da je došlo do povrede pravila o zaštiti osobnih podataka, nadzorno tijelo obavješćuje tijela za zaštitu podataka o rezultatima svojih revizija.

3. U slučaju kada nadzorno tijelo zahtijeva od pružatelja kvalificiranih usluga povjerenja da otkloni bilo kakvo nepoštovanje zahtjeva prema ovoj Uredbi i kada pružatelj usluge ne postupi u skladu s tim zahtjevom, te ako je to primjenjivo i u roku koji odredi nadzorno tijelo, nadzorno tijelo može, posebno uzimajući u obzir opseg, trajanje i posljedice tog nepoštovanja, ukinuti kvalificirani status tog pružatelja usluge ili obuhvaćene usluge koju on pruža te može za potrebe ažuriranja pouzdanih popisa iz članka 22. stavka 1. obavijestiti tijelo iz članka 22. stavka 3. Nadzorno tijelo obavješćuje kvalificiranog pružatelja usluga povjerenja o ukidanju njegova kvalificiranog statusa ili kvalificiranog statusa dotične usluge.

4. Komisija može provedbenim aktima utvrditi referentne brojeve sljedećih normi:

(a) akreditacije tijela za ocjenu sukladnosti i za izvješće o ocjenjivanju sukladnosti iz stavka 1.;

(b) pravila revizije prema kojima će tijela za ocjenjivanje sukladnosti provoditi ocjenjivanje sukladnosti kvalificiranih pružatelja usluga povjerenja kako je navedeno u stavku 1.

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 21.*

**Početak pružanja kvalificirane usluge povjerenja**

1. Ako pružatelji usluga povjerenja bez kvalificiranog statusa namjeravaju započeti s pružanjem kvalificiranih usluga povjerenja, oni nadzornom tijelu podnose prijavu o svojoj namjeri zajedno s izvješćem o ocjenjivanju sukladnosti koje je izdalo tijelo za ocjenjivanje sukladnosti.

2. Nadzorno tijelo provjerava je li pružatelj usluga povjerenja sukladan odnosno jesu li usluge povjerenja koje on pruža sukladne sa zahtjevima utvrđenima u ovoj Uredbi i posebno sa zahtjevima za kvalificirane pružatelje usluga povjerenja i za kvalificirane usluge povjerenja koje oni pružaju.

Ako nadzorno tijelo zaključi da su pružatelj usluga povjerenja i usluge povjerenja koje on pruža sukladni zahtjevima iz prvog podstavka, nadzorno tijelo odobrava kvalificirani status pružatelju usluga povjerenja i uslugama povjerenja koje on pruža te obavješćuje tijelo iz članka 22. stavka 3. u svrhu ažuriranja pouzdanih popisa iz članka 22. stavka 1., najkasnije tri mjeseca nakon prijave u skladu sa stavkom 1. ovog članka.

Ako provjera nije dovršena u roku od tri mjeseca od obavješćivanja, nadzorno tijelo o tome obavješćuje pružatelja usluga povjerenja, navodeći razloge za kašnjenje i rok do kojeg provjera mora biti dovršena.

3. Pružatelji kvalificiranih usluga povjerenja mogu početi pružati kvalificiranu uslugu povjerenja nakon što kvalificirani status bude naznačen na pouzdanim popisima iz članka 22. stavka 1.

4. Komisija može provedbenim aktima utvrditi oblike i postupke za potrebe stavaka 1. i 2. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 22.*

**Pouzdani popisi**

1. Svaka država članica izrađuje, vodi i objavljuje pouzdane popise, uključujući informacije o kvalificiranim pružateljima usluga povjerenja za koje je ta država članica odgovorna, zajedno s informacijama o kvalificiranim uslugama povjerenja koje oni pružaju.

2. Države članice u obliku prikladnom za automatiziranu obradu i na siguran način izrađuju, vode i objavljuju elektronički potpisane ili pečaćene pouzdane popise iz stavka 1.

3. Države članice bez odgađanja obavješćuju Komisiju o informacijama o tijelu odgovornom za izradu, vođenje i objavljivanje nacionalnih pouzdanih popisa i detaljima o tome gdje se takvi popisi objavljuju, certifikatima korištenima za potpisivanje ili pečaćenje pouzdanih popisa i svim njihovim izmjenama.

4. Komisija stavlja na raspolaganje javnosti informacije iz stavka 3. na siguran način, u elektronički potpisanom ili pečaćenom formatu prikladnom za automatiziranu obradu.

5. Komisija putem provedbenih akata do 18. rujna 2015. navodi informacije iz stavka 1. i utvrđuje tehničke specifikacije i formate za pouzdane popise primjenjive za potrebe stavaka od 1. do 4. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 23.*

**EU znak pouzdanosti za kvalificirane usluge povjerenja**

1. Nakon što kvalificirani status iz članka 21. stavka 2. drugog podstavka bude naznačen na popisu pružatelja usluga povjerenja iz članka 22. stavka 1., pružatelji kvalificiranih usluga povjerenja mogu se koristiti EU znakom pouzdanosti kako bi na jednostavan, prepoznatljiv i jasan način naznačili kvalificirane usluge povjerenja koje pružaju.

2. Pri korištenju EU znakom pouzdanosti za kvalificirane usluge povjerenja iz stavka 1. kvalificirani pružatelji usluga povjerenja osiguravaju da na njihovim mrežnim stranicama bude dostupna poveznica na odgovarajući popis pružatelja usluga povjerenja.

3. Komisija do 1. srpnja 2015. provedbenim aktima propisuje specifikacije u odnosu na oblik te posebno izgled, sastav, veličinu i dizajn EU znaka pouzdanosti za kvalificirane usluge povjerenja. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 24.*

**Zahtjevi u vezi s kvalificiranim pružateljima usluga povjerenja**

1. Pri izdavanju kvalificiranog certifikata za uslugu povjerenja kvalificirani pružatelj usluga povjerenja provjerava, na odgovarajući način i u skladu s nacionalnim pravom, identitet i, ako je to primjenjivo, posebna obilježja fizičke ili pravne osobe kojoj se izdaje kvalificirani certifikat.

