EIROPAS KOMISIJA

Briselē, 4.6.2012.
COM(2012) 238 final

2012/0146 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū

(Dokuments attiecas uz EEZ)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

Šajā paskaidrojuma rakstā ir izklāstīts ierosinātais tiesiskais regulējums, kura mērķis ir stiprināt elektronisko darījumu uzticamību iekšējā tirgū.

Ļoti svarīgs ekonomikas izaugsmes faktors ir uzticēšanās tiešsaistes videi. Uzticēšanās trūkums liek patērētājiem, uzņēmumiem un pārvaldes struktūrām vilcināties ar elektroniskajiem darījumiem tiešsaistē un jaunu pakalpojumu pieņemšanu.

Eiropas digitalizācijas programmā[1] ir uzskaitīti šķēršļi, kas patlaban kavē Eiropas digitālās vides attīstību, kā arī ierosināts tiesību akts par e-parakstu (3. pamatpasākums) un e-identifikācijas un autentifikācijas savstarpēju atzīšanu (16. pamatpasākums), izveidojot skaidru tiesisko regulējumu, lai tādējādi novērstu sadrumstalotību un sadarbspējas trūkumu, veicinātu iedzīvotāju piekļuvi digitālajām tehnoloģijām un novērstu kibernoziedzību. Tādu tiesību aktu pieņemšana, kas nodrošina elektroniskās identifikācijas un autentifikācijas savstarpējo atzīšanu visā Eiropas Savienībā, un Elektroniskā paraksta direktīvas pārskatīšana saistībā ar digitālā vienotā tirgus izveidi ir noteikti par galvenajiem darbības virzieniem arī *Vienotā tirgus aktā*[2]. *Rīcības plānā stabilitātei un izaugsmei*[3] uzsvērts, ka digitālās ekonomikas attīstībā būtiska nozīme ir turpmākam kopējam tiesiskajam regulējumam attiecībā uz elektroniskās identifikācijas un autentifikācijas savstarpēju atzīšanu un akceptēšanu pārrobežu līmenī.

Ierosinātais tiesiskais regulējums, proti, *Eiropas Parlamenta un Padomes regula par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū*, paredz nodrošināt, ka uzņēmumi, iedzīvotāji un publiskā sektora iestādes var droši un netraucēti veikt savstarpējus elektroniskus darījumus, tādējādi Eiropas Savienībā palielinot publiskā un privātā sektora tiešsaistes pakalpojumu, e-uzņēmējdarbības un elektroniskās tirdzniecības efektivitāti.

Spēkā esošie ES tiesību akti, proti, Direktīva 1999/93/EK par *Kopienas elektronisko parakstu sistēmu*[4], būtībā attiecas tikai uz elektroniskajiem parakstiem. Šajā jomā nav ieviests visaptverošs ES pārrobežu un starpnozaru regulējums drošiem, uzticamiem un viegli lietojamiem elektronisko darījumu mehānismiem, kas ietver gan elektronisko identifikāciju un autentifikāciju, gan elektroniskos parakstus.

Mērķis ir uzlabot spēkā esošos tiesību aktus, piemērošanas jomā ietverot arī paziņoto elektroniskās identifikācijas shēmu un ar tām saistīto citu nozīmīgu elektronisko uzticamības pakalpojumu savstarpēju atzīšanu un akceptēšanu ES līmenī.

---

1 COM(2010) 245, 19.5.2010.

2 COM(2011) 206 galīgā redakcija, 13.4.2011.

3 COM(2011) 669, 12.10.2011.

4 OV L 13, 19.1.2000., 12. lpp.

2. APSPRIEŠANĀS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

Šī iniciatīva ir tapusi pēc plašas apspriešanās, kuras laikā tika pārskatīts pašreizējais tiesiskais regulējums elektronisko parakstu jomā, Komisijai apkopojot dalībvalstu, Eiropas Parlamenta un citu ieinteresēto personu atsauksmes[5]. Lai apzinātu mazo un vidējo uzņēmumu (MVU) viedokli un īpašās vajadzības, papildus tiešsaistes sabiedriskajai apspriešanai tika izveidota MVU konsultatīvā grupa, turklāt mērķtiecīgas apspriešanās tika noorganizētas ar ieinteresētajām personām[6,7]. Komisija arī uzsāka vairākus pētījumus par elektronisko identifikāciju un autentifikāciju un elektroniskajiem parakstiem, kā arī saistītajiem uzticamības pakalpojumiem (*eIAS*).

