



EVROPSKA KOMISIJA

Bruselj, 4.6.2012  
COM(2012) 238 final

2012/0146 (COD)

Predlog

**UREDBA EVROPSKEGA PARLAMENTA IN SVETA**

**o elektronski identifikaciji in skrbniških storitvah za elektronske transakcije na  
notranjem trgu**

(Besedilo velja za EGP)

{SWD(2012) 135 final}

{SWD(2012) 136 final}

## OBRAZLOŽITVENI MEMORANDUM

### 1. OZADJE PREDLOGA

Ta memorandum pojasnjuje predlagani pravni okvir, zasnovan za krepitev zaupanja v elektronske transakcije na notranjem trgu.

Ustvarjanje zaupanja v spletno okolje je ključ do gospodarskega razvoja. Zaradi pomanjkanje zaupanja potrošniki, podjetja in uprave oklevajo pri izvajanju transakcij v elektronski obliki in pri sprejemanje novih storitev.

*Evropska digitalna agenda*<sup>1</sup> opredeljuje obstoječe ovire za digitalni razvoj v Evropi in predlaga zakonodajo za elektronske podpise (ključni ukrep št. 3) ter medsebojno priznavanje e-identifikacije in e-avtentikacije (ključni ukrep št. 16), s čimer vzpostavlja jasen pravni okvir za odpravo razdrobljenosti in pomanjkanja interoperabilnosti, krepitev digitalnega državljanstva ter preprečevanje kibernetkega kriminala. Zakonodaja, ki zagotavlja medsebojno priznavanje elektronske identifikacije in avtentikacije v EU in pregled direktive o elektronskem podpisu, je prav tako ključni ukrep v *Aktu za enotni trg*<sup>2</sup> za uresničitev enotnega digitalnega trga. *Načrt za stabilnost in rast*<sup>3</sup> poudarja ključno vlogo prihodnjega skupnega pravnega okvira za čezmejno medsebojno priznavanje in sprejemanje elektronske identifikacije in avtentikacije pri razvoju digitalnega gospodarstva.

Predlagani pravni okvir, ki je sestavljen iz *Uredbe Evropskega parlamenta in Sveta o elektronski identifikaciji in skrbniških storitvah za elektronske transakcije na notranjem trgu*, si prizadeva za vzpostavitev varnih in nemotenih elektronskih interakcij med podjetji, državljani in javnimi organi, s čimer bi se povečala učinkovitost javnih in zasebnih spletnih storitev, e-poslovanja in elektronskega trgovanja v EU.

Obstoječa zakonodaja EU, in sicer Direktiva 1999/93/ES o okviru *Skupnosti za elektronski podpis*<sup>4</sup>, v glavnem zajema le elektronske podpise. Celovit evropski čezmejni in medsektorski okvir za varno, zanesljivo in enostavno uporabo elektronskih transakcij, ki bi zajemal elektronsko identifikacijo, avtentikacijo in elektronske podpise, ne obstaja.

Cilj je izboljšati obstoječo zakonodajo in jo razširiti tako, da bo zajemala medsebojno priznavanje in sprejemanje priglašeni shem elektronske identifikacije ter drugih bistvenih povezanih skrbniških elektronskih storitev na ravni EU.

### 2. REZULTATI POSVETOVANJ Z ZAINTERESIRANIMI STRANMI IN OCENE UČINKA

Ta pobuda je rezultat obsežnih posvetovanj o pregledu sedanjega pravnega okvira za elektronske podpise, v okviru katerih je Komisija zbrala povratne informacije od držav članic, Evropskega parlamenta in drugih zainteresiranih strani<sup>5</sup>. Javno spletno posvetovanje je bilo dopolnjeno s „posvetovalnim odborom MSP“ za opredelitev posebnih stališč in potreb MSP

<sup>1</sup> COM(2010) 245 z dne 19.5.2010.

<sup>2</sup> COM(2011) 206 final z dne 13. aprila 2011.

<sup>3</sup> COM(2011) 669, 12.10.2011.

<sup>4</sup> UL L 13, 19.01.2000, str. 12.

<sup>5</sup> Podrobnosti o posvetovanjih najdete na [http://ec.europa.eu/information\\_society/policy/esignature/eu\\_legislation/revision](http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision).

in drugimi usmerjenimi posvetovanji z zainteresiranimi stranmi<sup>6,7</sup>. Komisija je začela tudi številne študije v zvezi z elektronsko identifikacijo, avtentikacijo, podpisom in povezanimi skrbniškimi storitvami (eIAS).

Posvetovanja so jasno pokazala, da se velika večina zainteresiranih strani strinja, da je treba pregledati sedanji okvir in zapolniti vrzeli, ki jih je pustila direktiva o elektronskem podpisu. Prevladovalo je mnenje, da bi to bil boljši odziv na izzive, ki jih predstavljata hiter razvoj novih tehnologij (zlasti spletni in mobilni dostop) in povečana globalizacija, ob tem pa bi se ohranila tehnološka nevtralnost pravnega okvira.

Komisija je v skladu s svojo politiko „boljših predpisov“ izvedla oceno učinka za možnosti politike. Ocenjeni so bili trije sklopi možnosti politike, ki so obravnavali (1) področje uporabe novega okvira, (2) pravni instrument in (3) raven potrebnega nadzora<sup>8</sup>. Izkazalo se je, da najprimernejša možnost politike krepi pravno varnost, spodbuja usklajevanje nacionalnega nadzora, zagotavlja medsebojno priznavanje in sprejemanje shem elektronske identifikacije in zajema bistvene povezane skrbniške storitve. V oceni učinka je bilo ugotovljeno, da bi na ta način znatno izboljšali pravno varnost, gotovost in zaupanje v zvezi s čezmejnimi elektronskimi transakcijami, kar bi prineslo manjšo razdrobljenost trga.

### 3. PRAVNI ELEMENTI PREDLOGA

#### 3.1 Pravna podlaga

Ta predlog temelji na členu 114 PDEU, ki se nanaša na sprejetje pravil za odpravo obstoječih ovir za delovanje notranjega trga. Državljeni, podjetja in uprave bodo imeli korist od čezmejnega medsebojnega priznavanja in sprejemanja elektronske identifikacije, avtentikacije, podpisov in drugih skrbniških storitev, kadar so te potrebne za dostop do elektronskih postopkov ali transakcij in njihov zaključek.

Uredba velja za najustreznejši pravni instrument. Zaradi neposredne uporabe Uredbe v skladu s členom 288 PDEU se bo zmanjšala pravna razdrobljenost in zagotovila večja pravna varnost z uvedbo usklajenega sklopa temeljnih pravil, ki bodo pripomogla k delovanju notranjega trga.

---

<sup>6</sup> Delavnica z zainteresiranimi stranmi je potekala 10. marca 2011 s predstavniki iz javnega in zasebnega sektorja ter akademskih krogov; na delavnici je potekala razprava o tem, kateri zakonodajni ukrepi so potrebni za obravnavanje prihodnjih izzivov. To je bil interaktivni forum za izmenjavo mnenj in razpravo o različnih stališčih o vprašanjih iz javnega posvetovanja. Več organizacij je na lastno pobudo poslalo dokumente o stališčih.

<sup>7</sup> Poljsko predsedstvo Sveta EU je 9. novembra 2011 v Varšavi organiziralo zasedanje z državami članicami o elektronskem podpisu in 17. novembra 2011 v Poznanu zasedanje o elektronski identifikaciji. 25. januarja 2012 je Komisija z državami članicami organizirala delavnico, na kateri so razpravljali o ostalih vprašanjih v zvezi z elektronsko identifikacijo, avtentikacijo in podpisom.

<sup>8</sup> V prvem sklopu so proučili štiri možnosti: razveljavitev direktive o elektronskem podpisu; brez spremembe politike; krepitev pravne varnosti, spodbujanje usklajevanja nacionalnega nadzora ter zagotavljanje medsebojnega priznavanja in sprejemanja elektronske identifikacije po vsej EU; in četrtič razširitev za vključitev določenih povezanih varnih storitev. Drugi sklop je zajemal oceno relativnih koristi možnosti urejanja z enim ali dvema instrumentoma in z direktivo ali uredbo. V tretjem sklopu so bile proučene možnosti, ki jih nudi izvajanje shem nacionalnega nadzora na podlagi skupnih bistvenih zahtev po nadzoru v primerjavi s sistemom nadzora na ravni EU. S pomočjo skupine vseh zainteresiranih generalnih direktoratsv Komisije je bila vsaka možnost politike ocenjena z vidika učinkovitosti pri doseganju ciljev politike, gospodarskega učinka na zainteresirane strani (tudi proračun institucij EU), socialnega in okoljskega učinka ter učinka na upravno obremenitev.

### 3.2 Subsidiarnost in sorazmernost

Ukrepi EU so upravičeni, če se upošteva načelo subsidiarnosti:

#### *a) nadnacionalna narava problema (preskus nujnosti)*

Nadnacionalna narava eIAS zahteva ukrepanje na ravni EU. Zgolj domače (tj. nacionalno) ukrepanje ne bi zadostovalo za uresničevanje ciljev iz *Strategije Evropa 2020*<sup>9</sup>. Nasprotno pa so izkušnje pokazale, da so nacionalni ukrepi dejansko ustvarili ovire za interoperabilnost elektronskih podpisov po vsej EU in da imajo trenutno enak učinek tudi na elektronsko identifikacijo, elektronsko avtentikacijo in povezane skrbniške storitve. Zato mora EU ustvariti učinkovit okvir za obravnavanje čezmejne interoperabilnosti in izboljšanje usklajevanja shem nacionalnega nadzora. Vendar elektronske identifikacije v predlagani uredbi ni mogoče obravnavati na enak splošen način kot druge skrbniške elektronske storitve, ker je izdajanje sredstev za identifikacijo v nacionalni pristojnosti. Zato se predlog osredotoča izključno na čezmejne vidike elektronske identifikacije.

Predlagana uredba ustvarja enake konkurenčne pogoje za podjetja, ki zagotavljajo skrbniške storitve, kadar razlike, ki trenutno obstajajo v nacionalni zakonodaji, pogosto vodijo k pravni negotovosti in dodatni obremenitvi. Pravna varnost se močno poveča, ko države članice jasno sprejmejo obveznosti glede kvalificiranih skrbniških storitev, kar bo dodatno spodbudilo podjetja k poslovanju v tujini. Podjetje bo na primer lahko po elektronski poti sodelovalo na javnih razpisih, ki jih objavi uprava druge države članice, ne da bi bil njegov elektronski podpis zavrnjen zaradi posebnih nacionalnih zahtev in težav z interoperabilnostjo. Podobno bo podjetje imelo možnost elektronskega podpisa pogodb s partnerjem iz druge države članice, ne da bi bilo podvrženo drugačnim pravnim zahtevam za skrbniške storitve, kot so elektronski žigi, elektronski dokumenti ali časovni žigi. Poleg tega bo obvestilo o neizpolnitvi obveznosti dostavljeno iz ene države članice v drugo z zagotovljeno pravno varnostjo v obeh državah članicah. Nazadnje bo tudi spletno trgovanje bolj zaupanja vredno, ko bodo kupci imeli sredstvo za preverjanje, da se zares nahajajo na spletni strani izbranega trgovca in ne na morebitni lažni spletni strani.

Vzajemno priznana sredstva elektronske identifikacije in široko sprejeti elektronski podpisi bodo poenostavili čezmejno zagotavljanje številnih storitev na notranjem trgu in podjetjem omogočili čezmejno poslovanje brez soočanja z ovirami in interakcij z javnimi organi. V praksi bo to pomenilo znatno izboljšanje učinkovitosti za podjetja in državljane, ko gre za izpolnjevanje upravnih formalnosti. Na primer, študent bo imel možnost elektronskega vpisa na univerzo v tujini, državljani bo lahko oddal davčno napoved po spletu drugi državi članici, pacient pa bo po spletu lahko dostopal do svojih zdravstvenih podatkov. Brez takih vzajemno priznanih sredstev elektronske identifikacije zdravnik ne bo mogel dostopati do pacientovih zdravstvenih podatkov, ki jih potrebuje za njegovo zdravljenje, zdravstvene in laboratorijske preiskave, ki jih je pacient že opravil, pa bo treba ponoviti;

#### *b) dodana vrednost (preskus učinkovitosti)*

Zgoraj navedenih ciljev trenutno ni mogoče doseči s prostovoljnim usklajevanjem med državami članicami, niti ni razumno pričakovati, da se bo to zgodilo v prihodnosti. To vodi do podvajanja prizadevanj, določanja različnih standardov, nadnacionalnih značilnosti prelivanja,

<sup>9</sup> Sporočilo Komisije: Evropa 2020. Strategija za pametno, trajnostno in vključujočo rast, COM(2010) 2020, 3.3.2010.

ki ga ustvarja IKT, in upravne zapletenosti vzpostavitve takega usklajevanja z dvostranskimi in večstranskimi sporazumi.

Poleg tega potreba po premagovanju težav, kot sta (a) odsotnost pravne varnosti zaradi različnih nacionalnih določb, ki izhajajo iz različnih razlag direktive o elektronskem podpisu, in (b) pomanjkanje interoperabilnosti sistemov za elektronski podpis, vzpostavljenih na nacionalni ravni, zaradi neenotne uporabe tehničnih standardov zahteva v vseh državah članicah EU tako usklajevanje, ki ga je mogoče učinkoviteje doseči na ravni EU.

### **3.3 Podrobna obrazložitev predloga**

#### *3.3.1 POGLAVJE I – SPLOŠNE DOLOČBE*

Člen 1 opredeljuje vsebino Uredbe.

Člen 2 določa stvarno področje uporabe Uredbe.

Člen 3 vsebuje opredelitve pojmov, ki se uporabljajo v Uredbi. Nekatere opredelitve so prevzete iz Direktive 1999/93/ES, druge pa so pojasnjene, dopolnjene z dodatnimi elementi ali na novo uvedene.

Člen 4 določa načela notranjega trga, kar zadeva ozemeljsko uporabo Uredbe. Izrecno je navedeno, da ni omejitev v zvezi s svobodo zagotavljanja storitev in prostim pretokom izdelkov.

#### *3.3.2 POGLAVJE II – ELEKTRONSKA IDENTIFIKACIJA*

Člen 5 določa medsebojno priznavanje in sprejemanje sredstev elektronske identifikacije v skladu s shemo, ki se prikladi Komisiji pod pogoji, določenimi v Uredbi. Večina držav članic EU je že uvedla določeno obliko sistema elektronske identifikacije. Vendar pa se razlikujejo v številnih vidikih. Pomanjkanje skupne pravne podlage, ki bi od vsake države članice zahtevala priznavanje in sprejetje sredstev elektronske identifikacije za dostop do spletnih storitev, izdanih v drugih državah članicah, skupaj z neustrezno čezmejno interoperabilnostjo nacionalnih elektronskih identifikacij ustvarja ovire, ki državljanom in podjetjem preprečujejo, da bi v celoti izkoristili enotni digitalni trg. Medsebojno priznavanje in sprejemanje vseh sredstev elektronske identifikacije v okviru priglašene sheme v skladu s to uredbo odpravlja te pravne ovire.

Uredba držav članic ne zavezuje k uvedbi ali priglasitvi sheme elektronske identifikacije, temveč od njih zahteva priznavanje in sprejetje priglašene elektronske identifikacije za tiste spletne storitve, pri katerih je elektronska identifikacija potrebna za pridobitev dostopa na nacionalni ravni. Potencialno povečanje ekonomij obsega zaradi čezmejne uporabe priglašene sredstev elektronske identifikacije in sistemov za avtentikacijo lahko države članice spodbudi k priglasitvi njihovih shem elektronske identifikacije. Člen 6 določa pet pogojev za priglasitev ureditev elektronske identifikacije:

Države članice lahko priglasijo sheme elektronske identifikacije, ki jih sprejmejo v svoji pristojnosti, kadar je elektronska identifikacija potrebna za javne storitve. Dodatna zahteva je, da mora zadevno sredstvo elektronske identifikacije izdati država članica, ki je shemo priglasila, oziroma mora biti sredstvo elektronske identifikacije izdano v njenem imenu ali vsaj v njeni pristojnosti.

Države članice morajo zagotoviti nedvoumno povezavo med podatki elektronske identifikacije in zadevno osebo. Ta obveznost ne pomeni, da oseba ne more imeti več sredstev elektronske identifikacije, vendar pa morajo biti vsa sredstva povezana z isto osebo.