Informacije iz prvog podstavka provjerava kvalificirani pružatelj usluga povjerenja bilo izravno ili oslanjajući se na treću osobu u skladu s nacionalnim pravom:

(a) fizičkom prisutnošću fizičke osobe ili ovlaštenog predstavnika pravne osobe; ili

(b) na daljinu, pomoću sredstava elektroničke identifikacije, za koja je prije izdavanja kvalificiranog certifikata osigurana fizička prisutnost fizičke osobe ili ovlaštenog predstavnika pravne osobe i koja ispunjavaju zahtjeve određene u članku 8. u pogledu sigurnosnih razina „značajna” ili „visoka”; ili

(c) pomoću certifikata kvalificiranog elektroničkog potpisa ili kvalificiranog elektroničkog pečata izdanog u skladu s točkom (a) ili (b); ili

(d) pomoću drugih metoda identifikacije priznatih na nacionalnoj razini koja po pitanju pouzdanosti pružaju sigurnost jednaku fizičkoj prisutnosti. Jednaku sigurnost potvrđuje tijelo za ocjenjivanje sukladnosti.

2. Kvalificirani pružatelj usluga povjerenja:

(a) obavješćuje nadzorno tijelo o svim promjenama u vezi s pružanjem svojih kvalificiranih usluga povjerenja te o namjeri prestanka obavljanja te djelatnosti;

(b) zapošljava osoblje i, ako je to primjenjivo, podizvođače koji posjeduju potrebno stručno znanje, pouzdanost, iskustvo i kvalifikacije i koji su prošli odgovarajuće osposobljavanje u vezi sa sigurnošću i propisima o zaštiti osobnih podataka te primjenjuju upravne i upravljačke postupke u skladu s europskim ili međunarodnim normama;

(c) u pogledu rizika od odgovornosti za štetu u skladu s člankom 13., raspolaže dostatnim financijskim sredstvima i/ili je sklopio odgovarajuće osiguranje od odgovornosti, u skladu s nacionalnim pravom;

(d) prije stupanja u ugovorni odnos, obavješćuje, na jasan i sveobuhvatan način, svaku osobu koja želi koristiti kvalificiranu uslugu povjerenja o točnim uvjetima korištenja tom uslugom, uključujući bilo kakva ograničenja korištenja;

(e) koristi vjerodostojne sustave i proizvode koji su zaštićeni od preinaka te osiguravaju tehničku sigurnost i pouzdanost postupaka koje ti sustavi i proizvodi podržavaju;

(f) koristi vjerodostojne sustave za pohranu podataka koji su mu dostavljeni, u obliku koji se može provjeriti, kako bi:

i. ti podaci bili javno dostupni za dohvat samo uz pristanak osobe na koju se ti podaci odnose;

ii. samo ovlaštene osobe mogle obavljati nove unose u pohranjene podatke i mijenjati ih;

iii. se mogla provjeriti autentičnost podataka;

(g) poduzima odgovarajuće mjere protiv krivotvorenja i krađe podataka;

(h) bilježi i čini dostupnima tijekom odgovarajućeg razdoblja, uključujući razdoblje nakon prestanka obavljanja djelatnosti kvalificiranog pružatelja usluga povjerenja, sve bitne informacije u vezi s podacima koje izdaje i prima kvalificirani pružatelj usluga povjerenja, a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge. Takvo se bilježenje može obavljati elektronički;

(i) ima ažuriran plan prekida pružanja usluge radi osiguravanja njezina kontinuiteta u skladu s odredbama koje je potvrdilo nadzorno tijelo prema članku 17. stavku 4. točki (i);

(j) osigurava zakonitu obradu osobnih podataka u skladu s Direktivom 95/46/EZ;

(k) ako je riječ o kvalificiranim pružateljima usluga povjerenja koji izdaju kvalificirane certifikate, uspostavlja i ažurira bazu podataka certifikata.

3. Ako kvalificirani pružatelj usluga povjerenja koji izdaje kvalificirane certifikate odluči opozvati certifikat, on registrira opoziv certifikata u svojoj bazi podataka certifikata i pravodobno objavljuje status opoziva certifikata, a u svakom slučaju unutar 24 sata nakon primitka zahtjeva. Opoziv stupa na snagu odmah nakon njegove objave.

4. Imajući u vidu stavak 3., kvalificirani pružatelji usluga povjerenja koji izdaju kvalificirane certifikate pružaju bilo kojoj pouzdajućoj strani informacije o statusu valjanosti ili opoziva kvalificiranih certifikata koje su izdali. Te informacije moraju biti dostupne barem za pojedinačne certifikate, u svakom trenutku i nakon isteka razdoblja valjanosti certifikata, na automatiziran način koji je pouzdan, besplatan i učinkovit.

5. Komisija može provedbenim aktima utvrditi referentne brojeve normi za vjerodostojne sustave i proizvode koji ispunjavaju zahtjeve u skladu sa stavkom 2. točkama (e) i (f) ovog članka. Ako vjerodostojni sustavi i proizvodi udovoljavaju tim normama, smatra se da su ispunjeni zahtjevi iz ovog članka. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*ODJELJAK 4.*

***Elektronički potpisi***

*Članak 25.*

**Pravni učinci elektroničkih potpisa**

1. Elektroničkom potpisu se kao dokazu u sudskim postupcima ne smiju uskratiti pravni učinak i dopuštenost samo zbog toga što je on u elektroničkom obliku ili zbog toga što ne ispunjava sve zahtjeve za kvalificirani elektronički potpis.