Apspriešanās laikā tika noskaidrots, ka lielākā daļa ieinteresēto personu ir vienisprātis par to, ka jāpārskata pašreizējais regulējums, lai novērstu nepilnības, kas pieļautas Elektroniskā paraksta direktīvā. Tika atzīts, ka tas būtu piemērotāks risinājums problēmām, ko radījusi jauno tehnoloģiju straujā attīstība (it īpaši interneta un mobilo sakaru pieejamības jomā) un pieaugošā globalizācija, taču vienlaikus būtu jāsaglabā tiesiskā regulējuma neitralitāte attiecībā uz tehnoloģijām.

Saskaņā ar savu labāka regulējuma politiku Komisija veica alternatīvu politikas pasākumu ietekmes novērtējumu. Tika izvērtēti trīs politisko risinājumu kopumi, proti, 1) jaunā regulējuma piemērošanas joma, 2) tiesību akts un 3) vajadzīgais uzraudzības līmenis[8]. Tika konstatēts, ka izvēlētais politiskais risinājums sekmē tiesisko noteiktību, uzlabo valsts līmeņa uzraudzības koordināciju un nodrošina elektroniskās identifikācijas shēmu savstarpēju atzīšanu un akceptēšanu, kā arī paplašina piemērošanas jomu, ietverot nozīmīgus saistītos uzticamības pakalpojumus. Ietekmes novērtējumā secināts, ka, izmantojot šādu pieeju, izdotos panākt ievērojamus uzlabojumus attiecībā uz tiesisko noteiktību, drošumu un uzticamību pārrobežu elektronisko darījumu jomā, tādējādi samazinot tirgus sadrumstalotību.

3. PRIEKŠLIKUMA JURIDISKIE ASPEKTI

3.1. Juridiskais pamats

Šis priekšlikums sagatavots, pamatojoties uz LESD 114. pantu, kas attiecas uz noteikumu pieņemšanu, lai novērstu pašreizējos šķēršļus iekšējā tirgus darbībai. Iedzīvotāji, uzņēmumi un pārvaldes struktūras varēs izmantot priekšrocības, ko sniedz elektroniskās identifikācijas un autentifikācijas un elektronisko parakstu, kā arī citu uzticamības pasākumu savstarpējā

---

5 Sīkāka informācija par apspriešanos: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision.

6 Darbseminārs ieinteresētajām personām tika noorganizēts 2011. gada 10. martā, piedaloties pārstāvjiem no publiskā un privātā sektora un akadēmiskajām aprindām, lai apspriestu, kādi tiesību akti ir vajadzīgi turpmāko uzdevumu risināšanai. Tas tika noorganizēts kā interaktīvs forums, kurā notika viedokļu apmaiņa un tika apzinātas dažādas nostājas par sabiedriskajā apspriešanā aktualizētajiem jautājumiem. Lai arī sākotnēji tas nebija plānots, vairākas organizācijas nosūtīja rakstiski formulētu nostāju.

7 Konkrēti – Polijas ES prezidentūra organizēja tikšanās ar dalībvalstu pārstāvjiem; 2011. gada 9. novembrī Varšavā notika elektroniskajam parakstam veltīta tikšanās, bet 2011. gada 17. novembrī Poznaņā – elektroniskajai identifikācijai veltīta tikšanās. Savukārt 2012. gada 25. janvārī Komisija rīkoja darbsemināru ar dalībvalstu pārstāvjiem, lai apspriestu pārējos jautājumus, kas saistīti ar elektronisko identifikāciju un autentifikāciju un elektronisko parakstu.

8 Pirmajā kopumā tika izvērtēti četri risinājumi: atcelt E-paraksta direktīvu; politikās izmaiņas neveikt; sekmēt tiesisko noteiktību, uzlabot valsts līmeņa uzraudzības koordināciju un nodrošināt elektroniskās identifikācijas sistēmu savstarpēju atzīšanu un akceptēšanu visā Eiropas Savienībā; un, ceturtkārt, paplašināt piemērošanas jomu, ietverot saistītos uzticamības pakalpojumus. Otrajā kopumā tika izvērtētas tās relatīvās priekšrocības, ko sniedz regulējums, izmantojot vienu vai divus instrumentus un izvēloties direktīvu regulas vietā. Trešajā kopumā tika izvērtētas iespējas, ko sniedz tādu valsts uzraudzības shēmu īstenošana, kuru pamatā ir kopējas būtiskas uzraudzības prasības, nevis ES mēroga uzraudzības sistēma. Šajā darbā piedaloties grupai, kurā apvienojušies visi ieinteresētie Komisijas ģenerāldirektorāti, tika izvērtēti visi politiskie risinājumi, ņemot vērā to lietderību politisko mērķu sasniegšanā, ekonomisko ietekmi uz ieinteresētajām personām (tostarp ES iestāžu budžetu), ietekmi sociālajā un vides jomā, kā arī sekām saistībā ar administratīvo slogu.

atzīšana un akceptēšana pārrobežu līmenī, ja tas vajadzīgs, lai veiktu vai pabeigtu elektroniskās procedūras vai darījumus.