Zanesljivost elektronske identifikacije je odvisna od razpoložljivosti sredstev avtentikacije (tj. možnosti preverjanja veljavnosti podatkov elektronske identifikacije). Uredba države članice, ki ureditev prigrasijo, zavezuje k brezplačnemu zagotavljanju spletne avtentikacije za tretje osebe. Možnost avtentikacije mora biti na voljo brez prekinitve. Osebam, ki uporabljajo tako avtentikacijo, ne smejo biti naložene posebne tehnične zahteve, kot je strojna ali programska oprema. Ta določba pa ne velja za zahteve v zvezi z uporabniki (imetniki) sredstev elektronske identifikacije, ki so tehnično potrebne za uporabo sredstev elektronske identifikacije, kot so čitalniki kartic.

Države članice morajo sprejeti odgovornost za nedvoumnost povezave (tj. da podatki identifikacije, ki so pripisani osebi, niso povezani s katero koli drugo osebo) in za možnost avtentikacije (tj. možnost preverjanja veljavnosti podatkov elektronske identifikacije). Odgovornost držav članic ne vključuje drugih vidikov postopka identifikacije ali transakcij, ki zahtevajo identifikacijo.

Člen 7 vsebuje pravila za prigrasitev shem elektronske identifikacije Komisiji.

Člen 8 želi zagotoviti tehnično interoperabilnost prigrasjenih shem identifikacije z usklajenim pristopom, vključno z delegiranimi akti.

### 3.3.3 *POGLAVJE III – SKRBNIŠKE STORITVE*

#### 3.3.3.1 Oddelek 1 – Splošne določbe

Člen 9 določa načela v zvezi z odgovornostjo ponudnikov nekvalificiranih in kvalificiranih skrbniških storitev. Temelji na členu 6 Direktive 1999/93/ES in razširja pravico do odškodnine za škodo, ki jo povzroči kateri koli malomarni ponudnik skrbniških storitev zaradi neupoštevanja dobrih praks glede varnosti, kar povzroči kršitev varnosti, ki ima pomemben vpliv na storitev.

Člen 10 opisuje mehanizem za priznavanje in sprejemanje kvalificiranih skrbniških storitev, ki jih zagotavlja ponudnik s sedežem v tretji državi. Temelji na členu 7 Direktive 1999/93/ES, vendar ohranja le edino praktično izvedljivo možnost, ki omogoča tako priznavanje v okviru mednarodnega sporazuma med Evropsko unijo in tretjimi državami ali mednarodnimi organizacijami.

Člen 11 določa načelo varstva podatkov in načelo zmanjšane količine podatkov. Temelji na členu 8 Direktive 1999/93/ES.

Člen 12 omogoča dostopnost skrbniških storitev invalidnim osebam.

#### 3.3.3.2 Oddelek 2 – Nadzor

Člen 13 države članice zavezuje k ustanovitvi nadzornih organov na podlagi člena 3(3) Direktive 1999/93/ES ter pojasnjuje in razširja njihovo pristojnost v zvezi s ponudniki skrbniških storitev in ponudniki kvalificiranih skrbniških storitev.

Člen 14 uvaja izrecni mehanizem medsebojne pomoči med nadzornimi organi v državah članicah za lažji čezmejni nadzor ponudnikov skrbniških storitev. Uvaja pravila o skupnem delovanju in pravici nadzornih organov do udeležbe pri takem delovanju.

Člen 15 uvaja obveznost za ponudnike kvalificiranih in nekvalificiranih skrbniških storitev, da izvedejo ustrezne tehnične in organizacijske ukrepe za varnost svojih dejavnosti. Poleg tega morajo biti pristojni nadzorni organi in drugi zadevni organi obveščeni o vseh kršitvah varnosti. Če je primerno, ti nadzorni organi obvestijo nadzorne organe drugih držav članic in, neposredno ali preko zadevnega ponudnika skrbniških storitev, obvestijo tudi javnost.

Člen 16 določa pogoje za nadzor ponudnikov kvalificiranih skrbniških storitev in kvalificiranih skrbniških storitev, ki jih zagotavljajo. Določa, da mora ponudnike kvalificiranih skrbniških storitev vsako leto revidirati priznan neodvisni organ, ki nato nadzornemu organu potrdi, da ponudniki izpolnjujejo obveznosti iz te uredbe. Poleg tega člen 16(2) daje nadzornemu organu pravico, da pri ponudniku kvalificiranih skrbniških storitev kadar koli opravi revizijo na kraju samem. Nadzorni organ je pooblaščen tudi za izdajo zavezujočih navodil ponudnikom kvalificiranih skrbniških storitev za odpravo neizpolnjevanja obveznosti, ki jih je pokazala varnostna revizija, in sicer na sorazmeren način.

Člen 17 se nanaša na dejavnost, ki jo izvede nadzorni organ na zahtevo ponudnika skrbniških storitev, ki želi začeti s kvalificirano skrbniško storitvijo.

Člen 18 določa pripravo seznamov ponudnikov skrbniških storitev<sup>10</sup>, ki vsebujejo informacije o ponudnikih kvalificiranih skrbniških storitev, ki so predmet nadzora, in o storitvah, ki jih zagotavljajo. Te informacije morajo biti javno dostopne s pomočjo skupnega modela, da se spodbudi njihova samodejna uporaba in zagotovi ustrezna raven podrobnosti.

Člen 19 določa zahteve, ki jih morajo izpolnjevati ponudniki kvalificiranih skrbniških storitev, da bi bili priznani kot taki. Temelji na Prilogi II k Direktivi 1999/93/ES.

### 3.3.3.3 Oddelek 3 – Elektronski podpis

Člen 20 vsebuje pravila v zvezi s pravnim učinkom elektronskih podpisov fizičnih oseb. Pojasnjuje in razširja člen 5 Direktive 1999/93/ES, ki uvaja izrecno obveznost, da imajo kvalificirani elektronski podpisi enak pravni učinek kot lastnoročni podpisi. Poleg tega morajo države članice v okviru opravljanja javnih storitev zagotoviti čezmejno sprejemanje kvalificiranih elektronskih podpisov, ne smejo pa uvesti dodatnih zahtev, ki bi lahko povzročile ovire za uporabo takih podpisov.

Člen 21 določa zahteve za certifikate za kvalificirane certifikate. Pojasnjuje Prilogo I k Direktivi 1999/93/ES in odpravlja določbe, ki niso delovale v praksi (npr. omejitve na vrednost transakcij).

Člen 22 določa zahteve za naprave za ustvarjanje kvalificiranega elektronskega podpisa. Pojasnjuje zahteve za naprave za varno ustvarjanje podpisa iz člena 3(5) Direktive 1999/93/ES, ki jih je zdaj v okviru te uredbe treba obravnavati kot naprave za ustvarjanje kvalificiranega elektronskega podpisa. Prav tako jasno navaja, da je lahko naprava za ustvarjanje podpisa veliko več kot le nekaj, kar vsebuje podatke za ustvarjanje podpisa.

<sup>10</sup> Zanesljivi seznam, uveden z Odločbo Komisije 2009/767/ES, kakor je bila spremenjena s Sklepom Komisije 2010/425/EU, so podlaga za novi sklep Komisije o seznamih kvalificiranega statusa v skladu s to uredbo.

Komisija lahko pripravi tudi seznam referenčnih števil standardov za varnostne zahteve za naprave.

Člen 23, ki temelji na členu 3(4) Direktive 1999/93/ES, uvaja pojem certificiranja naprav za ustvarjanje kvalificiranega elektronskega podpisa za ugotavljanje njihove skladnosti z varnostnimi zahtevami iz Priloge II. Če postopek certificiranja izvede overitelj, ki ga imenuje država članica, morajo vse države članice priznati skladnost teh naprav z zahtevami. Komisija objavi pozitivni seznam takih certificiranih naprav v skladu s členom 24. Komisija lahko pripravi tudi seznam referenčnih števil standardov za ocenjevanje varnosti izdelkov informacijske tehnologije iz člena 23(1).

Člen 24 se nanaša na objavo seznama naprav za ustvarjanje kvalificiranega elektronskega podpisa, ki ga Komisija objavi po tem, ko jo države članice obvestijo o skladnosti.

Člen 25 temelji na priporočilih iz Priloge IV k Direktivi 1999/93/ES in predpisuje zavezujoče zahteve za potrjevanje kvalificiranih elektronskih podpisov, da se poveča pravna varnost takega potrjevanja.

Člen 26 določa pogoje za kvalificirane storitve potrjevanja.

Člen 27 določa pogoj za dolgoročno hrambo kvalificiranih elektronskih podpisov. To je mogoče zaradi uporabe postopkov in tehnologij, ki lahko podaljšajo zanesljivost podatkov za potrjevanje kvalificiranega elektronskega podpisa preko datuma njihove tehnološke veljavnosti, kadar obstaja nevarnost ponarejanja s strani kibernetičnih kriminalcev.

#### 3.3.3.4 Oddelek 4 – Elektronski žigi

Člen 28 se nanaša na pravni učinek elektronskih žigov pravnih oseb. Za kvalificirani elektronski žig velja posebna pravna domneva, ki zagotavlja izvor in celovitost elektronskih dokumentov, s katerimi je žig povezan.

Člen 29 določa zahteve za kvalificirane certifikate za elektronske žige.

Člen 30 določa zahteve za seznam naprav za ustvarjanje kvalificiranega elektronskega žiga ter certificiranje in objavo tega seznama.

Člen 31 določa pogoj za potrjevanje in hrambo kvalificiranih elektronskih žigov.

#### 3.3.3.5 Oddelek 5 – Elektronski časovni žig

Člen 32 se nanaša na pravni učinek elektronskih časovnih žigov. Za kvalificirane elektronske časovne žige velja posebna pravna domneva v zvezi z zanesljivostjo časa.

Člen 33 določa zahteve za kvalificirane elektronske časovne žige.

#### 3.3.3.6 Oddelek 6 – Elektronski dokumenti

Člen 34 se nanaša na pravne učinke in pogoje za sprejetje elektronskih dokumentov. Za elektronske dokumente, podpisane s kvalificiranim elektronskim podpisom ali ožigosane s kvalificiranim elektronskim žigom, velja posebna pravna domneva v zvezi z njihovo avtentičnostjo in celovitostjo. Kar zadeva sprejemanje elektronskih dokumentov, kadar se za zagotavljanje javne storitve zahteva izvirnik ali overjena kopija, druge države članice brez



dodatnih zahtev sprejmejo vsaj elektronske dokumente, ki jih izdajo osebe, pristojne za izdajanje zadevnih dokumentov, in ki se štejejo za izvornike ali overjene kopije v skladu z nacionalno zakonodajo izvorne države članice.

#### 3.3.3.7 Oddelek 7 – Storitve elektronske dostave

Člen 35 se nanaša na pravni učinek podatkov, ki se pošljejo ali prejmejo s pomočjo storitve elektronske dostave. Za celovitost podatkov, ki se pošljejo ali prejmejo, in za točnost časa, ko so bili podatki poslani ali prejeti, velja posebna pravna domneva v zvezi s kvalificiranimi storitvami elektronske dostave. Zagotavlja tudi medsebojno priznavanje kvalificiranih storitev elektronske dostave.

Člen 36 določa zahteve za kvalificirane storitve elektronske dostave.

#### 3.3.3.8 Oddelek 8 – Avtentikacija spletnih strani

Ta oddelek je namenjen zagotavljanju avtentičnosti spletne strani v zvezi z lastnikom spletne strani.

Člen 37 določa zahteve za kvalificirane certifikate za avtentikacijo spletnih strani, s katerimi se zagotavlja avtentičnost spletnih strani. Kvalificirani certifikat za avtentikacijo spletne strani zagotavlja minimalne zanesljive informacije o spletni strani in o pravem obstoju njenega lastnika.

#### 3.3.4 *POGLAVJE IV – DELEGIRANI AKTI*

Člen 38 vsebuje standardne določbe za izvajanje prenosov pooblastil v skladu s členom 290 PDEU (delegirani akti). Ta člen omogoča zakonodajnemu organu, da na Komisijo prenese pooblastilo za sprejemanje nezakonodajnih aktov, ki se splošno uporabljajo in dopolnjujejo ali spreminjajo nekatere nebistvene elemente zakonodajnega akta.

#### 3.3.5 *POGLAVJE V – IZVEDBENI AKTI*

Člen 39 vsebuje določbo o postopku v odboru, ki je potreben za prenos izvedbenih pooblastil na Komisijo, kadar so v skladu s členom 291 PDEU potrebni enotni pogoji za izvajanje pravno zavezujočih aktov Unije. Uporablja se postopek pregleda.

#### 3.3.6 *POGLAVJE VI – KONČNE DOLOČBE*

Člen 40 Komisijo zavezuje k oceni Uredbe in poročanju o ugotovitvah.

Člen 41 razveljavlja Direktivo 1999/93/ES in zagotavlja nemoten prehod z obstoječe zakonodaje o elektronskem podpisu na nove zahteve Uredbe.

Člen 42 določa dan začetka veljavnosti Uredbe.

## 4. **VPLIV NA PRORAČUN**

Konkreten vpliv predloga na proračun je povezan z nalogami, dodeljenimi Evropski komisiji, kot je navedeno v oceni finančnih posledic, ki je priložena temu predlogu.

Predlog nima posledic za odhodke iz poslovanja.

Ocena finančnih posledic, ki je priložena temu predlogu Uredbe, obsega proračunske posledice Uredbe same.

Predlog

**UREDBA EVROPSKEGA PARLAMENTA IN SVETA**

**o elektronski identifikaciji in skrbniških storitvah za elektronske transakcije na notranjem trgu**

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora<sup>11</sup>,

po posvetovanju z evropskim nadzornikom za varstvo podatkov<sup>12</sup>,

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

- (1) Ustvarjanje zaupanja v spletno okolje je ključ do gospodarskega razvoja. Zaradi pomanjkanje zaupanja potrošniki, podjetja in uprave oklevajo pri izvajanju elektronskih transakcij in pri sprejemanje novih storitev.
- (2) Namen te uredbe je okrepiti zaupanje v elektronske transakcije na notranjem trgu tako, da se zagotovijo varne in nemotene elektronske interakcije med podjetji, državljani in javnimi organi, s čimer bi se povečala učinkovitost javnih in zasebnih spletnih storitev, elektronskega poslovanja in elektronskega trgovanja v EU.
- (3) Direktiva Evropskega parlamenta in Sveta št. 1999/93/EC z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis<sup>13</sup> je večinoma zajela elektronske podpise, ni pa zagotovila celovitega čezmejnega in medsektorskega okvira za varne in zanesljive elektronske transakcije, ki bi bile enostavne za uporabo. Ta uredba krepi in razširja področje uporabe Direktive.

---

<sup>11</sup> UL C, , str..

<sup>12</sup> UL C, , str..

<sup>13</sup> UL L 13, 19.01.2000, str. 12.

- (4) Evropska digitalna agenda Komisije<sup>14</sup> je razdrobljenost digitalnega trga, pomanjkanje interoperabilnosti in naraščanje kibernetnega kriminala opredelila kot velike ovire za uspešen krog digitalnega gospodarstva. V Poročilu o državljanstvu iz leta 2010 je dodatno izpostavila, da je treba odpraviti glavne težave, ki evropskim državljanom preprečujejo, da bi imeli koristi, ki jih nudijo enotni digitalni trg in čezmejne digitalne storitve<sup>15</sup>.
- (5) Evropski svet je Komisijo pozval, naj do leta 2015 vzpostavi enotni digitalni trg<sup>16</sup> da bi hitro napredovala na ključnih področjih digitalnega gospodarstva in s spodbujanjem čezmejne uporabe spletnih storitev, zlasti pospeševanja varne elektronske identifikacije in avtentikacije, spodbudila popolnoma enotni digitalni trg<sup>17</sup>.
- (6) Svet je Komisijo pozval, naj prispeva k enotnemu digitalnemu trgu tako, da oblikuje ustrezne pogoje za medsebojno priznavanje ključnih čezmejnih dejavnikov, kot so elektronska identifikacija, elektronski dokumenti, elektronski podpisi in storitve elektronske dostave, ter za interoperabilne storitve e-uprave v Evropski uniji<sup>18</sup>.
- (7) Evropski parlament je poudaril pomen varnosti elektronskih storitev, zlasti elektronskih podpisov, ter potrebo po vzpostavitvi infrastrukture javnih ključev na vseevropski ravni, ter pozval Komisijo, naj vzpostavi evropski portal za organe potrjevanja, da se zagotovi čezmejna interoperabilnost elektronskih podpisov in izboljša varnost transakcij prek interneta<sup>19</sup>.
- (8) V skladu z Direktivo 2006/123/ES Evropskega parlamenta in Sveta z dne 12. decembra 2006 o storitvah na notranjem trgu<sup>20</sup> morajo države članice ustanoviti „enotne kontaktne točke“, s katerimi zagotovijo, da se vsi postopki in formalnosti v zvezi z začetkom opravljanja in opravljanjem storitvene dejavnosti s pomočjo ustrezne enotne kontaktne točke in pri ustreznih pristojnih organih lahko enostavno zaključijo na daljavo ali elektronsko. Številne spletne storitve, dostopne prek enotnih kontaktnih točk, zahtevajo elektronsko identifikacijo, avtentikacijo in podpis.
- (9) V večini primerov ponudniki storitev iz druge države članice ne morejo uporabljati elektronske identifikacije za dostop do teh storitev, ker nacionalne sheme elektronske identifikacije niso priznane in sprejete v drugih državah članicah. Ta elektronska ovira ponudnikom storitev preprečuje, da bi v celoti izkoristili ugodnosti notranjega trga. Vzajemno priznana in sprejeta sredstva elektronske identifikacije bodo poenostavila čezmejno zagotavljanje številnih storitev na notranjem trgu in podjetjem omogočila čezmejno poslovanje brez ovir in interakcije z javnimi organi.