2. Kvalificirani elektronički potpis ima jednak pravni učinak kao vlastoručni potpis.

3. Kvalificirani elektronički potpis koji se temelji na kvalificiranom certifikatu izdanom u jednoj državi članici priznaje se kao kvalificirani elektronički potpis u svim ostalim državama članicama.

*Članak 26.*

**Zahtjevi za napredne elektroničke potpise**

Napredan elektronički potpis mora ispunjavati sljedeće zahtjeve:

(a) na nedvojben način je povezan s potpisnikom;

(b) omogućava identificiranje potpisnika;

(c) izrađen je korištenjem podacima za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom; i

(d) povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.

*Članak 27.*

**Elektronički potpisi u javnim uslugama**

1. Ako država članica zahtijeva napredan elektronički potpis za korištenje *online* uslugom koju nudi tijelo javnog sektora ili uslugom koja se nudi u ime tijela javnog sektora, ta država članica priznaje napredne elektroničke potpise, napredne elektroničke potpise koji se temelje na kvalificiranom certifikatu za elektroničke potpise i kvalificirane elektroničke potpise barem u formatima ili korištenjem metodama koji su određeni u provedbenim aktima iz stavka 5.

2. Ako država članica zahtijeva napredan elektronički potpis koji se temelji na kvalificiranom certifikatu za korištenje *online* uslugom koju nudi tijelo javnog sektora ili uslugom koja se nudi u ime tijela javnog sektora, ta država članica priznaje napredne elektroničke potpise koji se temelje na kvalificiranom certifikatu i kvalificirane elektroničke potpise barem u formatima ili korištenjem metodama koji su određeni u provedbenim aktima iz stavka 5.

3. Za prekograničnо korištenje *online* uslugom koju nudi tijelo javnog sektora države članice ne zahtijevaju elektronički potpis više sigurnosne razine od kvalificiranog elektroničkog potpisa.

4. Komisija može provedbenim aktima utvrditi referentne brojeve normi za napredne elektroničke potpise. Ako napredni elektronički potpis udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima za napredne elektroničke potpise iz stavaka 1. i 2. ovog članka te članka 26. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

5. Komisija, uzimajući u obzir postojeću praksu, norme i pravne akte Unije, putem provedbenih akata do 18. rujna 2015. utvrđuje referentne formate naprednih elektroničkih potpisa ili referentne metode ako se koriste alternativni formati. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 28.*

**Kvalificirani certifikati za elektroničke potpise**

1. Kvalificirani certifikati za elektroničke potpise moraju ispunjavati zahtjeve utvrđene u Prilogu I.

2. Kvalificirani certifikati za elektroničke potpise ne smiju podlijegati obveznim zahtjevima koji prelaze zahtjeve utvrđene u Prilogu I.

3. Kvalificirani certifikati za elektroničke potpise mogu uključivati dodatna posebna obilježja koja nisu obvezna. Ta obilježja ne utječu na interoperabilnost i priznavanje kvalificiranih elektroničkih potpisa.

4. Ako je kvalificirani certifikat za elektroničke potpise opozvan nakon početne aktivacije, on gubi valjanost od trenutka opoziva i njegov se status ni u kojem slučaju ne može vratiti u prijašnje stanje.

5. Države članice mogu utvrditi nacionalna pravila o privremenoj suspenziji kvalificiranih certifikata za elektronički potpis podložno sljedećim uvjetima:

(a) ako je kvalificirani certifikat za elektronički potpis privremeno suspendiran, taj certifikat gubi valjanost tijekom razdoblja suspenzije;

(b) razdoblje suspenzije jasno se naznačuje u bazi podataka certifikata, a status suspenzije je tijekom razdoblja suspenzije vidljiv iz usluge u okviru koje se pružaju informacije o statusu certifikata.

6. Komisija može provedbenim aktima utvrditi referentne brojeve normi za kvalificirane certifikate za elektronički potpis. Ako kvalificirani certifikat za elektronički potpis udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u Prilogu I. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 29.*

**Zahtjevi za kvalificirana sredstva za izradu elektroničkih potpisa**

1. Kvalificirana sredstva za izradu elektroničkih potpisa moraju ispunjavati zahtjeve utvrđene u Prilogu II.

2. Komisija može provedbenim aktima utvrditi referentne brojeve normi za kvalificirana sredstva za izradu elektroničkih potpisa. Ako kvalificirano sredstvo za izradu elektroničkog potpisa udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u Prilogu II. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 30.*

**Certificiranje kvalificiranih sredstava za izradu elektroničkih potpisa**

1. Sukladnost kvalificiranih sredstava za izradu elektroničkih potpisa sa zahtjevima utvrđenima u Prilogu II. potvrđuju odgovarajuća javna ili privatna tijela koja određuju države članice.

2. Države članice obavješćuju Komisiju o nazivima i adresama javnih ili privatnih tijela iz stavka 1. Komisija stavlja te informacije na raspolaganje državama članicama.

3. Certificiranje iz stavka 1. temelji se na jednom od sljedećeg:

(a) postupku sigurnosne evaluacije u skladu s jednom od normi za ocjenu sigurnosti proizvoda informacijske tehnologije uvrštenih na popis koji se utvrđuje u skladu s drugim podstavkom; ili

(b) postupku različitom od postupka iz prethodne točke, pod uvjetom da on koristi usporedive sigurnosne razine te pod uvjetom da javno ili privatno tijelo iz stavka 1. obavijesti Komisiju o tom postupku. Taj se postupak može koristiti samo u slučaju nepostojanja normi navedenih u točki (a) ili kada je postupak sigurnosne evaluacije iz točke (a) u tijeku.