Regula tiek uzskatīta par vispiemērotāko tiesību aktu. Regulas tiešā piemērojamība saskaņā ar LESD 288. pantu samazinās tiesisko sadrumstalotību un nodrošinās lielāku tiesisko noteiktību, ieviešot galveno noteikumu harmonizētu kopumu un sekmējot vienotā tirgus darbību.

3.2. Subsidiaritāte un proporcionalitāte

Lai ES rīcība būtu pamatota, jāievēro subsidiaritātes princips.

a) Problēmas transnacionālais raksturs (nepieciešamības pārbaude)

Ņemot vērā *eIAS* transnacionālo raksturu, ir nepieciešama ES rīcība. Ar iekšējiem jeb valsts līmeņa pasākumiem vien neizdotos ne sasniegt mērķus, ne arī īstenot uzdevumus, kas izklāstīti *stratēģijā „Eiropa 2020”*[9]. Tieši pretēji – pieredze ir pierādījusi, ka valsts pasākumi faktiski ir radījuši šķēršļus elektronisko parakstu sadarbspējai ES mērogā un ka patlaban tie tieši tādā pašā veidā ietekmē elektronisko identifikāciju, elektronisko autentifikāciju un saistītos uzticamības pakalpojumus. Tādēļ Eiropas Savienībai jāizveido regulējums, ar kura palīdzību varētu atrisināt jautājumu par pārrobežu sadarbspēju un uzlabot valsts uzraudzības shēmu koordināciju. Tomēr ierosinātajā regulā elektronisko identifikāciju nevar reglamentēt tikpat vispārēji, kā tas tiek darīts attiecībā uz citiem elektroniskajiem uzticamības pakalpojumiem, jo identifikācijas līdzekļu izsniegšana ir valsts prerogatīva. Tādēļ priekšlikumā uzmanība cieši pievērsta elektroniskās identifikācijas pārrobežu aspektiem.

Ar ierosināto regulu tiek izveidoti vienlīdzīgi konkurences apstākļi uzņēmumiem uzticamības pakalpojumu jomā, kurā pašreizējās atšķirības valsts tiesību aktos bieži rada tiesisko nenoteiktību un papildu slogu. Tiesiskā noteiktība ir ievērojami palielinājies, jo dalībvalstis uzņēmušās skaidri noteiktas akceptēšanas saistības kvalificētu uzticamības pakalpojumu jomā, un tas savukārt uzņēmumiem būs papildu stimuls paplašināt savu darbību ārzemēs. Piemēram, uzņēmums varēs elektroniski iesniegt pieteikumu atklātā konkursā, ko izsludinājusi citas dalībvalsts pārvaldes struktūra, un tā elektroniskais paraksts netiks bloķēts specifisku valsts prasību vai sadarbspējas problēmu dēļ. Tāpat, darījumu partnerim atrodoties citā dalībvalstī, uzņēmums varēs parakstīt līgumus elektroniski, nebaidoties par atšķirīgām juridiskām prasībām attiecībā uz uzticamības pakalpojumiem, piemēram, elektroniskajiem zīmogiem, elektroniskajiem dokumentiem vai laika zīmogiem. Turklāt paziņojumi par saistību neizpildi tiks pārsūtīti no vienas dalībvalsts uz citu ar pārliecību par tā juridisko derīgumu abās dalībvalstīs. Visbeidzot, tirdzniecība tiešsaistē būs uzticamāka, jo pircējiem būs līdzekļi, kurus izmantojot, tie varēs pārliecināties, ka patiešām atrodas tajā tirgotāja tīmekļa vietnē, ko tie izvēlējušies, nevis iespējami viltotā tīmekļa vietnē.

Savstarpēji atzīti elektroniskās identifikācijas līdzekļi un plaši akceptēti elektroniskie paraksti atvieglos daudzu pārrobežu pakalpojumu sniegšanu iekšējā tirgū un ļaus uzņēmumiem paplašināt savu darbību pāri robežām, neliekot tiem pārvarēt šķēršļus saskarsmē ar publiskā sektora iestādēm. Praksē gan uzņēmumi, gan iedzīvotāji varēs ievērojami efektīvāk nokārtot administratīvās formalitātes. Piemēram, studenti varēs elektroniski pieteikties studijām ārzemēs, iedzīvotāji varēs tiešsaistē iesniegt nodokļu deklarācijas citā dalībvalstī, bet pacientiem būs tiešsaistē pieejama viņu medicīniskā dokumentācija. Ja netiks ieviesta šādu