<sup>14</sup> COM(2010) 245 final/2.

<sup>15</sup> Poročilo o državljanstvu EU iz leta 2010: Odpravljanje ovir za pravice državljanov EU, COM(2010) 603 final, točka 2.2.2, stran 13.

<sup>16</sup> 4/2/2011: EUCO 2/1/11.

<sup>17</sup> 23/10/2011: EUCO 52/1/11.

<sup>18</sup> Sklepi Sveta o Evropskem akcijskem načrtu za e-upravo za obdobje 2011–2015, 3093. zasedanje Sveta za promet, telekomunikacije in energijo, Bruselj, 27. maja 2011.

<sup>19</sup> Resolucija Evropskega parlamenta z dne 21. septembra 2010 o dokončnem oblikovanju notranjega trga za e-poslovanje, 21.9.10, P7\_TA (2010)0320, in Resolucija Evropskega parlamenta z dne 15. junija 2010 o upravljanju interneta: naslednji koraki, P7\_TA (2010)0208.

<sup>20</sup> UL L 376, 27.12.2006, str. 36.

- (10) Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu<sup>21</sup> vzpostavlja mrežo nacionalnih organov, pristojnih za e-zdravje. Za izboljšanje varnosti in neprekinjenosti čezmejne oskrbe pacientov naj bi mreža pripravila smernice za čezmejni dostop do elektronskih zdravstvenih podatkov in storitev ter podprla *skupne ukrepe za identifikacijo in ugotavljanje avtentičnosti, s katerimi naj bi se olajšala prenosljivost podatkov v čezmejnem zdravstvenem varstvu*. Vzajemno priznavanje in sprejemanje elektronske identifikacije in avtentikacije je ključna pri uresničevanju čezmejnega zdravstvenega varstva evropskih državljanov. Kadar ljudje potujejo zaradi zdravljenja, morajo biti njihovi zdravstveni podatki dostopni v državi zdravljenja. To zahteva trden, varen in zanesljiv okvir za elektronsko identifikacijo.
- (11) Eden od ciljev te uredbe je odpraviti obstoječe ovire za čezmejno uporabo sredstev elektronske identifikacije, ki v državah članicah zagotavljajo dostop vsaj do javnih storitev. Ta uredba ni namenjena poseganju v elektronske sisteme za upravljanje identitete in z njimi povezane infrastrukture, vzpostavljene v državah članicah. Ta uredba naj bi zagotovila, da je za dostop do čezmejnih spletnih storitev, ki jih zagotavljajo države članice, mogoča varna elektronska identifikacija in avtentikacija.
- (12) Države članice bi morale imeti možnost, da še naprej prosto uporabljajo ali uvajajo sredstva za dostop do spletnih storitev za namene elektronske identifikacije. Prav tako bi morale imeti možnost, da se same odločijo, ali bodo v zagotavljanje teh sredstev vključile zasebni sektor. Države članice ne bi smele biti zavezane k priglasitvi shem elektronske identifikacije. Države članice bi se morale same odločiti, ali bodo priglasile vse sheme elektronske identifikacije, ki jih uporabljajo za dostop vsaj do javnih spletnih storitev ali posebnih storitev na nacionalni ravni, samo nekatere sheme ali nobene.
- (13) Uredba bi morala določiti nekaj pogojev v zvezi s tem, katera sredstva elektronske identifikacije bi bilo treba sprejeti in kako se sheme priglasijo. To bi državam članicam moralo pomagati lažje okrepiti potrebno zaupanje v sheme elektronske identifikacije drugih držav članic ter olajšati medsebojno priznavanje in sprejemanje sredstev elektronske identifikacije, ki spadajo v priglašene sheme. Načelo medsebojnega priznavanja in sprejemanja bi se moralo uporabljati, če država članica priglasiteljica izpolnjuje pogoje priglasitve, priglasitev pa je bila objavljena v *Uradnem listu Evropske unije*. Vendar pa bi morala biti dostop do teh spletnih storitev in njihova končna dostava prosilcu tesno povezana s pravico do prejema take storitve pod pogoji, ki jih določa nacionalna zakonodaja.
- (14) Države članice bi se morale same odločiti, ali bo pri izdaji sredstev elektronske identifikacije sodeloval zasebni sektor in ali mu bodo dovolile uporabljati sredstva elektronske identifikacije v okviru priglašene sheme za namene identifikacije, kadar je to potrebno za spletne storitve ali elektronske transakcije. Možnost uporabe takih sredstev elektronske identifikacije bi zasebnemu sektorju omogočila uporabo elektronske identifikacije in avtentikacije, ki se v veliko državah članicah že uporabljata vsaj za javne storitve, podjetja, državljanji pa bi tako imeli lažji dostop do čezmejnih spletnih storitev. Da se olajša čezmejna uporaba takih sredstev elektronske identifikacije v zasebnem sektorju, bi morala biti možnost avtentikacije, ki jo nudijo

---

<sup>21</sup> UL L 88, 4.4.2011, str. 45.

države članice, odvisnim stranem na voljo brez razlikovanja med javnim in zasebnim sektorjem.

- (15) Čezmejna uporaba sredstev elektronske identifikacije v okviru priglašene sheme od držav članic zahteva medsebojno sodelovanje pri vzpostavljanju tehnične interoperabilnosti. To izključuje posebne nacionalne tehnične predpise, ki od udeležencev iz drugih držav zahtevajo na primer namestitve posebne strojne ali programske opreme za preverjanje in potrjevanje priglašene elektronske identifikacije. Vendar pa so tehnične zahteve za uporabnika, ki izhajajo iz specifikacij, povezanih z uporabljenim varnostnim žetonom (npr. pametne kartice), neizogibne.
- (16) Sodelovanje držav članic bi moralo zagotoviti tehnično interoperabilnost priglašeni shem elektronske identifikacije ter tako vzpostaviti visoko raven zaupanja in varnosti, primerno stopnji tveganja. Izmenjava informacij in dobrih praks med državami članicami, da se doseže medsebojno priznavanje, bi morala pripomoči k takemu sodelovanju.
- (17) Ta uredba bi morala določiti tudi splošni pravni okvir za uporabo skrbniških elektronskih storitev. Vendar pa ne bi smela uvesti splošne obveznosti za njihovo uporabo. Zlasti ne sme urejati zagotavljanja storitev, ki temeljijo na prostovoljnih zasebnopravnih dogovorih. Prav tako ne bi smela urejati vidikov, povezanih s sklenitvijo in veljavnostjo pogodb ali drugih pravnih obveznosti, če nacionalna zakonodaja ali zakonodaja Unije predpisuje zahteve v zvezi s predpisano obliko.
- (18) Da bi spodbujali splošno čezmejno uporabo skrbniških elektronskih storitev, bi jih bi moralo biti mogoče uporabljati kot dokaz v sodnih postopkih v vseh državah članicah.
- (19) Države članice bi morale še naprej imeti možnost, da svobodno opredelijo druge vrste skrbniških storitev, ki niso del zaprtega seznama ponudnikov skrbniških storitev iz te uredbe, da bi jih lahko priznale kot kvalificirane skrbniške storitve na nacionalni ravni.
- (20) Zaradi hitrih tehnoloških sprememb bi moral biti s to uredbo sprejet pristop, ki je odprt za inovacije.
- (21) Ta uredba bi morala biti tehnološko nevtralna. Pravne učinke, ki jih zagotavlja, bi morala doseči s katerimi koli tehnološkimi sredstvi, pod pogojem, da so izpolnjene zahteve te uredbe.
- (22) Da se okrepi zaupanje ljudi v notranji trg ter spodbudi uporaba skrbniških storitev in izdelkov, bi bilo treba uvesti pojma kvalificirane skrbniške storitve in ponudnika kvalificiranih skrbniških storitev ter tako določile zahteve in obveznosti za zagotavljanje visoke varnostne ravni vseh kvalificiranih skrbniških storitev in izdelkov, ki se uporabljajo ali zagotavljajo.
- (23) V skladu z obveznostmi iz Konvencije ZN o pravicah invalidnih oseb, ki je začela veljati v EU, bi morale invalidne osebe možnost, da skrbniške storitve in izdelke za končne uporabnike, ki se uporabljajo pri zagotavljanju teh storitev, uporabljajo enako kot drugi potrošniki.
- (24) Ponudnik skrbniških storitev nadzira osebne podatke in mora zato izpolnjevati obveznosti iz Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku

takih podatkov<sup>22</sup>. Zlasti bi bilo treba ob upoštevanju namena zagotovljene storitve čim bolj zmanjšati zbiranje podatkov.

- (25) Nadzorni organi bi morali sodelovati in izmenjevati podatke z organi za varstvo podatkov, da se zagotovi, da ponudniki storitev ustrezno izvajajo zakonodajo o varstvu podatkov. Izmenjava podatkov bi morala zlasti zajemati varnostne incidente in kršitve varnosti osebnih podatkov.
- (26) Vsi ponudniki skrbniških storitev bi morali uporabljati dobro prakso varnosti, primerno za tveganja, povezana z njihovimi dejavnostmi, da bi tako okrepili zaupanje uporabnikov v enotni trg.
- (27) Določbe o uporabi psevdonimov v certifikatih ne bi smele ovirati držav članic, da zahtevajo identifikacijo oseb v skladu z zakonodajo Unije ali nacionalno zakonodajo.
- (28) Vse države članice bi morale upoštevati skupne bistvene zahteve po nadzoru, da se zagotovi primerljiva varnostna raven kvalificiranih skrbniških storitev. Za lažjo dosledno uporabo teh zahtev po vsej EU bi morale države članice sprejeti primerljive postopke ter si izmenjevati informacije o nadzornih dejavnosti in dobrih praksah na tem področju.
- (29) Prijave kršitev varnosti in ocene varnostnega tveganja so bistvene, da se lahko ob kršitvi varnosti ali izgubi celovitosti zadevnim zagotovijo ustrezne informacije.
- (30) Da bi Komisija in države članice lahko ocenile učinkovitost mehanizma za prijavo kršitev, ki ga uvaja ta uredba, bi morali nadzorni organi Komisiji ter Evropski agenciji za varnost omrežij in informacij (ENISA) zagotoviti povzetek informacij.
- (31) Da bi Komisija in države članice lahko ocenile učinek te uredbe, bi morali biti nadzorni organi obvezani, da zagotovijo statistične podatke o kvalificiranih skrbniških storitvah in njihovi uporabi.
- (32) Da bi Komisija in države članice lahko ocenile učinkovitost mehanizma okrepljenega nadzora, ki ga uvaja ta uredba, bi morali nadzorni organi poročati o svojih dejavnostih. To bi bistveno pripomoglo k boljši izmenjavi dobrih praks med nadzornimi organi ter hkrati zagotovilo, da se bistvene zahteve po nadzoru izvajajo dosledno in učinkovito v vseh državah članicah.
- (33) Da se zagotovita vzdržnost in trajnost kvalificiranih skrbniških storitev ter okrepi zaupanje uporabnikov v neprekinjenost kvalificiranih skrbniških storitev, bi morali nadzorni organi zagotoviti, da se podatki ponudnikov kvalificiranih skrbniških storitev hranijo in da so dostopni ustrezno časovno obdobje, tudi če ponudnik kvalificiranih skrbniških storitev svojih dejavnosti ne opravlja več.
- (34) Da se olajša nadzor ponudnikov kvalificiranih skrbniških storitev, na primer kadar ponudnik storitve zagotavlja na ozemlju druge države članice in tam ni predmet nadzora ali kadar se računalniki ponudnika nahajajo na ozemlju druge države članice in ne v državi, v kateri ima ponudnik sedež, bi bilo treba vzpostaviti sistem medsebojne pomoči med nadzornimi organi v državah članicah.

---

<sup>22</sup> UL L 281, 23.11.1995, str. 31.

- (35) Ponudniki skrbniških storitev so pri zagotavljanju skrbniških storitev, zlasti kvalificiranih skrbniških storitev, odgovorni za izpolnjevanje zahtev iz te uredbe. Nadzorni organi so odgovorni za nadzor nad tem, kako ponudniki skrbniških storitev izpolnjujejo te zahteve.
- (36) Da bi se postopek vključitve kvalificiranih skrbniških storitev in kvalificiranih skrbniških storitev, ki jih ti zagotavljajo, na sezname ponudnikov skrbniških storitev začel učinkovito, je treba spodbujati predhodno interakcijo med bodočimi ponudniki kvalificiranih skrbniških storitev in pristojnimi nadzornimi organi, da se pospeši skrbni pregled, ki bo vodil do zagotavljanja kvalificiranih skrbniških storitev.
- (37) Sezname ponudnikov skrbniških storitev so bistveni elementi za krepitev zaupanja med akterji na trgu, saj navajajo kvalificirani status ponudnika storitev v trenutku nadzora, vendar pa ti sezname niso predpogoj za doseganje kvalificiranega statusa in zagotavljanje kvalificiranih skrbniških storitev, ki se zagotovita z izpolnjevanjem zahtev iz te uredbe.
- (38) Prilgašene skrbniške storitve zadevni organ javnega sektorja med upravnim postopkom ali izpolnjevanju formalnosti ne sme zavrniti z utemeljitvijo, da ni vključena na sezname ponudnikov skrbniških storitev, ki jih vzpostavijo države članice. V ta namen je organ javnega sektorja vsak javni organ ali drug subjekt, ki je pooblaščen za zagotavljanje storitev e-uprave, kot so davčna napoved po spletu, izpis rojstnega lista, udeležba v elektronskih postopkih javnih naročil itd.
- (39) Čeprav je za zagotavljanje medsebojnega priznavanja elektronskih podpisov potrebna visoka varnostna raven, bi bilo treba v posebnih primerih, kot na primer v okviru Odločbe Komisije 2009/767/ES z dne 16. oktobra 2009 o vzpostavitvi ukrepov za pospeševanje uporabe postopkov po elektronski poti s pomočjo „enotnih kontaktnih točk“ po Direktivi 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu<sup>23</sup>, sprejeti tudi elektronske podpise z nižjo varnostno ravno.
- (40) Podpisnik bi moral imeti možnost, da naprave za ustvarjanje kvalificiranega elektronskega podpisa zaupa v oskrbo tretji osebi, pod pogojem, da se uvedejo ustrezni mehanizmi in postopki, ki zagotavljajo, da ima podpisnik izključni nadzor nad uporabo svojih podatkov za ustvarjanje elektronskega podpisa in da so pri uporabi naprave izpolnjene zahteve za kvalificirani podpis.
- (41) Da se zagotovi pravna varnost glede veljavnosti podpisa, je zelo pomembno, da se določi, katere dele kvalificiranega elektronskega podpisa mora odvisna oseba, ki izvaja potrjevanje, oceniti. Poleg tega bi opredelitev zahtev za ponudnike kvalificiranih skrbniških storitev, ki lahko zagotavljajo kvalificirano storitev potrjevanja za odvisne strani, ki potrjevanja kvalificiranih elektronskih podpisov ne želijo ali ne morejo opraviti same, morala zasebni ali javni sektor spodbuditi k naložbam v take storitve. Oba elementa bi morala zagotoviti enostavno potrjevanje kvalificiranega elektronskega podpisa, ki bi bilo primerno za vse stranke na ravni Unije.
- (42) Če transakcija zahteva kvalificirani elektronski žig pravne osebe, bi moral biti enako sprejemljiv tudi kvalificirani elektronski podpis pooblaščenega zastopnika pravne osebe.

---

<sup>23</sup> UL L 274, 20.10.2009, str. 36.