Komisija provedbenim aktima utvrđuje popis normi za ocjenu sigurnosti proizvoda informacijske tehnologije iz točke (a). Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

4. Komisija je ovlaštena donositi delegirane akte u skladu s člankom 47., u vezi s utvrđivanjem posebnih kriterija koje moraju ispuniti tijela iz stavka 1. ovog članka koja su određena.

*Članak 31.*

**Objavljivanje popisa certificiranih kvalificiranih sredstava za izradu elektroničkog potpisa**

1. Države članice obavješćuju Komisiju, bez odgađanja, a najkasnije u roku od mjeseca dana nakon dovršetka certificiranja, o informacijama o sredstvima za izradu kvalificiranog elektroničkog potpisa koja su certificirala tijela iz članka 30. stavka 1. Također obavješćuju Komisiju, bez odgađanja, a najkasnije u roku od mjeseca dana nakon poništenja certificiranja, o informacijama o sredstvima za izradu elektroničkog potpisa koja više nisu certificirana.

2. Na temelju primljenih informacija Komisija izrađuje, objavljuje i vodi popis certificiranih kvalificiranih sredstava za izradu elektroničkog potpisa.

3. Komisija može provedbenim aktima utvrditi formate i postupke primjenjive za potrebe stavka 1. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 32.*

**Zahtjevi za validaciju kvalificiranih elektroničkih potpisa**

1. Postupkom validacije kvalificiranog elektroničkog potpisa potvrđuje se valjanost kvalificiranog elektroničkog potpisa pod sljedećim uvjetima:

(a) certifikat koji podržava potpis je u trenutku potpisivanja bio kvalificirani certifikat za elektronički potpis koji je u skladu Prilogom I.;

(b) kvalificirani certifikat izdao je kvalificirani pružatelj usluga povjerenja i bio je valjan u trenutku potpisivanja;

(c) podaci za validaciju potpisa odgovaraju podacima koji se pružaju pouzdajućoj strani;

(d) jedinstveni skup podataka koji predstavlja potpisnika u certifikatu ispravno je dostavljen pouzdajućoj strani;

(e) korištenje pseudonimom, ako je pseudonim bio korišten u trenutku potpisivanja, jasno je naznačeno pouzdajućoj strani;

(f) elektronički potpis izrađen je sredstvom za izradu kvalificiranog elektroničkog potpisa;

(g) nije ugrožena cjelovitost potpisanih podataka;

(h) zahtjevi predviđeni u članku 26. bili su ispunjeni u trenutku potpisivanja.

2. Sustav koji se upotrebljava za potvrđivanje kvalificiranog elektroničkog potpisa osigurava pouzdajućoj strani točan rezultat postupka validacije i omogućuje joj otkrivanje svih poteškoća bitnih za sigurnost.

3. Komisija može provedbenim aktima utvrditi referentne brojeve normi za validaciju kvalificiranih elektroničkih potpisa. Ako validacija kvalificiranih elektroničkih potpisa udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u stavku 1. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 33.*

**Kvalificirana usluga validacije kvalificiranih elektroničkih potpisa**

1. Kvalificiranu uslugu validacije kvalificiranih elektroničkih potpisa može pružati samo kvalificirani pružatelj usluga povjerenja koji:

(a) pruža validaciju u skladu s člankom 32. stavkom 1.; i

(b) omogućuje pouzdajućim stranama primanje rezultata postupka validacije na automatizirani način koji je pouzdan, učinkovit i nosi napredan elektronički potpis ili napredan elektronički pečat kvalificiranog pružatelja usluge validacije.

2. Komisija može provedbenim aktima utvrditi referentne brojeve normi za kvalificiranu uslugu validacije iz stavka 1. Ako usluga validacije kvalificiranih elektroničkih potpisa udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u stavku 1. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 34.*

**Kvalificirana usluga čuvanja kvalificiranih elektroničkih potpisa**

1. Kvalificiranu uslugu čuvanja kvalificiranih elektroničkih potpisa može pružati samo kvalificirani pružatelj usluga povjerenja koji koristi postupke i tehnologije koje mogu produljiti pouzdanost kvalificiranog elektroničkog potpisa na razdoblje koje je dulje od razdoblja tehnološke valjanosti.

2. Komisija može provedbenim aktima utvrditi referentne brojeve normi za kvalificiranu uslugu čuvanja kvalificiranih elektroničkih potpisa. Ako dogovori za kvalificiranu uslugu čuvanja kvalificiranih elektroničkih potpisa udovoljavaju tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u stavku 1. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*ODJELJAK 5.*

***Elektronički pečati***

*Članak 35.*

**Pravni učinci elektroničkih pečata**

1. Elektroničkom pečatu se kao dokazu u sudskim postupcima ne smiju uskratiti pravni učinak i dopuštenost samo zbog toga što je on u elektroničkom obliku ili zbog toga što ne ispunjava sve zahtjeve za kvalificirani elektronički pečat.

2. Za kvalificirani elektronički pečat predmnijeva se cjelovitost podataka i točnost izvora podataka s kojima je kvalificirani elektronički pečat povezan.

3. Kvalificirani elektronički pečat koji se temelji na kvalificiranom certifikatu izdanom u jednoj državi članici priznaje se kao kvalificirani elektronički pečat u svim ostalim državama članicama.

*Članak 36.*

**Zahtjevi za napredan elektronički pečat**

Napredan elektronički pečat mora ispunjavati sljedeće zahtjeve:

(a) na nedvojben način je povezan s autorom pečata;

(b) omogućava identificiranje autora pečata;

(c) izrađen je korištenjem podacima za izradu elektroničkog pečata koje autor pečata može, uz visoku razinu pouzdanja i pod svojom kontrolom, koristiti za izradu elektroničkog pečata; i

(d) povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka.