[9] Komisijas 2010. gada 3. marta paziņojums *„Eiropa 2020. Stratēģija gudrai, ilgtspējīgai un integrējošai izaugsmei”*, COM(2010) 2020.

elektroniskās identifikācijas līdzekļu savstarpēja atzīšana, ārsts nevarēs piekļūt pacienta ārstēšanā vajadzīgajiem medicīniskajiem datiem, un pacientam būs atkārtoti jāveic medicīniskās un laboratoriskās pārbaudes.

b) Pievienotā vērtība (efektivitātes pārbaude)

Iepriekš izklāstītos mērķus patlaban nav iespējams sasniegt ar dalībvalstu brīvprātīgu koordināciju, un arī turpmāk to īstenošana nav paredzama. Šāda pieeja nozīmē darbu pārklāšanos, atšķirīgu standartu ieviešanu, IKT radītās plašākas ietekmes transnacionālo raksturu un sarežģītas administratīvās procedūras šādā koordinācijā, kuru iedibina, slēdzot divpusējas un daudzpusējas vienošanās.

Turklāt, ņemot vērā, ka jāatrisina tādas problēmas kā: a) tiesiskās noteiktības trūkums dažādo valsts noteikumu dēļ, ko savukārt radījusi Elektroniskā paraksta direktīvas atšķirīgā interpretācija, un b) valsts līmenī izveidoto elektronisko parakstu sistēmu nepietiekama sadarbspēja atšķirīgi piemēroto tehnisko standartu dēļ, ES dalībvalstu starpā jāievieš tāda koordinācijas sistēma, kas būtu efektīvāka ES līmenī.

3.3. Sīks priekšlikuma pārskats

3.3.1. I NODAĻA – VISPĀRĪGI NOTEIKUMI

Regulas 1. pantā definēts regulas priekšmets.

Regulas 2. pantā definēta regulas materiālā piemērošanas joma.

Regulas 3. pantā ietvertas regulā izmantoto terminu definīcijas. Dažas definīcijas ir pārņemtas no Direktīvas 1999/93/EK, bet citas ir precizētas, papildinātas vai ieviestas no jauna.

Regulas 4. pantā ir noteikti iekšējā tirgus principi attiecībā uz regulas teritoriālo piemērošanas jomu. Skaidri norādīts, ka pakalpojumu sniegšanas brīvībai un preču brīvai apritei netiek piemēroti ierobežojumi.

3.3.2. II NODAĻA – ELEKTRONISKĀ IDENTIFIKĀCIJA

Regulas 5. pantā paredzēta tādā shēmā ietverto elektroniskās identifikācijas līdzekļu savstarpējā atzīšana un akceptēšana, par kuru Komisijai tiks paziņots atbilstīgi šajā regulā izklāstītajiem nosacījumiem. Lielākā daļa dalībvalstu ir ieviesusi tādu vai citādu elektroniskās identifikācijas sistēmu. Tomēr tās atšķiras vairākos aspektos. Gan tas, ka nav kopēja juridiskā pamata, kuram atbilstīgi dalībvalstīm jāatzīst un jāakceptē elektroniskās identifikācijas līdzekļi, kas izsniegti citās dalībvalstīs tiešsaistes pakalpojumu piekļuvei, gan arī valstu elektroniskās identifikācijas sistēmu nepietiekamā pārrobežu sadarbspēja rada šķēršļus, iedzīvotājiem un uzņēmumiem liedzot pilnībā izmantot digitālā vienotā tirgus priekšrocības. Savstarpēji atzīstot un akceptējot saskaņā ar šo regulu paziņotajā shēmā ietvertos elektroniskās identifikācijas līdzekļus, šie juridiskie šķēršļi tiek likvidēti.

Regula neuzliek dalībvalstīm pienākumu ieviest elektroniskās identifikācijas shēmas vai paziņot par tām, bet gan nosaka, ka dalībvalstīm jāatzīst un jāakceptē paziņotās elektroniskās identifikācijas shēmas saistībā ar tiem tiešsaistes pakalpojumiem, kuru piekļuvei valsts līmenī ir jāizmanto šāda identifikācija. Apjomradīto ietaupījumu iespējamais palielinājums, kas tiktu panākts ar paziņoto elektroniskās identifikācijas līdzekļu un autentifikācijas sistēmu pārrobežu izmantošanu, varētu mudināt dalībvalstis paziņot par savām elektroniskās

identifikācijas shēmām. Regulas 6. pantā ir minēti pieci nosacījumi elektroniskās identifikācijas shēmu paziņošanai.