- (43) Elektronski žigi bi morali služiti kot dokaz, da je elektronski dokument izdala pravna oseba, ter zagotavljati zanesljivost izvora in celovitosti dokumenta.
- (44) Ta uredba bi morala zagotoviti dolgoročno hrambo informacij, tj. pravno veljavnost elektronskega podpisa in elektronskih žigov v daljšem časovnem obdobju, in hkrati zagotavljati, da se jih lahko potrdi ne glede na prihodnje tehnološke spremembe.
- (45) Da se izboljša čezmejna uporaba elektronskih dokumentov, bi morala ta uredba pravni učinek elektronskih dokumentov urejati tako, da bi bili ti odvisno od ocene tveganja ter pod pogojem, da sta zagotovljeni avtentičnost in celovitost dokumentov, obravnavani kot enakovredni dokumenti v papirni obliki. Za nadaljnji razvoj čezmejnih elektronskih transakcij na notranjem trgu je tudi zelo pomembno, da se izvirniki elektronskih dokumentov ali overjene kopije, ki jih izdajo zadevni pristojni organi v državi članici v skladu z nacionalno zakonodajo, sprejemajo kot taki tudi v drugih državah članicah. Ta uredba ne sme posegati v pravico držav članic, da določijo, kaj je na nacionalni ravni izvirnik in kaj kopija, temveč bi morala zagotoviti, da se lahko kot taka uporabljata tudi v drugih državah.
- (46) Ker pristojni organi v državah članicah trenutno uporabljajo različne oblike naprednih elektronskih podpisov za podpisovanje dokumentov v elektronski obliki, bi bilo treba zagotoviti, da lahko države članice, ko prejmejo elektronsko podpisane dokumente, tehnično podprejo vsaj nekaj oblik naprednih elektronskih podpisov. Podobno bi bilo treba v primeru, ko pristojni organi v državah članicah uporabljajo napredne elektronske žige, zagotoviti, da ti podpirajo vsaj nekaj oblik naprednih elektronskih žigov.
- (47) Poleg pri potrjevanju avtentičnosti dokumenta, ki ga izda pravna oseba, je elektronske žige mogoče uporabljati tudi pri potrjevanju avtentičnosti katerih koli digitalnih sredstev pravne osebe, npr. programskih kod in strežnikov.
- (48) Če bo mogoče potrjevati avtentičnost spletnih strani in lastnikov spletnih strani, bo spletne strani težje ponarejati, kar bo zmanjšalo goljufije.
- (49) Da se določeni podrobni tehnični vidiki te uredbe dopolnijo prilagodljivo in hitro, bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 Pogodbe o delovanju Evropske unije sprejema akte; o interoperabilnosti elektronske identifikacije, varnostnih ukrepih, ki se zahtevajo od ponudnikov srčbniških storitev, priznanih neodvisnih organih, ki so pristojni za revizijo ponudnikov storitev; seznamih ponudnikov skrbniških storitev; zahtevah v zvezi z varnostnimi ravnmi elektronskih podpisov; zahtevah kvalificiranih certifikatov za elektronske podpise ter njihovim potrjevanjem in hrambo; organi, pristojnimi za certificiranje naprav za ustvarjanje kvalificiranega elektronskega podpisa; zahtevah v zvezi z varnostnimi ravnmi elektronskih žigov in kvalificiranimi certifikati za elektronske žige; ter o interoperabilnosti med storitvami dostave. Zlasti je pomembno, da Komisija pri pripravljalnem delu opravi ustrezna posvetovanja, med drugim tudi na strokovni ravni.
- (50) Komisija bi morala pri pripravi in oblikovanju delegiranih aktov zagotoviti, da istočasno, pravočasno in na ustrezen način Evropskemu parlamentu in Svetu predloži ustrezne dokumente.
- (51) Da se zagotovijo enotni pogoji za izvajanje te uredbe, bi bilo treba na Komisijo prenesti izvedbena pooblastila, zlasti za določitev referenčnih števil standardov,

katerih uporaba bi zagotovila predpostavljane skladnosti z določenimi zahtevami iz te uredbe ali zahtevami iz delegiranih aktov. Ta pooblastila bi se morala izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije<sup>24</sup>.

- (52) Zaradi pravne varnosti in jasnosti bi bilo treba Direktivo 1999/93/ES razveljaviti.
- (53) Da se tržnim udeležencem, ki že uporabljajo kvalificirane certifikate, izdane v skladu z Direktivo 1999/93/ES, zagotovi pravna varnost, je treba za prehod zagotoviti dovolj dolgo prehodno obdobje. Prav tako je treba Komisiji zagotoviti sredstva za sprejemanje izvedbenih in delegiranih aktov še pred tem datumom.
- (54) Ker države članice ciljev te uredbe ne morejo doseči zadovoljivo in ker se zaradi obsega ali učinkov ukrepov lažje dosežejo na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega okvirov, potrebnih za doseganje navedenega cilja, zlasti v zvezi z vlogo Komisije kot koordinatorja nacionalnih dejavnosti –

SPREJELA NASLEDNJO UREDBO:

## **POGLAVJE I**

### **SPLOŠNE DOLOČBE**

#### *Člen 1*

##### **Predmet**

1. Ta uredba določa pravila za elektronsko identifikacijo in elektronske skrbniške storitve za elektronske transakcije, da se zagotovi pravilno delovanje notranjega trga.
2. Ta uredba določa pogoje, pod katerimi države članice priznajo in sprejmejo sredstva elektronske identifikacije fizičnih in pravnih oseb, ki spadajo v priglašeno shemo elektronske identifikacije druge države članice.
3. Ta uredba določa pravni okvir za elektronske podpise, elektronske žige, elektronske časovne žige, elektronske dokumente, storitve elektronske dostave in avtentikacijo spletnih strani.
4. Ta uredba zagotavlja prosti pretok skrbniških storitev in izdelkov, ki so v skladu s to uredbo, na notranjem trgu.

#### *Člen 2*

##### **Področje uporabe**

---

<sup>24</sup> UL L 55, 28.2.2011, str. 13.

1. Ta uredba se uporablja za elektronsko identifikacijo, ki jo zagotovijo države članice oziroma se zagotavlja v njihovem imenu ali pod njihovo pristojnostjo, in za ponudnike skrbniških storitev s sedežem v Uniji.

2. Ta uredba se ne uporablja za skrbniške elektronske storitve, ki se zagotavljajo na podlagi prostovoljnih zasebnopravnih dogovorov.

3. Ta uredba se ne uporablja za vidike, povezane s sklenitvijo in veljavnostjo pogodb ali drugimi pravnimi obveznostmi, če nacionalno pravo ali pravo Unije predpisuje zahteve za obliko.

### *Člen 3*

#### **Opredelitve**

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „elektronska identifikacija“ pomeni postopek uporabe identifikacijskih osebnih podatkov, ki v elektronski obliki nedvoumno predstavljajo fizično ali pravno osebo;

(2) „elektronsko identifikacijsko sredstvo“ je materialna ali nematerialna enota, ki vsebuje podatke iz točke 1 tega člena in ki se uporablja za dostop do spletnih storitev iz člena 5;

(3) „elektronska identifikacijska shema“ je sistem za elektronsko identifikacijo, v okviru katerega se osebam iz točke 1 tega člena izdajajo elektronska identifikacija sredstva;

(4) „avtentikacija“ pomeni elektronski postopek, ki omogoča potrjevanje elektronske identifikacije fizične ali pravne osebe oziroma izvora in celovitosti elektronskih podatkov;

(5) „podpisnik“ pomeni fizično osebo, ki ustvari elektronski podpis;

(6) „elektronski podpis“ pomeni podatke v elektronski obliki, ki so dodani drugim elektronskim podatkom oziroma z njimi logično povezani in ki ga podpisnik uporablja za podpisovanje;

(7) „napreden elektronski podpis“ je elektronski podpis, ki izpolnjuje naslednje zahteve:

(a) je povezan izključno s podpisnikom;

(b) je z njegovo pomočjo mogoče identificirati podpisnika;

(c) je ustvarjen s pomočjo podatkov za ustvarjanje elektronskega podpisa, ki jih lahko podpisnik uporablja z visoko ravno zaupanja izključno pod svojim nadzorom; in

(d) je s podatki, na katere se nanaša, povezan tako, da je opazna vsaka naknadna sprememba teh podatkov;

(8) „kvalificirani elektronski podpis“ pomeni napreden elektronski podpis, ki ga ustvari naprava za ustvarjanje kvalificiranega elektronskega podpisa in ki temelji na kvalificiranem certifikatu za elektronske podpise;

(9) „podatki za ustvarjanje elektronskega podpisa“ pomenijo enoznačne podatke, ki jih podpisnik uporablja za ustvarjanje elektronskega podpisa;

- (10) „certifikat“ je elektronsko potrdilo, ki podatke za potrjevanje elektronskega podpisa oziroma žiga fizične oziroma pravne osebe povezuje s certifikatom ter potrjuje podatke te osebe;
- (11) „kvalificirani certifikat za elektronski podpis“ pomeni potrdilo, ki podpira elektronske podpise, ga izda ponudnik kvalificiranih skrbniških storitev in ki izpolnjuje zahteve iz Priloge I;
- (12) „skrbniška storitev“ pomeni elektronsko storitev, ki vključuje ustvarjanje, preverjanje, potrjevanje elektronskih podpisov, ravnanje z njimi in njihovo hrambo, elektronskih žigov, elektronskih časovnih žigov, elektronskih dokumentov, storitev elektronske dostave, avtentikacije spletnih strani in elektronskih certifikatov, vključno s certifikati za elektronski podpis in elektronske žige;
- (13) „kvalificirana skrbniška storitev“ pomeni skrbniško storitev, ki izpolnjuje zadevne zahteve iz te uredbe;
- (14) „ponudnik skrbniških storitev“ pomeni fizično ali pravno osebo, ki zagotavlja eno ali več skrbniških storitev;
- (15) „ponudnik kvalificiranih skrbniških storitev“ pomeni ponudnika skrbniških storitev, ki izpolnjuje zahteve iz te uredbe;
- (16) „izdelek“ pomeni strojno ali programsko opremo ali njene specifične sestavne dele, ki se uporabljajo za zagotavljanje skrbniških storitev;
- (17) „naprava za ustvarjanje elektronskega podpisa“ pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega podpisa;
- (18) „naprava za ustvarjanje kvalificiranega elektronskega podpisa“ pomeni napravo za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II;
- (19) „ustvarjalec žiga“ pomeni pravno osebo, ki ustvari elektronski žig;
- (20) „elektronski žig“ pomeni podatke v elektronski obliki, ki so dodani drugim elektronskim podatkom ali z njimi logično povezani, da se zagotovita izvor in celovitost povezanih podatkov;
- (21) „napreden elektronski žig“ pomeni elektronski žig, ki izpolnjuje naslednje zahteve:
- (a) je povezan izključno z ustvarjalcem žiga;
  - (b) je iz njega mogoče identificirati ustvarjalca žiga;
  - (c) je ustvarjen je s podatki za ustvarjanje elektronskega žiga, ki jih lahko ustvarjalec žiga z visoko ravno zaupanja pod svojim nadzorom uporabi za ustvarjanje elektronskega žiga; in
  - (d) je s podatki, na katere se nanaša, povezan tako, da je opazna vsaka naknadna sprememba teh podatkov;
- (22) „kvalificirani elektronski žig“ pomeni napreden elektronski žig, ki ga ustvari naprava za ustvarjanje kvalificiranega elektronskega žiga in ki temelji na kvalificiranemu certifikatu za elektronski žig;
- (23) „podatki za ustvarjanje elektronskega žiga“ pomenijo enoznačne podatke, ki jih ustvarjalec elektronskega žiga uporablja za ustvarjanje elektronskega žiga;

(24) „kvalificirani certifikat za elektronski žig“ pomeni potrdilo, ki podpira elektronske podpise, ga izda ponudnik kvalificiranih skrbniških storitev in ki izpolnjuje zahteve iz Priloge;

(25) „elektronski časovni žig“ pomeni podatke v elektronski obliki, ki druge elektronske podatke povezujejo z določenim časom in tako zagotavljajo dokaze, da so ti podatki ob tem času obstajali;

(26) „kvalificirani elektronski časovni žig“ pomeni elektronski časovni žig, ki izpolnjuje zahteve iz člena 33;

(27) „elektronski dokument“ pomeni dokument v kateri koli elektronski obliki;

(28) „storitev elektronske dostave“ pomeni storitev, ki omogoča prenos podatkov z elektronskimi sredstvi, zagotavlja dokaze o ravnanju s prenesenimi podatki, vključno z dokazilom o pošiljanju ali prejemanju podatkov, ter prenesene podatke varuje pred izgubo, krajo, poškodbo ali kakršni koli nepooblaščen spremembo;

(29) „kvalificirana storitev elektronske dostave“ pomeni storitev elektronske dostave, ki izpolnjuje zahteve iz člena 36;

(30) „kvalificirani certifikat za avtentikacijo spletnih strani“ pomeni potrdilo, ki omogoča avtentikacijo spletne strani in ki spletno stran povezuje z osebo, za katero se izda certifikat, izda ga ponudnik kvalificiranih skrbniških storitev in izpolnjuje zahteve iz Priloge IV;

(31) „podatki za potrjevanje“ pomenijo podatke, ki se uporabljajo za potrjevanje elektronskega podpisa ali elektronskega žiga.

#### *Člen 4*

### **Načelo notranjega trga**

1. Za zagotavljanje skrbniških storitev, ki jih na ozemlju države članice zagotavlja ponudnik skrbniških storitev s sedežem v drugi državi članici, iz razlogov, ki spadajo v področje uporabe te uredbe, ni omejitev.

2. Za izdelke, ki so v skladu s to uredbo, se zagotavlja prosti pretok na notranjem trgu.

## **POGLAVJE II**

### **ELEKTRONSKA IDENTIFIKACIJA**

#### *Člen 5*

### **Medsebojno priznavanje in sprejemanje**

Če nacionalna zakonodaja ali upravna praksa za dostop do spletnih storitev predpisujeta elektronsko identifikacijo z uporabo sredstev elektronske identifikacije in avtentikacijo, se za namene dostopa do te storitve priznajo in sprejmejo vsa elektronska identifikacijska sredstva, ki so bila izdana v drugi državi članici in za katere velja sistem, ki je na seznamu, ki ga Komisija objavi v skladu s postopkom iz člena 7.

## Člen 6

### Pogoji za prigrasitev elektronske identifikacijske sheme

1. Elektronske identifikacijske sheme so upravičene do prigrasitve v skladu s členom 7, če so izpolnjeni vsi naslednji pogoji:

- (a) sredstva elektronske identifikacije je izdala država članica prigrasiteljica oziroma so bila izdana v njenem imenu ali v njeni pristojnosti;
- (b) sredstva elektronske identifikacije se lahko uporabljajo za dostop do vsaj javnih storitev, za katere se v državi članici prigrasiteljici zahteva elektronska identifikacija;
- (c) država članica prigrasiteljica zagotovi, da se osebni identifikacijski podatki nedvoumno dodelijo fizični ali pravni osebi iz točke 1 člena 3;
- (d) država članica prigrasiteljica zagotovi možnost avtentikacije prek spleta kadar koli in brezplačno, tako da lahko vsaka odvisna stran potrdi osebne identifikacijske podatke, prejete v elektronski obliki. Države članice za odvisne strani s sedežem zunaj njihovih ozemelj, ki nameravajo opravljati tako avtentikacijo, ne uvedejo posebnih tehničnih zahtev. Ob kršitvi ali delnem oviranju prigrasene identifikacijske sheme ali možnosti avtentikacije države članice takoj začasno prekličejo ali ukinejo prigraseni identifikacijski sistem ali možnost avtentikacije oziroma ogrožene dele ter o tem obvestijo druge države članice in Komisijo v skladu s členom 7;
- (e) država članica prigrasiteljica je odgovorna:
  - (i) da so osebni identifikacijski podatki iz točke (c) nedvoumno dodeljeni in
  - (ii) možnost avtentikacije iz točke (d).

2. Točka (e) v odstavku 1 ne posega v odgovornost udeleženih strani v transakciji, pri kateri se uporabljajo elektronska identifikacijska sredstva, ki so del prigrasene sheme.

## Člen 7

### Prigrasitev

1. Države članice, ki prigrasijo elektronsko identifikacijsko shemo, Komisiji predložijo naslednje informacije in takoj tudi vse naknadne spremembe:

- (a) opis prigrasenega elektronske identifikacijske sheme;
- (b) organe, pristojne za prigraseno elektronsko identifikacijsko shemo;
- (c) informacije o tem, kdo upravlja registracijo enoznačnih identifikatorjev oseb;
- (d) opis možnosti avtentikacije;
- (e) ureditve za začasni preklic ali ukinitvev prigrasene identifikacijske sheme ali možnosti avtentikacije oziroma zadevnih ogroženih delov.

2. Šest mesecev po začetku veljavnosti Uredbe Komisija v *Uradnem listu Evropske unije* objavi seznam elektronskih identifikacijskih shem, priglašenih v skladu z odstavkom 1, in osnovne informacije o njih.