*Članak 37.*

**Elektronički pečati u javnim uslugama**

1. Ako država članica zahtijeva napredan elektronički pečat za korištenje *online* uslugom koju nudi tijelo javnog sektora ili usluge koja se nudi u ime tijela javnog sektora, ta država članica priznaje napredne elektroničke pečate, napredne elektroničke pečate koji se temelje na kvalificiranom certifikatu za elektroničke pečate i kvalificirane elektroničke pečate barem u formatima ili korištenjem metodama koji su određeni u provedbenim aktima iz stavka 5.

2. Ako država članica zahtijeva napredan elektronički pečat koji se temelji na kvalificiranom certifikatu za korištenje *online* uslugom koju nudi tijelo javnog sektora ili usluge koja se nudi u ime tijela javnog sektora, ta država članica priznaje napredne elektroničke pečate koji se temelje na kvalificiranom certifikatu i kvalificiranom elektroničkom potpisu barem u formatima ili korištenjem metodama koji su određeni u provedbenim aktima iz stavka 5.

3. Za prekograničnо korištenje *online* uslugom koju nudi tijelo javnog sektora države članice ne zahtijevaju elektronički pečat više sigurnosne razine od kvalificiranog elektroničkog pečata.

4. Komisija može provedbenim aktima utvrditi referentne brojeve normi za napredne elektroničke pečate. Ako napredni elektronički pečat udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima za napredne elektroničke pečate iz stavaka 1. i 2. ovog članka i članka 36. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

5. Komisija, uzimajući u obzir postojeću praksu, norme i pravne akte Unije, do 18. rujna 2015. provedbenim aktima utvrđuje referentne formate naprednih elektroničkih pečata ili referentne metode ako se koriste alternativni formati. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 38.*

**Kvalificirani certifikati za elektroničke pečate**

1. Kvalificirani certifikati za elektroničke pečate moraju ispunjavati zahtjeve utvrđene u Prilogu III.

2. Kvalificirani certifikati za elektroničke pečate ne smiju podlijegati obveznim zahtjevima koji prelaze zahtjeve utvrđene u Prilogu III.

3. Kvalificirani certifikati za elektroničke pečate mogu uključivati dodatna posebna obilježja koja nisu obvezna. Ta obilježja ne utječu na interoperabilnost i priznavanje kvalificiranih elektroničkih pečata.

4. Ako je kvalificirani certifikat za elektronički pečat opozvan nakon početne aktivacije, on gubi valjanost od trenutka opoziva i njegov se status ni u kojem slučaju ne može vratiti u prijašnje stanje.

5. Države članice mogu utvrditi nacionalna pravila o privremenoj suspenziji kvalificiranih certifikata za elektroničke pečate podložno sljedećim uvjetima:

(a) ako je kvalificirani certifikat za elektronički pečat privremeno suspendiran, taj certifikat gubi valjanost tijekom razdoblja suspenzije;

(b) razdoblje suspenzije jasno se naznačuje u bazi podataka certifikata, a status suspenzije je tijekom razdoblja suspenzije vidljiv iz usluge u okviru koje pružaju informacije o statusu certifikata.

6. Komisija može provedbenim aktima utvrditi referentne brojeve normi za kvalificirane certifikate za elektroničke pečate. Ako kvalificirani certifikat za elektronički pečat udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u Prilogu III. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*Članak 39.*

**Kvalificirana sredstva za izradu elektroničkog pečata**

1. Članak 29. primjenjuje se *mutatis mutandis* na zahtjeve za kvalificirana sredstva za izradu elektroničkog pečata.

2. Članak 30. primjenjuje se *mutatis mutandis* na certificiranje kvalificiranih sredstva za izradu elektroničkog pečata.

3. Članak 31. primjenjuje se *mutatis mutandis* na objavu popisa certificiranih kvalificiranih sredstava za izradu elektroničkih pečata.

*Članak 40.*

**Validacija i čuvanje kvalificiranih elektroničkih pečata**

Članci 32., 33. i 34. primjenjuju se *mutatis mutandis* na validaciju i čuvanje kvalificiranih elektroničkih pečata.

*ODJELJAK 6.*

***Elektronički vremenski žigovi***

*Članak 41.*

**Pravni učinak elektroničkih vremenskih žigova**

1. Elektroničkom vremenskom žigu se kao dokazu u sudskim postupcima ne smiju uskratiti pravni učinak i dopuštenost samo zbog toga što je on u elektroničkom obliku ili zbog toga što ne ispunjava sve zahtjeve kvalificiranog elektroničkog vremenskog žiga.

2. Za kvalificirani elektronički vremenski žig predmnijeva se točnost datuma i vremena koje pokazuje te cjelovitost podataka s kojima su datum i vrijeme povezani.

3. Kvalificirani elektronički vremenski žig izdan u jednoj državi članici priznaje se kao kvalificirani elektronički vremenski žig u svim državama članicama.

*Članak 42.*

**Zahtjevi za kvalificirane elektroničke vremenske žigove**

1. Kvalificirani elektronički vremenski žig mora ispunjavati sljedeće zahtjeve:

(a) povezuje datum i vrijeme s podacima na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene promjene podataka;

(b) temelji se na izvoru točnog vremena povezanom s koordiniranim svjetskim vremenom; i

(c) potpisan je pomoću naprednog elektroničkog potpisa ili pečaćen pomoću naprednog elektroničkog pečata kvalificiranog pružatelja usluga povjerenja ili jednakovrijednom metodom.

2. Komisija može provedbenim aktima utvrditi referentne brojeve normi za povezivanje datuma i vremena s podacima i za izvore točnog vremena. Ako povezivanje datuma i vremena s podacima i izvor točnog vremena udovoljavaju tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u stavku 1. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*ODJELJAK 7.*

***Usluge elektroničke preporučene dostave***

*Članak 43.*

**Pravni učinak usluge elektroničke preporučene dostave**

1. Podacima poslanima i primljenima uporabom usluge elektroničke preporučene dostave ne smije se kao dokazima u sudskim postupcima uskratiti pravni učinak i dopuštenost samo zbog toga što su oni u elektroničkom obliku ili zbog toga što ne ispunjavaju sve zahtjeve kvalificirane usluge elektroničke preporučene dostave.