Dalībvalstis var paziņot par tām elektroniskās identifikācijas shēmām, ko tās akceptē savā jurisdikcijā, ja elektroniskā identifikācija ir nepieciešama sabiedrisko pakalpojumu jomā. Papildus noteikta prasība, ka attiecīgie elektroniskās identifikācijas līdzekļi jāizsniedz tajā dalībvalstī, kura paziņo par shēmu, vai arī jāizsniedz šīs dalībvalsts vārdā, vai vismaz – tai uzņemoties atbildību.

Dalībvalstīm jānodrošina, ka elektroniskās identifikācijas dati ir nepārprotami saistīti ar attiecīgo personu. Šis pienākums nenozīmē, ka personai nevar būt vairāki elektroniskās identifikācijas līdzekļi, taču tiem jābūt saistītiem ar vienu un to pašu personu.

Elektroniskās identifikācijas uzticamība ir atkarīga no autentifikācijas līdzekļu pieejamības (t.i., no iespējas pārbaudīt elektroniskās identifikācijas datu derīgumu). Regulā noteikts, ka paziņotājām dalībvalstīm ir pienākums nodrošināt trešo pušu bezmaksas autentifikāciju tiešsaistē. Autentifikācijas iespējai jābūt izmantojamai nepārtraukti. Pusēm, kuras izmanto šo autentifikāciju, nevar noteikt īpašas tehniskas prasības, piemēram, saistībā ar aparatūru vai programmatūru. Šo noteikumu nepiemēro prasībām, kas noteiktas elektroniskās identifikācijas līdzekļu lietotājiem (turētājiem) un kas elektroniskās identifikācijas līdzekļu, piemēram, karšu lasītāju, lietošanai ir nepieciešamas no tehniskā viedokļa.

Dalībvalstīm jāuzņemas atbildība par nepārprotamas saiknes izveidi (t.i., apliecinot, ka personai piešķirtie identifikācijas dati nav saistīti ar citu personu) un autentifikācijas iespēju (t.i., iespēju pārbaudīt elektroniskās identifikācijas datu derīgumu). Dalībvalstu atbildība neattiecas uz citiem identifikācijas procesa aspektiem vai darījumiem, kuros nepieciešama identifikācija.

Regulas 7. pantā izklāstīti noteikumi par to, kā Komisijai tiek paziņots par elektroniskās identifikācijas shēmām.

Regulas 8. panta mērķis ir nodrošināt paziņoto identifikācijas shēmu tehnisko sadarbspēju, izmantojot saskaņotu pieeju, tostarp deleģētos aktus.

3.3.3. III NODAĻA – UZTICAMĪBAS PAKALPOJUMI

3.3.3.1. – 1. iedaļa – Vispārīgi noteikumi

Regulas 9. pantā noteikti gan nekvalificētu, gan kvalificētu uzticamības pakalpojumu sniedzēju atbildības principi. Ar šo pantu, kura pamatā izmantots Direktīvas 1999/93/EK 6. pants, ir paplašinātas tiesības uz kompensāciju par zaudējumiem, ko nodarījis jebkurš uzticamības pakalpojumu sniedzējs, kurš nav ievērojis labu praksi drošības jomā, tādējādi pārkāpjot drošības prasības un būtiski ietekmējot pakalpojumus.

Regulas 10. pantā aprakstīts tādu kvalificētu uzticamības pakalpojumu atzīšanas un akceptēšanas mehānisms, ko sniedz trešā valstī reģistrēts pakalpojumu sniedzējs. Šajā pantā, kura pamatā izmantots Direktīvas 1999/93/EK 7. pants, ir saglabāts vienīgais praktiski īstenojamais risinājums, proti, šādu atzīšanu atļaut saskaņā ar starptautiskiem nolīgumiem starp Eiropas Savienību un trešām valstīm vai starptautiskām organizācijām.

Regulas 11. pantā izklāstīti datu aizsardzības un minimizēšanas principi. Tā pamatā izmantots Direktīvas 1999/93/EK 8. pants.

Regulas 12. pantā noteikta uzticamības pakalpojumu pieejamība personām ar invaliditāti.

3.3.3.2. – 2. iedaļa – Uzraudzība

Regulas 13. pantā, pamatojoties uz Direktīvas 1999/93/EK 3. panta 3. punktu, dalībvalstīm noteikts pienākums izveidot uzraudzības iestādes, precizējot un paplašinot to darbības jomu attiecībā gan uz uzticamības pakalpojumu sniedzējiem, gan kvalificētiem uzticamības pakalpojumu sniedzējiem.