3. Če Komisija prejme priglasitev po izteku obdobja iz odstavka 2, seznam spremeni v treh mesecih.

4. Komisija lahko z izvedbenimi akti določi okoliščine, oblike in postopke za priglasitev v skladu z odstavkoma 1 in 3. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

#### *Člen 8*

### **Usklajevanje**

1. Države članice sodelujejo, da se zagotovi interoperabilnost elektronskih identifikacijskih sredstev, ki so del priglašene sheme, in da se okrepi njihova varnost.

2. Komisija z izvedbenimi akti določi potrebne podrobnosti za pospeševanje sodelovanja med državami članicami iz odstavka 1, da se spodbudi visoka raven zaupanja in varnosti, ki ustreza stopnji tveganja. Ti izvedbeni akti se nanašajo zlasti na izmenjavo informacij, izkušenj in dobrih praks v zvezi z elektronskimi identifikacijskimi sistemi, medsebojni pregled priglašenih elektronskih identifikacijskih shem in preverjanje zadevnega razvoja v sektorju elektronske identifikacije s strani pristojnih organov držav članic. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

3. Komisija se pooblasti za sprejemanje delegiranih aktov v skladu s členom 38, v katerih določi minimalne tehnične zahteve za spodbujanje čezmejne interoperabilnosti elektronskih identifikacijskih sredstev.

## **POGLAVJE III**

### **SKRBNIŠKE STORITVE**

#### **Oddelek 1**

#### *Splošne določbe*

#### *Člen 9*

### **Odgovornost**

1. Ponudnik skrbniških storitev je odgovoren za kakršno koli neposredno škodo, povzročeno fizični ali pravni osebi zaradi neizpolnjevanja obveznosti iz člena 15(1), razen če dokaže, da ni deloval iz malomarnosti.

2. Ponudnik kvalificiranih skrbniških storitev je odgovoren za kakršno koli neposredno škodo, povzročeno fizični ali pravni osebi zaradi neizpolnjevanja zahtev iz te uredbe, zlasti člena 19, razen če dokaže, da ni deloval iz malomarnosti.

## *Člen 10*

### **Ponudniki skrbniških storitev iz tretjih držav**

1. Kvalificirane skrbniške storitve in kvalificirani certifikati, ki jih zagotovijo ponudniki kvalificiranih skrbniških storitev s sedežem v tretji državi, se sprejmejo za kvalificirane skrbniške storitve in kvalificirane certifikate, ki jih zagotavljajo ponudniki kvalificiranih skrbniških storitev s sedežem na ozemlju Evropske unije, če so kvalificirane skrbniške storitve ali kvalificirani certifikati iz tretje države priznani v okviru sporazuma med Unijo in tretjimi državami ali mednarodnimi organizacijami v skladu s členom 218 PDEU.
2. V skladu z odstavkom 1 taki sporazumi zagotavljajo, da ponudniki skrbniških storitev v tretjih državah ali mednarodnih organizacijah izpolnjujejo zahteve, ki veljajo za kvalificirane skrbniške storitve in kvalificirane certifikate, ki jih zagotovijo ponudniki kvalificiranih skrbniških storitev s sedežem na ozemlju Unije, zlasti v zvezi z varstvom osebnih podatkov, varnostjo in nadzorom.

## *Člen 11*

### **Obdelava in varstvo podatkov**

1. Ponudniki skrbniških storitev in nadzorni organi pri obdelavi osebnih podatkov zagotovijo, da je ta poštena in zakonita v skladu z Direktivo 95/46/ES.
2. Ponudniki skrbniških storitev osebne podatke obdelujejo v skladu z Direktivo 95/46/ES. Taka obdelava je strogo omejena na najmanjši obseg podatkov, ki je potreben za izdajo in ohranitev certifikata ali za zagotavljanje skrbniške storitve.
3. Ponudniki skrbniških storitev zagotovijo zaupnost in celovitost podatkov o osebi, ki ji zagotavljajo skrbniško storitev.
4. Ne glede na pravni učinek psevdonimov v skladu z nacionalno zakonodajo države članice ponudnikom skrbniških storitev ne smejo preprečiti, da v certifikatih za elektronski podpis navedejo psevdonim namesto imena podpisnika.

## *Člen 12*

### **Dostopnost za invalide**

Skrbniške storitve in izdelki za končne uporabnike, ki se uporabljajo pri zagotavljanju teh storitev, so dostopni za invalide, če je to mogoče.

## **Oddelek 2**

### *Nadzor*

## *Člen 13*

### **Nadzorni organ**



1. Države članice imenujejo ustrezen organ s sedežem na njihovem ozemlju ali – po medsebojnem dogovoru – na ozemlju druge države članice pod pristojnostjo države članice, ki organ imenuje. Nadzorni organi imajo vsa nadzorna in preiskovalna pooblastila, ki jih potrebujejo za opravljanje svojih nalog.

2. Nadzorni organ je pristojen za opravljanje naslednjih nalog:

- (a) spremljanje ponudnikov skrbniških storitev s sedežem na ozemlju države članice, ki organ imenuje, da zagotovijo, da ti izpolnjujejo zahteve iz člena 15;
- (b) izvajanje nadzora nad ponudniki kvalificiranih skrbniških storitev s sedežem na ozemlju države članice, ki organ imenuje, in kvalificiranih skrbniških storitev, ki jih zagotavljajo, da zagotovijo, da ponudniki in kvalificirane skrbniške storitve, ki jih zagotavljajo, izpolnjujejo zadevne zahteve iz te uredbe;
- (c) zagotavljajo, da se pomembne informacije in podatki iz točke (g) člena 19(2), ki jih beležijo ponudniki kvalificiranih skrbniških storitev, hranijo in so dostopne dovolj dolgo tudi po tem, ko ponudnik kvalificiranih skrbniških storitev preneha opravljati dejavnosti, da tako zagotovijo neprekinjenost storitve.

3. Vsak nadzorni organ Komisiji in državam članicam do konca prvega četrtletja naslednjega leta predloži letno poročilo o nadzornih dejavnostih v zadnjem koledarskem letu. To poročilo vsebuje najmanj:

- (a) informacije o nadzornih dejavnostih;
- (b) povzetek obvestil o kršitvah, ki jih je prejel od ponudnika skrbniških storitev v skladu s členom 15(2);
- (c) statistične podatke o trgu in uporabi kvalificiranih skrbniških storitev, vključno z informacijami o samih ponudnikih kvalificiranih skrbniških storitev, kvalificiranih skrbniških storitvah, ki jih zagotavljajo, in uporabljenih izdelkih ter splošni opis njihovih strank.

4. Države članice Komisiji in državam članicam sporočijo imena in naslove posameznih imenovanih nadzornih organov.

5. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih določi postopke, ki se uporabljajo za opravljanje nalog iz odstavka 2.

6. Komisija lahko z izvedbenimi akti določi okoliščine, oblike in postopke, ki se nanašajo na poročilo iz odstavka 3. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

#### *Člen 14*

#### **Medsebojna pomoč**

1. Nadzorni organi sodelujejo, da bi si izmenjali dobre prakse ter drug drugemu v najkrajšem možnem času zagotovili pomembne informacije in medsebojno pomoč ter tako skladno opravili svoje dejavnosti. Medsebojna pomoč se zagotavlja zlasti pri zahtevkih za informacije

in nadzorne ukrepe, kot so zahtevki za opravljanje inšpekcijskih pregledov, ki se nanašajo na varnostne revizije v skladu s členi 15, 16 in 17.

2. Nadzorni organ, na katerega se naslovi zahtevek za pomoč, tega zahtevka ne sme zavrnil, razen če:

- (a) ni pristojen za obravnavanje zahtevka; ali
- (b) bi bilo obravnavanje zahtevka neskladno s to uredbo.

3. Nadzorni organi po potrebi izvajajo skupne preiskave, v katerih sodeluje osebje nadzornih organov drugih držav članic.

Nadzorni organ države članice, v kateri poteka preiskava, lahko v skladu z nacionalno zakonodajo preiskovalne naloge prenese na osebje nadzornega organa, ki mu pomaga. Taka pooblastila se lahko izvajajo samo pod vodstvom in v prisotnosti osebja nadzornega organa gostitelja. Za osebje nadzornega organa, ki mu pomaga, velja nacionalna zakonodaja nadzornega organa gostitelja. Nadzorni organ gostitelj je odgovoren za dejanja osebja nadzornega organa, ki mu pomaga.

4. Komisija lahko z izvedbenimi akti določi oblike in postopke za medsebojno pomoč iz tega člena. Navedene izvedbene akt sprejme v skladu s postopkom pregleda iz člena 39(2).

## *Člen 15*

### **Varnostne zahteve za ponudnike skrbniških storitev**

1. Ponudniki skrbniških storitev s sedežem na ozemlju Unije sprejmejo ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj, povezanih z varnostjo skrbniških storitev, ki jih zagotavljajo. Ti ukrepi ob upoštevanju obstoječega stanja zagotovijo, da raven varnosti ustreza stopnji tveganja. Ti ukrepi se sprejmejo zlasti zato, da bi se preprečil in zmanjšal vpliv varnostnih incidentov ter da bi bile o škodljivih učinkih takih incidentov obveščene zainteresirane strani.

Ne glede na člen 16(1) lahko vsak ponudnik skrbniških storitev nadzornemu organu predloži poročilo o varnostni reviziji priznanega neodvisnega organa, s katero potrdi, da so bili sprejeti ustrezni varnostni ukrepi.

2. Ponudniki skrbniških storitev o vseh kršitvah varnosti ali izgubi celovitosti, ki so pomembno vplivale na zagotovljeno skrbniško storitev in na v njej vsebovane podatke, takoj in, če je izvedljivo, najmanj 24 ur po ugotovitvi obvestijo pristojni nadzorni organ, pristojni nacionalni organ za varnost informacij in druge zadevne tretje osebe, kot je organ za varstvo podatkov.

Zadevni nadzorni organ po potrebi obvesti nadzorne organe drugih držav članic in Evropsko agencijo za varnost omrežij in informacij (ENISA), zlasti če se kršitev varnosti ali izguba celovitosti nanaša na dve ali več držav članic.

Zadevni nadzorni organ lahko o tem obvesti tudi javnost ali to zahteva od ponudnika skrbniških storitev, če ugotovi, da je razkritje kršitve v javnem interesu.

3. Nadzorni organ agenciji ENISA in Komisiji enkrat letno predloži povzetek obvestil o kršitvah, ki jih je prejel od ponudnikov skrbniških storitev.
4. Za izvajanje odstavkov 1 in 2 je pristojni nadzorni organi pooblaščen, da za ponudnike skrbniških storitev izda zavezujoča navodila.
5. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih podrobneje določi ukrepe iz odstavka 1.
6. Komisija lahko z izvedbenimi akti določi okoliščine, oblike in postopke, vključno z roki, ki se uporabljajo za namene odstavkov 1 do 3. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

## *Člen 16*

### **Nadzor ponudnikov kvalificiranih skrbniških storitev**

1. Ponudnike kvalificiranih skrbniških storitev enkrat letno revidira priznani neodvisni organ, s čimer zagotovi, da ponudniki in kvalificirane skrbniške storitve, ki jih zagotavljajo, izpolnjujejo zahteve iz te uredbe, in nadzornemu organu predloži poročilo o varnostni reviziji.
2. Nadzorni organ lahko ne glede na odstavek 1 na lastno pobudo ali na zahtevo Komisije kadar koli revidira ponudnike kvalificiranih skrbniških storitev, s čimer potrdi, da ponudniki in kvalificirane skrbniške storitve, ki jih zagotavljajo, še vedno izpolnjuje pogoje iz te uredbe. Nadzorni organ obvesti organe za varstvo podatkov o rezultatih revizij, če domneva, da so bili kršeni predpisi o varstvu osebnih podatkov.
3. Nadzorni organ je pristojen za izdajanje zavezujočih navodil ponudnikom kvalificiranih skrbniških storitev, da se izpolnijo neizpolnjene zahteve, ugotovljene v varnostni reviziji.
4. Če ponudnik kvalificiranih skrbniških storitev take pomanjkljivosti iz odstavka 3 ne odpravi v roku, ki ga določi nadzorni organ, izgubi kvalificirani status, nadzorni organ pa ga obvesti, da bo njegov status na seznamih ponudnikov skrbniških storitev iz člena 18 temu ustrezno spremenjen.
5. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v kateri določi pogoje, pod katerimi se prizna neodvisni organ, ki opravlja revizijo iz odstavka 1 tega člena ter členov 15(1) in 17(1).
6. Komisija lahko z izvedbenimi akti določi okoliščine, postopke in oblike, ki se uporabljajo za namene odstavkov 1, 2 in 4. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

## *Člen 17*

### **Začetek zagotavljanja kvalificirane skrbniške storitve**

1. Ponudniki kvalificiranih skrbniških storitev nadzorni organ obvestijo, da nameravajo začeti zagotavljati kvalificirano skrbniško storitev, ter mu poročilo o varnostni reviziji, ki jo opravi priznani neodvisni organ, kot to določa člen 16(1). Ponudniki kvalificiranih skrbniških

storitev lahko kvalificirane skrbniške storitve začnejo zagotavljati po tem, ko so nadzornemu organu predložili priglasitev in poročilo o varnostni reviziji.

2. Ko so zadevni dokumenti predloženi nadzornemu organu v skladu z odstavkom 1, se ponudniki kvalificiranih storitev vključijo na sezname ponudnikov skrbniških storitev iz člena 18, pri čemer se navede, da je bila priglasitev predložena.

3. Nadzorni organ preveri skladnost ponudnika kvalificiranih skrbniških storitev in kvalificiranih skrbniških storitev, ki jih ta zagotavlja, z zahtevami iz te uredbe.

Nadzorni organ kvalificirani status ponudnikov kvalificiranih storitev in kvalificiranih skrbniških storitev, ki jih ti zagotavljajo, vključi na sezname ponudnikov skrbniških storitev po pozitivnem zaključku preverjanja najpozneje mesec dni po predloženi priglasitvi v skladu z odstavkom 1.

Če preverjanja ne konča v enem mesecu, o tem obvesti ponudnika kvalificiranih skrbniških storitev ter podrobno navede razloge za zamudo in rok, do katerega bo preverjanje končal.

4. Kvalificirane skrbniške storitve, ki je bil priglášena v skladu z odstavkom 1, zadevni organ javnega sektorja med upravnim postopkom ali izpolnjevanju formalnosti ne sme zavrniti z utemeljitvijo, da ni vključena na sezname iz odstavka 3.

5. Komisija lahko z izvedbenimi akti določi okoliščine, oblike in postopke za namene odstavkov 1, 2 in 3. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

## *Člen 18*

### **Seznami ponudnikov skrbniških storitev**

1. Vsaka država članica sestavi, vodi in objavi sezname ponudnikov skrbniških storitev z informacijami o ponudnikih kvalificiranih skrbniških storitev, za katere je pristojna, skupaj z informacijami, ki se nanašajo na kvalificirane skrbniške storitve, ki jih ponudniki zagotavljajo.

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

3. Države članice Komisiji o organu, ki je pristojen za sestavljanje, vodenje in objavljanje nacionalnih seznamov ponudnikov skrbniških storitev, takoj predložijo informacije ter podrobnosti o tem, kje so taki sezname objavljeni, o uporabljenih certifikatih za podpisovanje ali ožigosanje seznamov ponudnikov skrbniških storitev in o vseh njihovih spremembah.

4. Komisija po varnem kanalu in v elektronsko podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo, javnosti razkrije informacije iz odstavka 3.

5. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih določi informacije iz odstavka 1.

6. Komisija lahko z izvedbenimi akti določi tehnične specifikacije in oblike za sezname ponudnikov skrbniških storitev, ki se uporabljajo za namene odstavkov 1 do 4. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

## Člen 19

### Zahteve za ponudnike kvalificiranih skrbniških storitev

1. Ob izdaji kvalificiranega certifikata ponudnik kvalificiranih skrbniških storitev z ustreznimi sredstvi in v skladu z nacionalno zakonodajo preveri istovetnost in po potrebi druge posebne lastnosti fizične ali pravne osebe, za katero se izdaja kvalificirani certifikat.

Te podatke preveri ponudnik kvalificiranih storitev ali pooblaščen tretja oseba, ki deluje v pristojnosti ponudnika kvalificiranih storitev:

- (a) po fizičnem videzu fizične osebe ali pooblaščenega predstavnika pravne osebe ali
- (b) na daljavo s pomočjo elektronskih identifikacijskih shem iz priglašene sistema, izdanih v skladu s točko (a).