2. Za podatke poslane i primljene uporabom kvalificirane usluge elektroničke preporučene dostave predmnijeva se cjelovitost podataka, slanje tih podataka od strane identificiranog pošiljatelja, njihov primitak od strane identificiranog primatelja te točnost datuma i vremena slanja i primitka podataka kako su naznačeni kvalificiranom uslugom elektroničke preporučene dostave.

*Članak 44.*

**Zahtjevi za kvalificirane usluge elektroničke preporučene dostave**

1. Kvalificirane usluge elektroničke preporučene dostave moraju ispunjavati sljedeće zahtjeve:

(a) pruža ih jedan kvalificirani pružatelj usluga povjerenja ili više njih;

(b) uz visoku razinu pouzdanja osiguravaju identifikaciju pošiljatelja;

(c) osiguravaju identifikaciju primatelja prije dostave podataka;

(d) slanje i primanje podataka osigurano je naprednim elektroničkim potpisom ili naprednim elektroničkim pečatom kvalificiranog pružatelja usluga povjerenja na način kojim se isključuje mogućnost nezapažene promjene podataka;

(e) pošiljatelju i primatelju podataka jasno se naznačuje svaka promjena podataka potrebna radi slanja ili primanja podataka;

(f) datum i vrijeme slanja, primanja i eventualne promjene podataka naznačuju se kvalificiranim elektroničkim vremenskim žigom.

U slučaju prijenosa podataka između dvaju kvalificiranih pružatelja usluga povjerenja ili više njih, zahtjevi iz točaka od (a) do (f) primjenjuju se na sve kvalificirane pružatelje usluga povjerenja.

2. Komisija može provedbenim aktima utvrditi referentne brojeve normi za postupke slanja i primanja podataka. Ako postupak slanja i primanja podataka udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u stavku 1. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

*ODJELJAK 8.*

***Autentikacija mrežnih stranica***

*Članak 45.*

**Zahtjevi za kvalificirane certifikate za autentikaciju mrežnih stranica**

1. Kvalificirani certifikati za autentikaciju mrežnih stranica moraju ispunjavati zahtjeve utvrđene u Prilogu IV.

2. Komisija može provedbenim aktima utvrditi referentne brojeve normi za kvalificirane certifikate za autentikaciju mrežnih stranica. Ako kvalificirani certifikat za autentikaciju mrežnih stranica udovoljava tim normama, smatra se da je postignuta sukladnost sa zahtjevima utvrđenima u Prilogu IV. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 48. stavka 2.

POGLAVLJE IV.

**ELEKTRONIČKI DOKUMENTI**

*Članak 46.*

**Pravni učinci elektroničkih dokumenata**

Elektroničkom dokumentu se kao dokazu u sudskim postupcima ne smiju uskratiti pravni učinak i dopuštenost samo zbog toga što je on u elektroničkom obliku.

POGLAVLJE V.

**DELEGIRANJA OVLASTI I PROVEDBENE ODREDBE**

*Članak 47.*

**Izvršavanje ovlasti**

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.

2. Ovlast za donošenje delegiranih akata iz članka 30. stavka 4. dodjeljuje se Komisiji na neodređeno razdoblje počevši od 17. rujna 2014.

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 30. stavka 4. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv proizvodi učinke dan nakon objave spomenute odluke u *Službenom listu Europske unije* ili na kasniji datum naveden u spomenutoj odluci. Opoziv ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.

5. Delegirani akt donesen na temelju članka 30. stavka 4. stupa na snagu samo ako Europski parlament ili Vijeće u roku od dva mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne ulože nikakav prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće uložiti prigovore. Taj se rok produljuje za dva mjeseca na inicijativu Europskog parlamenta ili Vijeća.

*Članak 48.*

**Postupak odbora**

1. Komisiji pomaže odbor. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.

2. Kod upućivanja na ovaj stavak, primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

POGLAVLJE VI.

**ZAVRŠNE ODREDBE**

*Članak 49.*

**Preispitivanje**

Komisija preispituje primjenu ove Uredbe i podnosi izvješće Europskom parlamentu i Vijeću najkasnije do 1. srpnja 2020. Komisija posebno provodi evaluaciju potrebe za izmjenom područja primjene ove Uredbe ili njezinih određenih odredaba, uključujući članak 6., članak 7. točku (f) te članke 34., 43., 44. i 45., uzimajući u obzir iskustvo stečeno primjenom ove Uredbe, kao i tehnološki, tržišni i pravni razvoj.

Izvješće iz prvog stavka je, prema potrebi, popraćeno zakonodavnim prijedlozima.

Osim toga, svake četiri godine nakon izvješća iz prvog stavka, Komisija podnosi izvješće Europskom parlamentu i Vijeću o napretku prema ostvarivanju ciljeva ove Uredbe.

*Članak 50.*

**Stavljanje izvan snage**

1. Direktiva 1999/93/EZ stavlja se izvan snage s učinkom od 1. srpnja 2016.

2. Upućivanja na Direktivu stavljenu izvan snage tumače se kao upućivanja na ovu Uredbu.

*Članak 51.*

**Prijelazne mjere**

1. Sredstva za sigurnu izradu potpisa čija je sukladnost utvrđena u skladu s člankom 3. stavkom 4. Direktive 1999/93/EZ smatraju se kvalificiranim sredstvima za izradu elektroničkih potpisa prema ovoj Uredbi.

2. Kvalificirani certifikati izdani fizičkim osobama prema Direktivi 1999/93/EZ smatraju se kvalificiranim certifikatima za elektroničke potpise prema ovoj Uredbi do njihova isteka.