Ar regulas 14. pantu ir ieviests skaidrs savstarpējās palīdzības mehānisms, kas dalībvalstīs izmantojams uzraudzības iestāžu starpā, lai atvieglotu uzticamības pakalpojumu sniedzēju pārrobežu uzraudzību. Šajā pantā ieviesti noteikumi par kopīgām operācijām un uzraudzības iestāžu tiesībām piedalīties šādās operācijās.

Regulas 15. pantā ir ieviests pienākums gan kvalificētiem, gan nekvalificētiem uzticamības pakalpojumu sniedzējiem veikt atbilstīgus tehniskus un organizatoriskus pasākumus, kas vajadzīgi saistībā ar viņu darbības drošību. Turklāt kompetentās uzraudzības iestādes un citas attiecīgās iestādes ir jāinformē par drošības prasību pārkāpumiem. Savukārt tās, ja vajadzīgs, informēs citu dalībvalstu uzraudzības iestādes un tieši vai ar attiecīgā uzticamības pakalpojumu sniedzēja starpniecību informēs sabiedrību.

Regulas 16. pantā ir izklāstīti kvalificētu uzticamības pakalpojumu sniedzēju un to sniegto kvalificētu uzticamības pakalpojumu uzraudzības nosacījumi. Šajā pantā noteikts, ka atzītai neatkarīgai iestādei reizi gadā jāpārbauda kvalificēti uzticamības pakalpojumu sniedzēji, lai uzraudzības iestādei apstiprinātu, ka tie pilda šajā regulā izklāstītos pienākumus. Turklāt 16. panta 2. punktā uzraudzības iestādei piešķirtas tiesības veikt revīziju uz vietas, kvalificētos uzticamības pakalpojumu sniedzējus pārbaudot jebkurā laikā. Uzraudzības iestāde ir arī pilnvarota izdot saistošus norādījumus kvalificētiem uzticamības pakalpojumu sniedzējiem, lai, ievērojot samērības principu, labotu jebkuru drošības revīzijā atklātu pienākumu neizpildi.

Regulas 17. pants attiecas uz uzraudzības iestādes darbību, kas veikta pēc tāda uzticamības pakalpojumu sniedzēja pieprasījuma, kurš vēlas sākt kvalificētu uzticamības pakalpojumu sniegšanu.

Regulas 18. pantā ir paredzēts izveidot uzticamības sarakstus[10], kuros ietverta informācija par kvalificētiem uzticamības pakalpojumu sniedzējiem, kas tiek uzraudzīti, un to piedāvātajiem kvalificētajiem pakalpojumiem. Lai veicinātu šādas informācijas automatizētu izmantošanu un nodrošinātu pietiekamu precizitātes līmeni, tā jāpublisko, izmantojot vienotu paraugu.

Regulas 19. pantā noteiktas prasības, kuras kvalificētajiem uzticamības pakalpojumu sniedzējiem jāizpilda, lai tie tiktu par tādiem atzīti. Tā pamatā izmantots Direktīvas 1999/93/EK II pielikums.

3.3.3.3. – 3. iedaļa – Elektroniskais paraksts

Regulas 20. pantā iekļauti noteikumi par fizisko personu elektronisko parakstu juridisko spēku. Ar to ir precizēts un paplašināts Direktīvas 1999/93/EK 5. pants, ieviešot skaidru pienākumu kvalificētiem elektroniskajiem parakstiem noteikt tādu pašu juridisko spēku, kāds ir parakstiem ar roku. Turklāt dalībvalstīm jānodrošina kvalificētu elektronisko parakstu

[10] Jaunu Komisijas lēmumu par uzticamības sarakstiem saskaņā ar šo regulu sagatavo, pamatojoties uz uzticamības sarakstiem, kas izveidoti ar Komisijas Lēmumu 2009/767/EK, kurā grozījumi izdarīti ar Komisijas Lēmumu 2010/425/ES.

pārrobežu akceptēšana sabiedrisko pakalpojumu jomā, un tās nedrīkst ieviest papildu prasības, kas varētu radīt šķēršļus šādu parakstu izmantošanai.

Regulas 21. pantā ir noteiktas prasības kvalificētiem e-paraksta sertifikātiem. Tajā precizēts Direktīvas 1999/93/EK I pielikums un svītroti noteikumi, kuri praksē nav izrādījušies lietderīgi (piemēram, ierobežojumi attiecībā uz darījumu vērtību).

Regulas 22. pantā ir noteiktas prasības kvalificētām elektroniskā paraksta radīšanas ierīcēm. Tajā precizētas prasības drošām paraksta radīšanas ierīcēm, kuras minētas Direktīvas 1999/93/EK 3. panta 5. punktā un kuras tagad saskaņā ar šo regulu jāuzskata par kvalificētām paraksta radīšanas ierīcēm. Šajā pantā arī precizēts, ka paraksta radīšanas ierīces var definēt daudz plašāk, neaprobežojoties tikai ar paraksta radīšanas datu uzglabāšanas ierīci. Komisija var arī izveidot sarakstu ar šo ierīču drošības prasību standartu identifikācijas numuriem.