2. Ponudniki kvalificiranih skrbniških storitev, ki zagotavljajo kvalificirane skrbniške storitve:

- (a) zaposlujejo osebje s potrebnim strokovnim znanjem, izkušnjami in kvalifikacijami, ki uporablja upravne in vodstvene postopke, ki so v skladu z evropskimi ali mednarodnimi standardi, in ki se je udeležilo ustreznega usposabljanja v zvezi z varnostjo in predpisi o varstvu osebnih podatkov;
- (b) nosijo tveganje škode in imajo dovolj finančnih sredstev ali sklenjeno ustrezno zavarovanje odgovornosti;
- (c) pred vstopom v pogodbeno razmerje vsako osebo, ki želi uporabljati kvalificirano skrbniško storitev, obvestijo o natančnih pogojih uporabe zadevne storitve;
- (d) uporabljajo zanesljive sisteme in opremo, ki so zaščiteni pred spreminjanjem ter zagotavljajo tehnično varnost in zanesljivost postopkov, pri katerih se uporabljajo;
- (e) uporabljajo zanesljive sisteme za shranjevanje podatkov, ki jih prejmejo, v preverljivi obliki, tako da:
  - so ti javno dostopni samo, če je bilo pridobljeno soglasje osebe, za katero so bili podatki izdani,
  - lahko podatke vnašajo in spreminjajo samo pooblaščen osebe,
  - se lahko preveri avtentičnost podatkov;
- (f) sprejmejo ukrepe proti ponarejanju in kraji podatkov;
- (g) v ustreznem časovnem obdobju beležijo vse pomembne informacije o podatkih, ki jih je izdal in prejel ponudnik kvalificiranih skrbniških storitev, zlasti zato, da se lahko v sodnih postopkih zagotovijo dokazi. Zapisovanje je lahko elektronsko;

- (h) imajo posodobljene načrte za prenehanje zagotavljanja storitve, da se zagotovi neprekinjenost v skladu z ureditvami, ki jih izda nadzorni organ v skladu s točko (c) člena 13(2);
- (i) zagotovijo zakonito obdelavo osebnih podatkov v skladu s členom 11.

3. Ponudniki kvalificiranih skrbniških storitev, ki izdajajo kvalificirane certifikate, v svojih podatkovnih zbirkah certifikatov preklic certifikata zabeležijo v desetih minutah po preklicu.

4. V zvezi z odstavkom 3 ponudniki kvalificiranih skrbniških storitev, ki izdajajo kvalificirane certifikate, vsaki odvisni strani zagotovijo informacije o veljavnosti ali preklicu kvalificiranih izdanih certifikatov. Te informacije predložijo na zanesljiv, brezplačen in učinkovit avtomatiziran način kadar koli vsaj za posamezne certifikate.

5. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za sisteme skrbniških storitev in izdelke. Zahteve iz člena 19 se štejejo za izpolnjene, če sistemi skrbniških sistemov in izdelki izpolnjujejo te standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

### **Oddelek 3**

#### ***Elektronski podpis***

##### *Člen 20*

#### **Pravni učinki in sprejemljivost elektronskih podpisov**

1. Elektronskemu podpisu se kot dokazu v sodnih postopkih ne smeta odvzeti pravni učinek in dopustnost zgolj zato, ker je ta v elektronski obliki.
2. Kvalificirani elektronski podpis ima enak pravni učinek kot lastnoročni podpis.
3. Vse države članice priznajo in sprejmejo kvalificirane elektronske podpise.
4. Če se zahteva elektronski podpis z nižjo varnostno ravno, kot jo ima kvalificirani elektronski podpis, zlasti če to pri dostopu do spletne storitve, ki jo zagotavlja organ javnega sektorja, na podlagi ustrezne ocene tveganj, povezanih s tako storitvijo, zahteva država članica, se priznajo in sprejmejo vsi elektronski podpisi, ki ustrezajo vsaj enaki ravni varnosti.
5. Države članice za čezmejni dostop do spletne storitve, ki jo zagotavlja organ javnega sektorja, ne zahtevajo elektronskega podpisa z višjo varnostno ravno, kot jo ima kvalificirani elektronski podpis.
6. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih določi različne varnostne ravni elektronskega podpisa iz odstavka 4.
7. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za varnostne ravni elektronskega podpisa. Skladnost z varnostno ravno iz delegiranega akta, sprejetega v skladu z odstavkom 6, se šteje za izpolnjeno, če elektronski podpisi izpolnjujejo te standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

## Člen 21

### **Kvalificirani certifikati za elektronski podpis**

1. Kvalificirani certifikati za elektronski podpis izpolnjujejo zahteve iz Priloge I.
2. Za kvalificirane certifikate za elektronski podpis ne veljajo obvezne zahteve, ki presegajo zahteve iz Priloge I.
3. Če je bil kvalificirani certifikat za elektronski podpis po prvotnem aktiviranju preklican, izgubi veljavnost, status pa se mu v nobenem primeru ne povrne z obnovitvijo veljavnosti.
4. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih podrobneje določi zahteve iz Priloge I.
5. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirane certifikate za elektronski podpis. Zahteve iz Priloge I se štejejo za izpolnjene, če kvalificirani certifikat za elektronski podpis izpolnjuje navedene standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

## Člen 22

### **Zahteve za naprave za ustvarjanje kvalificiranega elektronskega podpisa**

1. Naprave za ustvarjanje kvalificiranega elektronskega podpisa izpolnjujejo zahteve iz Priloge II.
2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za naprave za ustvarjanje kvalificiranega elektronskega podpisa. Zahteve iz Priloge II se štejejo za izpolnjene, če naprava za ustvarjanje kvalificiranega elektronskega podpisa izpolnjuje navedene standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

## Člen 23

### **Certificiranje naprav za ustvarjanje kvalificiranega elektronskega podpisa**

1. Naprave za ustvarjanje kvalificiranega elektronskega podpisa lahko certificirajo ustrezni javni ali zasebni organi, ki jih imenujejo države članice, pod pogojem, da je bila zanje opravljena varnostna ocena v skladu z enim od standardov za ocenjevanje varnosti izdelkov informacijske tehnologije s seznama, ki ga je sestavila Komisija v izvedbenih aktih. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.
2. Države članice Komisiji in drugim državam članicam sporočijo imena in naslove imenovanega javnega ali zasebnega organa iz odstavka 1.
3. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih določi posebna merila, ki jih morajo izpolnjevati imenovani organi iz odstavka 1.

## Člen 24

### **Objava seznama certificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa**

1. Države članice Komisiji takoj predložijo informacije o napravah za ustvarjanje kvalificiranega elektronskega podpisa, ki so jih certificirali organi iz člena 23. Komisiji takoj sporočijo tudi informacije o napravah za ustvarjanje elektronskega podpisa, ki niso več certificirane.
2. Komisija na podlagi prejetih informacij sestavi, objavi in vodi seznam certificiranih naprav za ustvarjanje elektronskega podpisa.
3. Komisija lahko z izvedbenimi akti določi okoliščine, oblike in postopke za namene odstavka 1. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

## Člen 25

### **Zahteve za potrjevanje kvalificiranih elektronskih podpisov**

1. Kvalificirani elektronski podpis se šteje za veljavnega, če je mogoče z visoko ravno zanesljivosti ugotoviti, da je med podpisovanjem:
  - (a) certifikat, na katerem temelji podpis, kvalificirani certifikat za elektronski podpis, ki izpolnjuje določbe iz Priloge I;
  - (b) zahtevani kvalificirani certifikat pristen in veljaven;
  - (c) podatki za potrjevanja podpisa ustrezajo podatkom, zagotovljenim odvisnim stranem;
  - (d) nabor podatkov, ki nedvoumno predstavlja podpisnika, je odvisni strani pravilno posredovan;
  - (e) če se uporablja psevdonim, je njegova uporaba odvisni strani jasno sporočena;
  - (f) elektronski podpis je bil ustvarjen z napravo za ustvarjanje kvalificiranega elektronskega podpisa;
  - (g) celovitost podpisanih podatkov ni ogrožena;
  - (h) izpolnjene so zahteve iz točke 7 člena 3;
  - (i) sistem za potrjevanje podpisa odvisni strani zagotavlja pravilne rezultate postopka potrjevanja in ji omogoča odkrivanje vseh varnostnih težav.
2. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih podrobneje določi zahteve iz odstavka 1.
3. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za potrjevanje kvalificiranih elektronskih podpisov. Zahteve iz odstavka 1 se štejejo za izpolnjene, če so pri potrjevanju kvalificiranih elektronskih podpisov izpolnjeni ti standardi. Komisija navedene



izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

#### *Člen 26*

##### **Kvalificirana storitev potrjevanja za kvalificirane elektronske podpise**

1. Kvalificirano storitev potrjevanja za kvalificirane elektronske storitve zagotavlja ponudnik kvalificiranih skrbniških storitev, ki:

- (a) potrjevanje opravi v skladu s členom 25(1) in
- (b) odvisnim stranem omogoči, da prejme rezultat postopka potrjevanja na zanesljiv in učinkovit avtomatiziran način z naprednim elektronskim podpisom ali naprednim elektronskim žigom ponudnika kvalificiranih storitev potrjevanja.

2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirano storitev potrjevanja iz odstavka 1. Zahteve iz točke (b) odstavka 1 se štejejo za izpolnjene, če storitev potrjevanja za kvalificirani elektronski podpis izpolnjuje navedene standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

#### *Člen 27*

##### **Hramba kvalificiranih elektronskih podpisov**

1. Storitev hrambe kvalificiranega elektronskega podpisa zagotavlja ponudnik kvalificiranih skrbniških storitev, ki uporablja postopke in tehnologije, ki omogočajo podaljšanje zanesljivosti podatkov za potrjevanje kvalificiranega elektronskega podpisa po obdobju tehnološke veljavnosti.

2. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih podrobneje določi zahteve iz odstavka 1.

3. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za hrambo kvalificiranih elektronskih podpisov. Zahteve iz odstavka 1 se štejejo za izpolnjene, če ureditve za hrambo kvalificiranih elektronskih podpisov izpolnjujejo te standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

#### **Oddelek 4**

##### ***Elektronski žigi***

#### *Člen 28*

##### **Pravni učinki elektronskega žiga**

1. Elektronskemu žigu se ne odvzmeta pravni učinek in dopustnost kot dokaz v sodnih postopkih zgolj zato, ker je v elektronski obliki.

2. Za kvalificirani elektronski žig velja pravna domneva, da zagotavlja izvor in celovitost podatkov, s katerimi je povezan.

3. Kvalificirani elektronski žig priznajo in sprejmejo vse države članice.

4. Če se zahteva elektronski žig z nižjo varnostno ravno, kot jo ima kvalificirani elektronski žig, zlasti če to pri dostopu do spletne storitve, ki jo zagotavlja organ javnega sektorja, na podlagi ustrezne ocene tveganj, povezanih s tako storitvijo, zahteva država članica, se priznajo in sprejmejo vsi elektronski podpisi, ki ustrezajo vsaj enaki varnostni ravni.

5. Države članice za dostop do spletne storitve, ki jo zagotavlja organ javnega sektorja, ne zahtevajo elektronskega žiga z višjo varnostno ravno, kot jo ima kvalificirani elektronski žig.

6. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih določi različne varnostne ravni elektronskih žigov iz odstavka 4.

7. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za varnostne ravni elektronskih žigov. Skladnost z varnostno ravno iz delegiranega akta, sprejetega v skladu z odstavkom 6, se šteje za izpolnjeno, če elektronski žig izpolnjuje navedene standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

## Člen 29

### **Zahteve za kvalificirane certifikate za elektronski žig**

1. Kvalificirani certifikati za elektronski žig izpolnjujejo zahteve iz Priloge III.

2. Za kvalificirane certifikate za elektronski žig ne veljajo obvezne zahteve, ki presegajo zahteve iz Priloge III.

3. Če je bil kvalificirani certifikat za elektronski žig po aktiviranju preklican, izgubi veljavnost, status pa se mu v nobenem primeru ne povrne z obnovitvijo veljavnosti.

4. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih podrobneje določi zahteve iz Priloge III.

5. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirane certifikate za elektronski žig. Zahteve iz Priloge III se štejejo za izpolnjene, če kvalificirani certifikat za elektronski žig izpolnjuje navedene standarde. Komisija izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Te akte objavi v *Uradnem listu Evropske unije*.

## Člen 30

### **Naprave za ustvarjanje kvalificiranega elektronskega žiga**

1. Člen 22 se smiselno uporablja za zahteve za naprave za ustvarjanje kvalificiranega elektronskega žiga.

2. Člen 23 se smiselno uporablja za certificiranje naprav za ustvarjanje kvalificiranega elektronskega žiga.

3. Člen 24 se smiselno uporablja za objavo seznama certificiranih naprav za ustvarjanje kvalificiranega elektronskega žiga.

### *Člen 31*

#### **Potrjevanje in hramba kvalificiranih elektronskih žigov**

Členi 25, 26 in 27 se smiselno uporabljajo za potrjevanje in hrambo kvalificiranih elektronskih žigov.

### **Oddelek 5**

#### ***Elektronski časovni žig***

### *Člen 32*

#### **Pravni učinek elektronskih časovnih žigov**

1. Elektronskemu časovnemu žigu se ne odvzmeta pravni učinek in dopustnost kot dokaz v sodnih postopkih zgolj zato, ker je v elektronski obliki.
2. Za kvalificirani elektronski časovni žig velja pravna domneva, da zagotavlja zanesljivost navedenega datuma in celovitosti podatkov, s katerimi je datum povezan.
3. Kvalificirani elektronski časovni žig priznajo in sprejmejo vse države članice.

### *Člen 33*

#### **Zahteve za kvalificirane elektronske časovne žige**

1. Kvalificirani elektronski časovni žig izpolnjuje naslednje zahteve:
  - (a) natančno je povezan z univerzalnim koordiniranim časom (UTC) tako, da je možnost nezaznavnosti spremembe podatkov izključena;
  - (b) temelji na pravilnem časovnem viru;
  - (c) izda ga ponudnik kvalificiranih skrbniških storitev;
  - (d) podpisan je z naprednim elektronskim podpisom ali naprednim elektronskim žigom ponudnika kvalificiranih skrbniških storitev ali drugo enakovredno metodo.
2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za natančno povezovanje časa s podatki in za pravilen časovni vir. Skladnost z zahtevami iz odstavka 1 se šteje za izpolnjeno, če natančna povezava časa s podatki in natančen časovni vir izpolnjujeta navedene standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

### **Oddelek 6**

#### ***Elektronski dokumenti***

## Člen 34

### **Pravni učinki in sprejem elektronskih dokumentov**

1. Elektronski dokument se ob upoštevanju njegove varnostne ravni avtentičnosti in celovitosti šteje za enakovrednega dokumentu v papirni obliki in za dopustnega kot dokaz v sodnih postopkih.
2. Za dokument s kvalificiranim elektronskim podpisom ali kvalificiranim elektronskim žigom osebe, ki je pristojna za izdajo zadevnega dokumenta, velja pravna domneva o njegovi avtentičnosti in celovitosti, pod pogojem, da dokument ne vsebuje dinamičnih elementov, ki ga lahko samodejno spremenijo.
3. Če se pri zagotavljanju spletne storitve, ki jo zagotavlja organ javnega sektorja, zahteva izvirnik ali certificirana kopija, druge države članice brez dodatnih zahtev sprejmejo vsaj elektronske dokumente, ki jih izdajo osebe, pristojne za izdajanje zadevnih dokumentov, in ki se štejejo za izvornike ali certificirane kopije v skladu z nacionalno zakonodajo izvorne države članice.
4. Komisija lahko z izvedbenimi akti določi oblike elektronskih podpisov in žigov, ki se sprejmejo, če država članica pri zagotavljanju spletne storitve, ki jo zagotavlja organ javnega sektorja iz odstavka 2, zahteva podpisan ali ožigosan dokument. Navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2).

## **Oddelek 7**

### ***Kvalificirana storitev elektronske dostave***

## Člen 35

### **Pravni učinek storitve elektronske dostave**

1. Podatki, poslani ali prejeti s pomočjo storitve elektronske dostave, so v zvezi s celovitostjo podatkov ter zanesljivostjo datuma in časa pošiljanja podatkov določenemu naslovniku oziroma prejetja podatkov s strani naslovnika, dopustni kot dokaz v sodnih postopkih.
2. Za podatke, poslane ali prejete s pomočjo kvalificirane storitve elektronske dostave, velja pravna domneva o celovitosti podatkov ter točnosti datuma in časa pošiljanja ali prejema podatkov, ki sta navedena v kvalificiranem elektronskem sistemu za dostavo.
3. Komisija se v skladu s členom 38 pooblasti za sprejetje delegiranih aktov, v katerih natančno določi mehanizme za pošiljanje ali prejemanje podatkov s pomočjo storitev elektronske dostave, ki se uporabljajo za spodbujanje interoperabilnosti med storitvami elektronske dostave.