3. Pružatelj usluga certificiranja koji izdaje kvalificirane certifikate u skladu s Direktivom 1999/93/EZ podnosi izvješće o ocjenjivanju sukladnosti nadzornom tijelu što je prije moguće, no najkasnije do 1. srpnja 2017. Do podnošenja takvog izvješća o ocjenjivanju sukladnosti i dovršetka ocjenjivanja od strane nadzornog tijela taj se pružatelj usluga certificiranja smatra kvalificiranim pružateljem usluga povjerenja prema ovoj Uredbi.

4. Ako pružatelj usluga certificiranja koji izdaje kvalificirane certifikate prema Direktivi 1999/93/EZ nadzornom tijelu ne podnese izvješće o ocjenjivanju sukladnosti u roku iz stavka 3., taj se pružatelj usluga certificiranja ne smatra kvalificiranim pružateljem usluga povjerenja prema ovoj Uredbi od 2. srpnja 2017.

*Članak 52.*

**Stupanje na snagu**

1. Ova Uredba stupa na snagu dvadesetog dana nakon dana objave u *Službenom listu Europske unije*.

2. Ova se Uredba primjenjuje od 1. srpnja 2016. izuzevši sljedeće:

(a) članak 8. stavak 3., članak 9. stavak 5., članak 12. stavci od 2. do 9., članak 17. stavak 8., članak 19. stavak 4., članak 20. stavak 4., članak 21. stavak 4., članak 22. stavak 5., članak 23. stavak 3., članak 24. stavak 5., članak 27. stavci 4. i 5., članak 28. stavak 6., članak 29. stavak 2., članak 30. stavci 3. i 4., članak 31. stavak 3., članak 32. stavak 3., članak 33. stavak 2., članak 34. stavak 2., članak 37. stavci 4. i 5., članak 38. stavak 6., članak 42. stavak 2., članak 44. stavak 2., članak 45. stavak 2., članak 47. i članak 48. primjenjuju se od 17. rujna 2014.;

(b) članak 7., članak 8. stavci 1. i 2., članci 9.,10., 11. i članak 12. stavak 1. primjenjuju se od dana primjene provedbenih akata iz članka 8. stavka 3. i članka 12. stavka 8.;

(c) članak 6. primjenjuje se nakon tri godine od dana primjene provedbenih akata iz članka 8. stavka 3. i članka 12. stavka 8.

3. Ako je prijavljeni sustav elektroničke identifikacije uvršten na popis koji je objavila Komisija na temelju članka 9. prije datuma iz stavka 2. točke (c) ovog članka, priznavanje sredstava elektroničke identifikacije u okviru tog sustava na temelju članka 6. odvija se najkasnije 12 mjeseci nakon objave tog sustava, ali ne prije datuma iz stavka 2. točke (c) ovog članka.

4. Neovisno o stavku 2. točki (c) ovog članka, država članica može odlučiti da sredstva elektroničke identifikacije u okviru sustava elektroničke identifikacije koji je prijavila druga država članica na temelju člankom 9. stavka 1. budu priznata u prvoj državi članici od dana primjene provedbenih akata iz članka 8. stavka 3. i članka 12. stavka 8. Dotične države članice o tome obavješćuju Komisiju. Komisija objavljuje te informacije.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 23. srpnja 2014.

| *Za Parlament* | *Za Vijeće* |
|---|---|
| *Predsjednik* | *Predsjednik* |
| M. SCHULZ | S. GOZI |

*PRILOG I.*

**ZAHTJEVI ZA KVALIFICIRANE CERTIFIKATE ZA ELEKTRONIČKE POTPISE**

Kvalificirani certifikati za elektroničke potpise sadržavaju:

(a) naznaku, barem u obliku prikladnom za automatiziranu obradu, da je certifikat izdan kao kvalificirani certifikat za elektroničke potpise;

(b) skup podataka koji nedvojbeno predstavlja kvalificiranog pružatelja usluga povjerenja koji izdaje kvalificirane certifikate uključujući barem državu članicu u kojoj pružatelj ima poslovni nastan i

— za pravnu osobu: naziv i, kada je to primjenjivo, registracijski broj kako je navedeno u službenoj evidenciji,

— za fizičku osobu: ime osobe;

(c) barem ime potpisnika, ili pseudonim; ako se koristi pseudonimom, on se mora jasno naznačiti;

(d) podatke za validaciju elektroničkog potpisa koji odgovaraju podacima za izradu elektroničkog potpisa;

(e) podatke o početku i završetku roka valjanosti certifikata;

(f) identifikacijsku oznaku certifikata koja mora biti jedinstvena za kvalificiranog pružatelja usluga povjerenja;

(g) napredan elektronički potpis ili napredan elektronički pečat kvalificiranog pružatelja usluga povjerenja koji izdaje certifikat;

(h) lokaciju na kojoj je besplatno dostupan certifikat koji podržava napredan elektronički potpis ili napredan elektronički pečat iz točke (g);

(i) lokaciju usluga koje se mogu koristiti za ispitivanje statusa valjanosti kvalificiranog certifikata;

(j) ako su podaci za izradu elektroničkog potpisa koji su povezani s podacima za validaciju elektroničkog potpisa smješteni u kvalificiranom sredstvu za izradu elektroničkog potpisa, odgovarajuću naznaku navedenog, barem u obliku prikladnom za automatiziranu obradu.