Pamatojoties uz Direktīvas 1999/93/EK 3. panta 4. punktu, regulas 23. pantā ir ieviests kvalificētu paraksta radīšanas ierīču sertificēšanas jēdziens, lai noteiktu to atbilstību II pielikumā uzskaitītajām drošības prasībām. Visām dalībvalstīm ir jāatzīst šīs ierīces un gadījumā, ja dalībvalsts izraudzīta sertifikācijas iestāde veic sertificēšanas procedūru, tās jāuzskata par prasībām atbilstošām. Komisija publicēs sarakstu, kurā būs uzskaitītas atļautās un atbilstīgi 24. pantam sertificētās ierīces. Komisija var arī izveidot sarakstu ar standartu identifikācijas numuriem saistībā ar to informācijas tehnoloģiju produktu drošības prasību novērtējumu, kas minēti 23. panta 1. punktā.

Regulas 24. pants attiecas uz Komisijas pienākumu publicēt kvalificētu elektroniskā paraksta radīšanas ierīču sarakstu pēc tam, kad dalībvalstis nosūtījušas paziņojumu par atbilstību.

Regulas 25. pantā, kura pamatā izmantoti Direktīvas 1999/93/EK IV pielikuma ieteikumi, noteiktas saistošas prasības kvalificētu elektronisko parakstu validācijai, lai tādējādi palielinātu šādas validēšanas tiesisko noteiktību.

Regulas 26. pantā ir noteikti nosacījumi attiecībā uz kvalificētiem validēšanas pakalpojumiem.

Savukārt 27. pantā ir paredzēts nosacījums attiecībā uz kvalificētu elektronisko parakstu ilgtermiņa saglabāšanu. Tā ir iespējama, izmantojot tādas procedūras un tehnoloģijas, ar kurām var nodrošināt kvalificētā elektroniskā paraksta validācijas datu uzticamību ilgāk par to tehnoloģiskā derīguma termiņu, gadījumā, ja tie kļūst kibernoziedzniekiem vienkārši viltojami.

3.3.3.4. – 4. iedaļa – Elektroniskais zīmogs

Regulas 28. pants attiecas uz juridisko personu elektronisko zīmogu juridisko spēku. Attiecībā uz kvalificētu elektronisko zīmogu pastāv īpaša juridiskā prezumpcija, garantējot to elektronisko dokumentu izcelsmi un integritāti, ar kuriem tas ir saistīts.

Regulas 29. pantā ir noteiktas prasības kvalificētiem elektroniskā zīmoga sertifikātiem.

Regulas 30. pantā ir noteiktas prasības kvalificēto elektroniskā zīmoga radīšanas ierīču saraksta sertificēšanai un publicēšanai.

Regulas 31. pantā ir paredzēts nosacījums attiecībā uz kvalificētu elektronisko zīmogu validāciju un saglabāšanu.

3.3.3.5. – 5. iedaļa – Elektroniskais laika zīmogs

Regulas 32. pants attiecas uz elektronisko laika zīmogu juridisko spēku. Attiecībā uz kvalificētiem elektroniskajiem laika zīmogiem pastāv īpaša juridiskā prezumpcija par konkrētu laiku.

Regulas 33. pantā ir noteiktas prasības kvalificētiem elektroniskajiem laika zīmogiem.

3.3.3.6. – 6. iedaļa – Elektroniskie dokumenti

Regulas 34. pants ir saistīts ar elektronisko dokumentu akceptēšanas juridiskajām sekām un nosacījumiem. Attiecībā uz visu to elektronisko dokumentu autentiskumu un integritāti, kuri parakstīti ar kvalificētu elektronisko parakstu vai apzīmogoti ar kvalificētu elektronisko zīmogu, pastāv īpaša juridiskā prezumpcija. Attiecībā uz elektronisko dokumentu akceptēšanu noteikts, ka tad, ja sabiedrisko pakalpojumu sniegšanas nolūkā ir jāiesniedz dokumenta oriģināls vai apliecināta kopija, tad citā dalībvalstī bez papildu prasībām jāakceptē vismaz tādi elektroniski dokumenti, ko izsniegušas personas, kuras ir pilnvarotas izsniegt attiecīgos dokumentus, un kas atzīti par oriģināliem vai apliecinātām kopijām saskaņā ar izcelsmes dalībvalsts tiesību aktiem.