## Člen 36

### **Zahteve za kvalificirane storitve elektronske dostave**

1. Kvalificirane storitve elektronske dostave izpolnjujejo naslednje zahteve:
  - (a) zagotavlja jih eden ali več ponudnikov kvalificiranih skrbniških storitev;

- (b) omogočajo nedvoumno identifikacijo pošiljatelja in po potrebi naslovnika;
- (c) postopek pošiljanja ali prejemanja podatkov je z naprednim elektronskim podpisom ali naprednim elektronskim žigom ponudnika kvalificiranih skrbniških storitev zavarovan tako, da je možnost nezaznavnosti spremembe podatkov izključena;
- (d) vsaka sprememba podatkov, potrebna za pošiljanje ali prejemanje podatkov, se jasno sporoči pošiljatelju in naslovniku podatkov;
- (e) čas pošiljanja, prejema in vseh sprememb podatkov se navede s kvalificiranim elektronskim časovnim žigom;
- (f) pri prenašanju podatkov med dvema ali več ponudniki kvalificiranih skrbniških storitev za vse ponudnike kvalificiranih skrbniških storitev veljajo zahteve iz točk (a) do (e).

2. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za postopke pošiljanja in prejemanja podatkov. Zahteve iz odstavka 1 se štejejo za izpolnjene, če postopek pošiljanja in prejemanja podatkov izpolnjuje navedene standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

## **Oddelek 8**

### ***Avtentikacija spletnih strani***

#### *Člen 37*

#### **Zahteve za kvalificirane certifikate za avtentikacijo spletnih strani**

1. Kvalificirani certifikati za avtentikacijo spletnih strani izpolnjujejo zahteve iz Priloge IV.
2. Kvalificirani certifikati za avtentikacijo spletnih strani se priznajo in sprejmejo v vseh državah članicah.
3. Komisija se v skladu s členom 38 pooblasti za sprejemanje delegiranih aktov, v katerih podrobneje določi zahteve iz Priloge IV.
4. Komisija lahko z izvedbenimi akti določi referenčne številke standardov za kvalificirane certifikate za avtentikacijo spletnih strani. Zahteve iz Priloge IV se štejejo za izpolnjene, če kvalificirani certifikat za avtentikacijo spletnih strani izpolnjuje navedene standarde. Komisija navedene izvedbene akte sprejme v skladu s postopkom pregleda iz člena 39(2). Navedene akte objavi v *Uradnem listu Evropske unije*.

## **POGLAVJE IV**

### **DELEGIRANI AKTI**

#### *Člen 38*

#### **Izvajanje pooblastila**

1. Pooblastilo za sprejemanje delegiranih aktov se na Komisijo prenese pod pogoji iz tega člena.
2. Pooblastilo za sprejemanje delegiranih aktov iz členov 8(3), 13(5), 15(5), 16(5), 18(5), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) in 37(3) se prenese na Komisijo za nedoločen čas po začetku veljavnosti te uredbe.
3. Evropski parlament in Svet lahko pooblastilo iz členov 8(3), 13(5), 15(5), 16(5), 18(5), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) in 37(3) kadar koli prekličeta. S sklepom o preklicu pooblastilo iz navedenega sklepa preneha veljati. Preklic začne veljati dan po objavi sklepa v *Uradnem listu Evropske unije* ali na poznejši datum, ki je v njem naveden. Preklic ne vpliva na veljavnost že veljavnih delegiranih aktov.
4. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.
5. Delegirani akt, sprejet na podlagi členov 8(3), 13(5), 15(5), 16(5), 18(5), 20(6), 21(4), 23(3), 25(2), 27(2), 28(6), 29(4), 30(2), 31, 35(3) in 37(3), začne veljati samo, če mu Evropski parlament ali Svet v dveh mesecih od uradnega obvestila o tem aktu ne nasprotujeta ali če sta pred iztekom navedenega roka oba obvestila Komisijo, da mu ne bosta nasprotovala. Na pobudo Evropskega parlamenta ali Sveta se to obdobje podaljša za dva meseca.

## **POGLAVJE V**

### **IZVEDBENI AKTI**

#### *Člen 39*

#### **Postopek v odboru**

1. Komisiji pomaga odbor. Ta odbor je odbor po Uredbi (EU) št. 182/2011.
2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe št. 182/2011.

## **POGLAVJE VI**

### **KONČNE DOLOČBE**

#### *Člen 40*

#### **Poročilo**

Komisija o uporabi te uredbe poroča Evropskemu parlamentu in Svetu. Prvo poročilo predloži najpozneje štiri leta po začetku veljavnosti te uredbe. Nadaljnja poročila nato predloži vsaka štiri leta.

#### *Člen 41*

#### **Razveljavitev**

1. Direktiva 1999/93/ES se razveljavi.

2. Sklici na razveljavljeno direktivo se štejejo za sklice na to uredbo.

3. Naprave za varno ustvarjanje podpisa, katerih skladnost je bila ugotovljena v skladu s členom 3(4) Direktive 1999/93/ES, se štejejo za naprave za ustvarjanje kvalificiranega podpisa po tej uredbi.

4. Kvalificirani certifikati, izdani v skladu z Direktivo 1999/93/ES, se štejejo za kvalificirane certifikate za elektronske podpise po tej uredbi do njihovega izteka veljavnosti oziroma največ pet let od začetka veljavnosti te uredbe.

#### *Člen 42*

#### **Začetek veljavnosti**

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

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

V Bruslju,

*Za Evropski parlament*  
*Predsednik*

*Za Svet*  
*Predsednik*

## **PRILOGA I**

### **Zahteve za kvalificirane certifikate za elektronske podpise**

Kvalificirani certifikati za elektronske podpise vsebujejo:

- (a) navedbo, vsaj v obliki, primerni za avtomatizirano obdelavo, da je bil certifikat izdan kot kvalificirani certifikat za elektronski podpis;
- (b) nabor podatkov, ki nedvoumno predstavlja ponudnika kvalificiranih skrbniških storitev, ki izdaja kvalificirane certifikate, vključno vsaj z državo članico, v kateri ima zadevni ponudnik sedež, in
  - za pravne osebe: ime in registrsko številko, kot sta navedena v uradnih evidencah;
  - za fizične osebe: ime osebe;
- (c) nabor podatkov, ki nedvoumno predstavlja podpisnika, za katerega se izdaja certifikat, vključno vsaj z imenom podpisnika ali psevdonimom, ki je kot tak opredeljen;
- (d) podatke za potrjevanje elektronskega podpisa, ki ustrezajo podatkom za ustvarjanje elektronskega podpisa;
- (e) podrobnosti o začetku in koncu veljavnosti certifikata;
- (f) identifikacijsko šifro certifikata, ki je za ponudnika kvalificiranih skrbniških storitev edinstvena;
- (g) napredni elektronski podpis ali napredni elektronski žig ponudnika kvalificiranih skrbniških storitev, ki izdaja certifikat;
- (h) lokacijo, na kateri je certifikat, ki podpira napredni elektronski podpis ali napredni elektronski žig iz točke (g), dostopen brezplačno;
- (i) lokacijo storitev za preverjanje statusa veljavnosti certifikata, s katerimi je mogoče preveriti veljavnost kvalificiranega certifikata;
- (j) če se podatki za ustvarjanje elektronskega podpisa, povezani s podatki za potrjevanje elektronskega podpisa, nahajajo v napravi za ustvarjanje kvalificiranega elektronskega podpisa, se to ustrezno navede vsaj v obliki, primerni za avtomatizirano obdelavo.



## **PRILOGA II**

### **Zahteve za naprave za ustvarjanje kvalificiranega elektronskega podpisa**

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

- (a) je zagotovljena tajnost podatkov za ustvarjanje elektronskega podpisa, s katerimi se izdelava elektronski podpis;
- (b) se podatki za ustvarjanje elektronskega podpisa, s katerimi se izdelava elektronski podpis, pojavijo samo enkrat;
- (c) podatkov za ustvarjanje elektronskega podpisa, s katerimi se izdelava elektronski podpis, ni mogoče pridobiti z razumno stopnjo zanesljivosti in da je elektronski podpis med uporabo trenutno razpoložljive tehnologije zaščiten pred ponarejanjem;
- (d) lahko zakoniti podpisnik zanesljivo štiti podatke za ustvarjanje elektronskega podpisa, s katerimi se izdelava elektronski podpis, pred tem, da bi jih lahko uporabljali drugi.

2. Naprave za ustvarjanje kvalificiranega elektronskega podpisa ne smejo spreminjati podatkov, ki naj bi bili podpisani, ali preprečiti, da bi se ti podatki podpisniku prikazali pred podpisom.

3. Podatke za ustvarjanje elektronskega podpisa v imenu podpisnika pripravi ali upravlja ponudnik kvalificiranih skrbniških storitev.

4. Ponudniki kvalificiranih skrbniških storitev, ki upravljajo podatke za ustvarjanje elektronskega podpisa v imenu podpisnika, lahko podatke za ustvarjanje elektronskega podpisa varnostno kopirajo, če so izpolnjene naslednje zahteve:

- (a) varnost podvojenih naborov podatkov je enaka ravni, ki jo ima varnost prvotnih naborov podatkov;
- (b) število podvojenih naborov podatkov ni večje, kot je to nujno potrebno, da se zagotovi neprekinjenost storitve.

### **PRILOGA III**

#### **Zahteve za kvalificirane certifikate za elektronske žige**

Kvalificirani certifikati za elektronske žige vsebujejo:

- (a) navedbo, vsaj v obliki, primerni za avtomatizirano obdelavo, da je bil certifikat izdan kot kvalificirani certifikat za elektronski žig;
- (b) nabor podatkov, ki nedvoumno predstavlja ponudnika kvalificiranih skrbniških storitev, ki izdaja kvalificirane certifikate, vključno vsaj z državo članico, v kateri ima zadevni ponudnik sedež, in
  - za pravne osebe: ime in registrsko številko, kot sta navedena v uradnih evidencah;
  - za fizične osebe: ime osebe;
- (c) nabor podatkov, ki nedvoumno predstavlja pravno osebo, za katero se certifikat izdaja, vključno vsaj z imenom in registrsko številko, kot sta navedena v uradnih evidencah;
- (d) podatke za potrjevanje elektronskega žiga, ki ustrezajo podatkom za ustvarjanje elektronskega žiga;
- (e) podrobnosti o začetku in koncu veljavnosti certifikata;
- (f) identifikacijsko šifro certifikata, ki je za ponudnika kvalificiranih skrbniških storitev edinstvena;
- (g) napredni elektronski podpis ali napredni elektronski žig ponudnika kvalificiranih skrbniških storitev, ki izdaja certifikat;
- (h) lokacijo, na katerem je certifikat, ki podpira napredni elektronski podpis ali napredni elektronski žig iz točke (g), dostopen brezplačno;
- (i) lokacijo storitev za preverjanje statusa veljavnosti certifikata, s katerimi je mogoče preveriti veljavnost kvalificiranega certifikata;
- (j) če se podatki za ustvarjanje elektronskega žiga, povezani s podatki za potrjevanje elektronskega žiga, nahajajo v napravi za ustvarjanje kvalificiranega elektronskega žiga, se to ustrezno navede vsaj v obliki, primerni za avtomatizirano obdelavo.

## **PRILOGA IV**

### **Zahteve za kvalificirane certifikate za avtentikacijo spletnih strani**

Kvalificirani certifikati za avtentikacijo spletnih strani vsebujejo:

- (a) navedbo, vsaj v obliki, primerni za avtomatizirano obdelavo, da je bil certifikat izdan kot kvalificirani certifikat za avtentikacijo spletnih strani;
- (b) nabor podatkov, ki nedvoumno predstavlja ponudnika kvalificiranih skrbniških storitev, ki izdaja kvalificirane certifikate, vključno vsaj z državo članico, v kateri ima zadevni ponudnik sedež, in
  - za pravne osebe: ime in registrsko številko, kot sta navedena v uradnih evidencah;
  - za fizične osebe: ime osebe;
- (c) nabor podatkov, ki nedvoumno predstavlja pravno osebo, za katero se izdaja certifikat, vključno vsaj z imenom in registrsko številko, kot sta navedena v uradnih evidencah;
- (d) elemente naslova pravne osebe, vključno vsaj z krajem in državo članico, za katero se izdaja certifikat, kot so navedeni v uradnih evidencah;
- (e) ime/imena domene, ki jo upravlja pravna oseba, za katero se izdaja certifikat;
- (f) podrobnosti o začetku in koncu veljavnosti certifikata;
- (g) identifikacijsko šifro certifikata, ki je za ponudnika kvalificiranih skrbniških storitev edinstvena;
- (h) napredni elektronski podpis ali napredni elektronski žig ponudnika kvalificiranih skrbniških storitev, ki izdaja certifikat;
- (i) lokacijo, na katerem je certifikat, ki podpira napredni elektronski podpis ali napredni elektronski žig iz točke (h), dostopen brezplačno;
- (j) lokacijo storitev za preverjanje statusa veljavnosti certifikata, s katerimi je mogoče preveriti veljavnost kvalificiranega certifikata.

## OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

### 1. OKVIR PREDLOGA/POBUDE

Ta ocena finančnih posledic določa zahteve glede upravnih odhodkov za izvajanje predlagane uredbe o *elektronski identifikaciji in skrbniških storitvah za elektronske transakcije na notranjem trgu*.

Po zakonodajnem postopku in razpravi Evropskega parlamenta in Sveta v zvezi s sprejetjem predlagane uredbe bo Komisija zahtevala dvanajst EPDČ za pripravo povezanih delegiranih in izvedbenih aktov, za zagotovitev razpoložljivosti organizacijskih in tehničnih standardov, za obravnavo informacij, ki jih priglasijo države članice, zlasti za vzdrževanje informacij v zvezi z seznama ponudnikov skrbniških storitev, za zagotovitev ozaveščenosti zainteresiranih strani – zlasti državljanov in MSP – o prednostih uporabe elektronske identifikacije, avtentikacije, podpisa in povezanih skrbniških storitev (eIAS) ter za začetek razprav s tretjimi državami z namenom vzpostavitve interoperabilnosti eIAS na globalni ravni.

#### 1.1. Naslov predloga/pobude

**Predlog Komisije za Uredbo o elektronski identifikaciji in skrbniških storitvah za elektronske transakcije na notranjem trgu**

#### 1.2. Zadevna področja v okviru ABM/ABB<sup>25</sup>

**09 INFORMACIJSKA DRUŽBA**

#### 1.3. Vrsta predloga/pobude

- Predlog/pobuda se nanaša na **nov ukrep**.
- Predlog/pobuda se nanaša na **nov ukrep, ki je nadaljevanje pilotnega projekta/pripravljalnega ukrepa**.<sup>26</sup>
- Predlog/pobuda je namenjena **podaljšanju obstoječega ukrepa**.
- Predlog/pobuda se nanaša na **nadaljevanje obstoječega ukrepa z novo usmeritvijo**.

#### 1.4. Cilji

##### 1.4.1. Večletni strateški cilji Komisije, ki naj bi bili doseženi s predlogom/pobudo

Splošni cilji predloga so cilji splošnih politik EU, v katerih se predlog nahaja, kot je strategija EU 2020. Strategija Evropa 2020 naj bi zagotovila „preoblikovanje EU v pametno, trajnostno in vključujoče gospodarstvo, ki ga bo odlikovala visoka stopnja zaposlenosti, produktivnosti in socialne kohezije“.

<sup>25</sup> ABM: upravljanje proračuna po dejavnostih – ABB: oblikovanje proračuna po dejavnostih.

<sup>26</sup> Pilotni in pripravljalni ukrepi iz člena 49(6)(a) ali (b) finančne uredbe.

#### 1.4.2. *Specifični cilji in zadevne dejavnosti ABM/ABB*

Okrepiti zaupanje v vseevropske elektronske transakcije ter zagotoviti čezmejno pravno priznavanje elektronske identifikacije, avtentikacije, podpisa in povezanih skrbniških storitev, pa tudi visoko raven varstva podatkov in okrepitev položaja uporabnikov na enotnem trgu (glej Evropska digitalna agenda, ključna ukrepa 3 in 16).

##### Zadevne dejavnosti AMB/ABB

09 02 — Regulativni okvir za Evropsko digitalno agendo

#### 1.4.3. *Pričakovani izid in učinki*

*Navedite, kakšne posledice naj bi imel predlog/pobuda na upravičence/ciljne skupine.*

Vzpostaviti jasno zakonodajno okolje za storitve eIAS, ki bo povečalo uporabnost za uporabnike in zaupanje v digitalni svet.