*PRILOG II.*

**ZAHTJEVI ZA KVALIFICIRANA SREDSTVA ZA IZRADU ELEKTRONIČKIH POTPISA**

1. Kvalificirana sredstva za izradu elektroničkih potpisa moraju pomoću odgovarajućih tehničkih i postupovnih sredstava osigurati barem da:

   (a) je u razumnoj mjeri osigurana povjerljivost podataka za izradu elektroničkog potpisa koji se upotrebljavaju za izradu elektroničkog potpisa;

   (b) se podaci za izradu elektroničkog potpisa koji se upotrebljavaju za izradu elektroničkog potpisa praktički mogu pojaviti samo jedanput;

   (c) se podaci za izradu elektroničkog potpisa koji se upotrebljavaju za izradu elektroničkog potpisa ne mogu, uz razuman stupanj pouzdanja, iz njega izvesti, te da je elektronički potpis pouzdano zaštićen od krivotvorenja korištenjem trenutačno dostupnom tehnologijom;

   (d) da zakoniti potpisnik može pouzdano zaštititi podatke za izradu elektroničkog potpisa koji se koriste za izradu elektroničkog potpisa od korištenja od strane drugih osoba.

2. Kvalificirana sredstva za izradu elektroničkih potpisa ne smiju mijenjati podatke koji se potpisuju niti priječe prikazivanje takvih podataka potpisniku prije potpisivanja.

3. Generiranje ili upravljanje podacima za izradu elektroničkog potpisa u ime potpisnika može obavljati isključivo kvalificirani pružatelj usluga povjerenja.

4. Ne dovodeći u pitanje stavak 1. točku (d), kvalificirani pružatelji usluga povjerenja koji upravljaju podacima za izradu elektroničkog potpisa u ime potpisnika smiju duplicirati podatke za izradu elektroničkog potpisa isključivo u svrhu izrade sigurnosnih kopija pod uvjetom da su ispunjeni sljedeći zahtjevi:

   (a) sigurnost dupliciranih skupova podataka mora biti na razini jednakoj razini sigurnosti izvornih skupova podataka;

   (b) broj dupliciranih skupova podataka ne prelazi broj neophodan za osiguravanje kontinuiteta usluge.

*PRILOG III.*

**ZAHTJEVI ZA KVALIFICIRANE CERTIFIKATE ZA ELEKTRONIČKE PEČATE**

Kvalificirani certifikati za elektroničke pečate sadržavaju:

(a) naznaku, barem u obliku prikladnom za automatiziranu obradu, da je certifikat izdan kao kvalificirani certifikat za elektroničke pečate;

(b) skup podataka koji nedvojbeno predstavljaju kvalificiranog pružatelja usluga povjerenja koji izdaje kvalificirane certifikate, uključujući barem državu članicu u kojoj pružatelj ima poslovni nastan i

— za pravnu osobu: naziv i, kada je to primjenjivo, registracijski broj kako je navedeno u službenoj evidenciji,

— za fizičku osobu: ime osobe;

(c) barem naziv autora pečata i, kada je to primjenjivo, registracijski broj kako je navedeno u službenoj evidenciji;

(d) podatke za validaciju elektroničkog pečata koji odgovaraju podacima za izradu elektroničkog pečata;

(e) podatke o početku i kraju roka valjanosti certifikata;

(f) identifikacijsku oznaku certifikata koja mora biti jedinstvena za tog kvalificiranog pružatelja usluga povjerenja;

(g) napredan elektronički potpis ili napredan elektronički pečat kvalificiranog pružatelja usluga povjerenja koji izdaje certifikat;

(h) lokaciju na kojoj je besplatno dostupan certifikat koji podržava napredan elektronički potpis ili napredan elektronički pečat iz točke (g);

(i) lokaciju usluga koje se mogu koristiti za ispitivanje statusa valjanosti kvalificiranog certifikata;

(j) kada su podaci za izradu elektroničkog pečata koji su povezani s podacima za validaciju elektroničkog pečata smješteni u kvalificiranom sredstvu za izradu elektroničkog pečata, odgovarajuću naznaku navedenog, barem u obliku prikladnom za automatiziranu obradu.

*PRILOG IV.*

**ZAHTJEVI ZA KVALIFICIRANE CERTIFIKATE ZA AUTENTIKACIJU MREŽNIH STRANICA**

Kvalificirani certifikati za autentikaciju mrežnih stranica sadrže:

(a) naznaku, barem u obliku prikladnom za automatiziranu obradu, da je certifikat izdan kao kvalificirani certifikat za autentikaciju mrežnih stranica;

(b) skup podataka koji nedvojbeno predstavljaju kvalificiranog pružatelja usluga povjerenja koji izdaje kvalificirane certifikate, uključujući barem državu članicu u kojoj pružatelj ima poslovni nastan i

— za pravnu osobu: naziv i, kada je to primjenjivo, registracijski broj kako je navedeno u službenoj evidenciji,

— za fizičku osobu: ime osobe;

(c) za fizičke osobe: barem ime osobe kojoj je izdan certifikat ili pseudonim. Ako se koristi pseudonim, on se mora jasno naznačiti;

za pravne osobe: barem naziv pravne osobe kojoj je izdan certifikat i, kada je to primjenjivo, registracijski broj kako je navedeno u službenoj evidenciji;

(d) elementi adrese, uključujući barem grad i državu, fizičke ili pravne osobe kojoj je izdan certifikat i, kada je to primjenjivo, kako je navedeno u službenoj evidenciji;

(e) naziv(i) domene(-a) kojom(-ima) upravlja fizička ili pravna osoba kojoj je izdan certifikat;

(f) podatke o početku i kraju roka valjanosti certifikata;

(g) identifikacijsku oznaku certifikata koja mora biti jedinstvena za kvalificiranog pružatelja usluga povjerenja;

(h) napredan elektronički potpis ili napredan elektronički pečat kvalificiranog pružatelja usluga povjerenja koji izdaje certifikat;

(i) lokaciju na kojoj je besplatno dostupan certifikat koji podržava napredan elektronički potpis ili napredan elektronički pečat iz točke (h);

(j) lokaciju usluga statusa valjanosti certifikata koje se mogu koristiti za ispitivanje statusa valjanosti kvalificiranog certifikata.