#### 1.4.4. *Kazalniki izida in učinkov*

*Navedite, s katerimi kazalniki se bo spremljalo izvajanje predloga/pobude.*

1. obstoj ponudnikov eIAS, ki delujejo v več državah članicah EU;
2. raven, na kateri naprave postanejo interoperabilne (npr. čitalci pametnih kartic) med sektorji in državami;
3. uporaba eIAS s strani vseh kategorij prebivalstva;
4. obseg, v katerem končni uporabniki uporabljajo eIAS za nacionalne in mednarodne (čezmejne) transakcije;
5. raven usklajenosti zakonodaje o eIAS v državah članicah;
6. elektronske identifikacijske sheme, priglašene Komisiji;
7. storitve, dostopne s priglašeni sredstvi elektronske identifikacije v javnem sektorju (npr. e-vlada, e-zdravje, e-pravosodje, e-javna naročila);
8. storitve, dostopne s priglašeni sredstvi elektronske identifikacije v zasebnem sektorju (npr. spletno bančništvo, e-poslovanje, e-stave, prijava na spletne strani, varnejše internetne storitve).

### 1.5. **Utemeljitev predloga/pobude**

#### 1.5.1. *Potrebe, ki jih je treba kratkoročno ali dolgoročno zadovoljiti*

Različne nacionalne uporabe direktive o elektronskem podpisu zaradi različnih razlag te direktive s strani držav članic so privedle do težav pri čezmejni interoperabilnosti ter s tem do razdrobljenosti v EU in izkrivljanj na notranjem trgu. To spremlja še pomanjkanje zaupanja v elektronske sisteme, kar evropske državljane ovira pri koriščenju enakih storitev, ki jih koristijo v resničnem svetu, tudi v digitalnem svetu.

### 1.5.2. *Dodana vrednost ukrepanja Evropske unije*

Ukrepanje na ravni EU bi imelo jasne koristi v primerjavi z ukrepanjem na ravni držav članic. Izkušnje so pokazale, da nacionalni ukrepi niso le nezadostni za omogočanje čezmejnih elektronskih transakcij, temveč so celo ustvarili ovire za vseevropsko interoperabilnost elektronskih podpisov, trenutno pa imajo enak učinek tudi na elektronsko identifikacijo, avtentikacijo in povezane skrbniške storitve.

### 1.5.3. *Glavna spoznanja iz podobnih izkušenj*

Predlog temelji na izkušnjah z direktivo o elektronskem podpisu in težavah, ki so se pojavile zaradi razdrobljenega prenosa in izvajanja navedene direktive ter so preprečile uspešno izpolnitev njenih ciljev.

### 1.5.4. *Skladnost in možnosti dopolnjevanja z drugimi relevantnimi instrumenti*

Direktiva o elektronskem podpisu je povezana z več drugimi pobudami EU, ki so bile oblikovane za odpravo težav z interoperabilnostjo ter reševanje težav s čezmejnimi priznavanjem in sprejemanjem v zvezi z nekaterimi vrstami elektronskih interakcij, npr. z direktivo o storitvah, direktivami o javnih naročilih, revidirano direktivo o DDV (elektronsko izstavljanje računov) in uredbo o evropski državljski pobudi.

Poleg tega bo predlagana uredba zagotovila pravni okvir, ki bo koristil široki uporabi obsežnih pilotnih projektov, ki so bili vzpostavljeni na ravni EU za podporo razvoja interoperabilnih in zanesljivih sredstev elektronske komunikacije (vključno s SPOCS, ki podpira izvajanje direktive o storitvah; STORK, ki podpira razvoj in uporabo eID; PEPPOL, ki podpira razvoj in uporabo interoperabilnih rešitev za e-javna naročila; epSOS, ki podpira razvoj in uporabo interoperabilnih rešitev za e-zdravje; eCODEX, ki podpira razvoj in uporabo interoperabilnih rešitev za e-pravosodje).

## 1.6. **Trajanje ukrepa in finančnih posledic**

**Časovno omejen** predlog/pobuda:

- trajanje predloga/pobude od [DD. MM. ]LLLL do [DD. MM. ]LLLL,
- finančne posledice med letoma LLLL in LLLL.

**Časovno neomejen** predlog/pobuda:

## 1.7. **Načrtovani načini upravljanja<sup>27</sup>**

**Neposredno centralizirano upravljanje** – Komisija

**Posredno centralizirano upravljanje** – prenos izvrševanja na:

- izvajalske agencije,

<sup>27</sup>

Pojasnitve načinov upravljanja in sklicevanje na finančno uredbo so na voljo na spletišču BudgWeb: [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html).

- organe, ki jih ustanovita Skupnosti<sup>28</sup>,
- nacionalne javne organe/organe, ki opravljajo javne storitve,
- osebe, ki se jim zaupa izvedba določenih ukrepov v skladu z naslovom V Pogodbe o Evropski uniji in so določene v zadevnem temeljnem aktu v smislu člena 49 finančne uredbe.

**Deljeno upravljanje** z državami članicami

**Decentralizirano upravljanje** s tretjimi državami

**Skupno upravljanje** z mednarodnimi organizacijami (*navedite*)

*Pri navedbi več kot enega načina upravljanja je treba to natančneje razložiti v oddelku „opombe“.*

Opombe

[//]

---

<sup>28</sup>

Organi iz člena 185 finančne uredbe.

## **2. UKREPI UPRAVLJANJA**

### **2.1. Določbe glede spremljanja in poročanja**

*Navedite pogostost in pogoje.*

Prva ocena se izvede štiri leta po začetku veljavnosti Uredbe. V Uredbo je vključena izrecna določba o poročilu, v skladu s katero bo Komisija Evropskemu parlamentu in Svetu poročala o uporabi Uredbe. Naslednja poročila je treba predložiti vsaka 4 leta. Uporabljena bo metodologija Komisije za ocenjevanje. Ta ocenjevanja bodo izvedena s pomočjo usmerjenih študij o izvajanju pravnih aktov, vprašalnikov, namenjenih nacionalnim organom, razprav strokovnjakov, delavnic, raziskav Eurobarometra itd.

### **2.2. Sistem upravljanja in nadzora**

#### *2.2.1. Ugotovljena tveganja*

Izvedena je bila ocena učinka, ki spremlja predlog uredbe. Novi pravni instrument bo zagotovil čezmejno medsebojno priznavanje in sprejemanje elektronske identifikacije, izboljšal sedanji okvir za elektronski podpis, okreplil nacionalni nadzor ponudnikov skrbniških storitev ter zagotovil pravni učinek in priznavanje povezanih skrbniških storitev. Uvaja tudi uporabo delegiranih in izvedbenih aktov kot mehanizmov za zagotavljanje prilagodljivosti tehnološkemu razvoju.

#### *2.2.2. Načrtovani načini nadzora*

Veljavni načini nadzora, ki jih uporablja Komisija, bodo zajeli dodatne odobritve.

### **2.3. Ukrepi preprečevanja goljufij in nepravilnosti**

*Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe.*

Veljavni ukrepi za preprečevanje goljufij, ki jih uporablja Komisija, bodo zajeli dodatne odobritve.



### 3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

#### 3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

- Obstoječe odhodkovne proračunske vrstice

Po vrsti, v skladu z razdelki večletnega finančnega okvira in proračunskimi vrsticami.

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	Številka [opis.....]	dif./ nedif. <sup>(29)</sup>	držav Efte <sup>30</sup>	držav kandidat <sup>31</sup>	tretjih držav	v smislu člena 18(1)(aa) finančne uredbe
5	09. 01 01 01 Izdatki za aktivno zaposlene v GD za informacijsko družbo in medije	nedif.	NE	NE	NE	NE
5	09. 01 02 01 Zunanji sodelavci	nedif.	NE	NE	NE	NE

<sup>29</sup> Dif. = diferencirana sredstva / nedif. = nediferencirana sredstva.

<sup>30</sup> EFTA: Evropsko združenje za prosto trgovino.

<sup>31</sup> Države kandidatke in, če je primerno, potencialne države kandidatke Zahodnega Balkana.

### 3.2. Ocenjeni učinek na odhodke

#### 3.2.1. Povzetek ocenjenega učinka na odhodke

<b>Razdelek večletnega finančnega okvira:</b>	Številka	[Razdelek 1. Pametna in vključujoča rast .....]
---	----------	--

GD: INFSO			Leto 2014	Leto 2015	Leto 2016	Leto 2017	Leto 2018	Leto 2019	Leto 2020	SKUPAJ
• Odobritve za poslovanje										
Številka proračunske vrstice – n.r.	prevzete obveznosti	(1)	0,000	0,000	0,000	0,000	0,000	0,000	<b>0,000</b>	<b>0,000</b>
	plačila	(2)	0,000	0,000	0,000	0,000	0,000	0,000	<b>0,000</b>	<b>0,000</b>
Številka proračunske vrstice – n.r.	prevzete obveznosti	(1a)	0,000	0,000	0,000	0,000	0,000	0,000	<b>0,000</b>	<b>0,000</b>
	plačila	(2a)	0,000	0,000	0,000	0,000	0,000	0,000	<b>0,000</b>	<b>0,000</b>
Odobritve upravne narave, ki se financirajo iz sredstev nekaterih specifičnih programov <sup>32</sup>			0,000	0,000	0,000	0,000	0,000	0,000	<b>0,000</b>	<b>0,000</b>
Številka proračunske vrstice		(3)	0,000	0,000	0,000	0,000	0,000	0,000	<b>0,000</b>	<b>0,000</b>
<b>Odobritve za DG INFSO SKUPAJ</b>	prevzete obveznosti	=1+1a +3	0,000	0,000	0,000	0,000	0,000	0,000	<b>0,000</b>	<b>0,000</b>
	plačila	=2+2a +3	0,000	0,000	0,000	0,000	0,000	0,000	<b>0,000</b>	<b>0,000</b>

<sup>32</sup> Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

<b>Razdelek večletnega finančnega okvira:</b>	<b>5</b>	„Upravni odhodki“
---	----------	-------------------

v mio. EUR (na tri decimalna mesta natančno)

	Leto 2014	Leto 2015	Leto 2016	Leto 2017	Leto 2018	Leto 2019	Leto 2020	SKUPAJ
GD: INFSO								
• Človeški viri	1 344	1 344	1 344	1 344	1 344	1 344	1 344	9 408
• Drugi upravni odhodki								
<b>GD INFSO SKUPAJ</b>	1 344	1 344	1 344	1 344	1 344	1 344	1 344	9 408
odobritve								

<b>Odobritve za RAZDELEK 5 večletnega finančnega okvira SKUPAJ</b>	(prevzete obveznosti SKUPAJ = plačila SKUPAJ)	1 344	1 344	1 344	1 344	1 344	1 344	1 344	9 408

v mio. EUR (na tri decimalna mesta natančno)

	Leto 2014	Leto 2015	Leto 2016	Leto 2017	Leto 2018	Leto 2019	Leto 2020	SKUPAJ
<b>Odobritve za RAZDELKE od 1 do 5 večletnega finančnega okvira SKUPAJ</b>	prevzete obveznosti	1 344	1 344	1 344	1 344	1 344	1 344	9 408
	plačila	1 344	1 344	1 344	1 344	1 344	1 344	9 408

3.2.2. *Ocenjeni učinek na odobritve za poslovanje*

- Predlog/pobuda ne zahteva porabe odobritev za poslovanje.
- Predlog/pobuda zahteva porabo odobritev za poslovanje, kot je pojasnjeno v nadaljevanju:

### 3.2.3. Ocenjeni učinek na odobritve upravne narave

#### 3.2.3.1. Povzetek

- Predlog/pobuda ne zahteva porabe odobritev za upravne zadeve.
- Predlog/pobuda zahteva porabo odobritev za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

	Leto N 2014	Leto 2015	Leto 2016	Leto 2017	Leto 2018	Leto 2019	Leto 2020	SKUPAJ
--	----------------	--------------	--------------	--------------	--------------	--------------	--------------	--------

<b>RAZDELEK 5 večletnega finančnega okvira</b>								
Človeški viri	1 344	1 344	1 344	1 344	1 344	1 344	1 344	<b>9 408</b>
Drugi upravni odhodki								
<b>Odobritve za RAZDELEK 5 večletnega finančnega okvira</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>9 408</b>

<b>Seštevek za odobritve zunaj RAZDELKA 5<sup>33</sup> večletnega finančnega okvira</b>								
Človeški viri								
Drugi odhodki upravne narave								
<b>Seštevek zunaj RAZDELKA 5 večletnega finančnega okvira</b>								

<b>SKUPAJ</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>1 344</b>	<b>9 408</b>
---------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------

<sup>33</sup>

Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

### 3.2.3.2. Ocenjene potrebe po človeških virih

- Predlog/pobuda ne zahteva porabe človeških virov.
- Predlog/pobuda zahteva porabo človeških virov, kot je pojasnjeno v nadaljevanju:

*ocena, izražena v celih številkah (ali na največ eno decimalno mesto natančno)*

	Leto 2014	Leto 2015	Leto 2016	Leto 2017	Leto 2018	Leto 2019	Leto 2020
<b>• Načrt delovnih mest (za uradnike in začasne uslužbence)</b>							
09 01 01 01 (sedež ali predstavništva Komisije)	9	9	9	9	9	9	9
XX 01 01 02 (delegacije)							
XX 01 05 01 (posredne raziskave)							
10 01 05 01 (neposredne raziskave)							
<b>• Zunanje osebje (v ekvivalentu polnega delovnega časa: EPDČ)<sup>34</sup></b>							
09 01 02 01 (PU, ZU, NNS iz splošnih sredstev)	3	3	3	3	3	3	3
XX 01 02 02 (PU, ZU, MSD, LU in NNS na delegacijah)							
<b>XX 01 04 yy<sup>35</sup></b>	– na sedežu <sup>36</sup>						
	– na delegacijah						
XX 01 05 02 (PU, ZU, NNS za posredne raziskave)							
10 01 05 02 (PU, ZU, NNS za neposredne raziskave)							
Druge proračunske vrstice (navedite)							
<b>SKUPAJ</b>	<b>12</b>	<b>12</b>	<b>12</b>	<b>12</b>	<b>12</b>	<b>12</b>	<b>12</b>

Potrebe po človeških virih se krijejo z osebjem iz GD, že dodeljenim za upravljanje tega ukrepa in/ali prerazporejenim v GD, po potrebi dopolnjenim z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v okviru postopka letne dodelitve virov glede na proračunske omejitve.

Opis nalog:

Uradniki in začasni uslužbenci	Upravljaajo zakonodajne postopke za sprejetje načrtovane uredbe in povezanih delegiranih/izvedbenih aktov s strani EP in Sveta.  Prednostna področja: 1. vzpostavitev novega zakonodajnega okvira o skrbniških elektronskih storitvah; 2. spodbujanje uporabe skrbniških elektronskih storitev z ozaveščanjem MSP in državljanov o njihovem potencialu; 3. spremljanje izvajanja Direktive 1999/93/ES, vključno z mednarodnimi vidiki; 4. spodbujanje obsežnih pilotnih projektov za pospešitev dejanske uresničitve cilja novega zakonodajnega okvira.
Zunanje osebje	Enako kot zgoraj

<sup>34</sup> PU = pogodbeni uslužbenec; ZU = začasni uslužbenec; MSD = mlajši strokovnjak v delegaciji; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak.

<sup>35</sup> V okviru zgornje meje za zunanje sodelavce iz odobritev za poslovanje (prej vrstice BA).

<sup>36</sup> Predvsem strukturni skladi, Evropski kmetijski sklad za razvoj podeželja (EKSRP) in Evropski sklad za ribištvo (ESR).

#### 3.2.4. *Skladnost z veljavnim večletnim finančnim okvirom*

- Predlog/pobuda je skladna z veljavnim večletnim finančnim okvirom.
- Predlog/pobuda bo pomenila spremembo ustreznega razdelka večletnega finančnega okvira.

Pojasnite zahtevano spremembo ter navedite zadevne proračunske vrstice in ustrezne zneske.

- Predlog/pobuda zahteva uporabo instrumenta prilagodljivosti ali spremembe večletnega finančnega okvira<sup>37</sup>.

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice ter ustrezne zneske.

#### 3.2.5. *Udeležba tretjih oseb pri financiranju*

- V predlogu/pobudi ni načrtovano sofinanciranje tretjih oseb.
- V predlogu/pobudi je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

#### 3.3. *Ocenjeni učinek na prihodke*

- Predlog/pobuda nima finančnih posledic za prihodke.
- Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:
  - na lastna sredstva,
  - na razne prihodke.

<sup>37</sup> Glej točki 19 in 24 Medinstitucionalnega sporazuma.