3.3.3.7. – 7. iedaļa – Elektroniskie piegādes pakalpojumi

Regulas 35. pants attiecas uz to datu juridisko spēku, kas nosūtīti vai saņemti, izmantojot elektroniskos piegādes pakalpojumus. Kvalificētu elektronisko piegādes pakalpojumu jomā ir garantēta īpaša juridiskā prezumpcija attiecībā uz nosūtīto vai saņemto datu integritāti un datu nosūtīšanas vai saņemšanas laika precizitāti. Tajā arī nodrošināta kvalificētu elektronisko piegādes pakalpojumu savstarpējā atzīšana ES līmenī.

Regulas 36. pantā ir noteiktas prasības kvalificētiem elektroniskajiem piegādes pakalpojumiem.

3.3.3.8. – 8. iedaļa – Tīmekļa vietņu autentifikācija

Šīs iedaļas mērķis ir nodrošināt, ka attiecībā uz vietnes īpašnieku tiek garantēts tīmekļa vietnes autentiskums.

Regulas 37. pantā ir noteiktas prasības kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem, ko var izmantot, lai garantētu tīmekļa vietnes autentiskumu. Kvalificēts tīmekļa vietņu autentifikācijas sertifikāts nodrošinās uzticamas informācijas minimumu tīmekļa vietnē un šīs vietnes īpašnieka juridisko pastāvēšanu.

3.3.4. IV NODAĻA – DELEĢĒTIE AKTI

Regulas 38. pantā ietverti standarta noteikumi par deleģēšanu saskaņā ar LESD 290. pantu (deleģētie akti). Minētais pants ļauj likumdevējam deleģēt Komisijai pilnvaras pieņemt vispārēji piemērojamus neleģislatīvus aktus, lai papildinātu vai grozītu dažus nebūtiskus leģislatīvu aktu elementus.

3.3.5. V NODAĻA – ĪSTENOŠANAS AKTI

Regulas 39. pantā ietverts noteikums par komiteju procedūru, kas nepieciešama, lai piešķirtu Komisijai īstenošanas pilnvaras gadījumos, kad saskaņā ar LESD 291. pantu ir nepieciešami vienoti nosacījumi juridiski saistošo Savienības aktu īstenošanai. Piemēro pārbaudes procedūru.

3.3.6. VI NODAĻA – NOSLĒGUMA NOTEIKUMI

Regulas 40. pantā Komisijai uzlikts pienākums novērtēt regulas darbību un iesniegt ziņojumus par tās konstatētajiem faktiem.

Ar regulas 41. pantu ir atcelta Direktīva 1999/93/EK un paredzēta pašreizējās elektroniskā paraksta infrastruktūras vienmērīga pārveidošana atbilstīgi jaunajām regulas prasībām.

Regulas 42. pantā noteikta regulas spēkā stāšanās diena.

4. IETEKME UZ BUDŽETU

Priekšlikuma īpašā ietekme uz budžetu saistīta ar Eiropas Komisijas uzdevumiem, un tā sīkāk raksturota priekšlikuma finanšu pārskatā, kas pievienots šim priekšlikumam.

Priekšlikums neietekmē darbības izdevumus.

Tiesību akta priekšlikuma finanšu pārskatā, kas pievienots šīs regulas priekšlikumam, apskatīta ietekme uz budžetu attiecībā uz šo regulu.

2012/0146 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 114. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[11],

pēc apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju[12],

saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Ļoti svarīgs ekonomikas izaugsmes faktors ir uzticēšanās tiešsaistes videi. Uzticēšanās trūkums liek patērētājiem, uzņēmumiem un pārvaldes struktūrām vilcināties ar elektroniskajiem darījumiem tiešsaistē un jaunu pakalpojumu pieņemšanu.

(2) Šīs regulas mērķis ir stiprināt elektronisko darījumu uzticamību iekšējā tirgū, uzņēmumiem, iedzīvotājiem un publiskā sektora iestādēm dodot iespēju droši un netraucēti veikt savstarpējus elektroniskus darījumus un tādējādi palielinot publiskā un privātā sektora tiešsaistes pakalpojumu, elektroniskās uzņēmējdarbības un elektroniskās tirdzniecības efektivitāti Eiropas Savienībā.

(3) Eiropas Parlamenta un Padomes 1999. gada 13. decembra Direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu[13] būtībā attiecas tikai uz elektroniskajiem parakstiem, un ar to nav ieviests visaptverošs ES pārrobežu un starpnozaru regulējums drošiem, uzticamiem un viegli lietojamiem elektronisko darījumu mehānismiem. Šī regula stiprina un paplašina direktīvā paredzēto *acquis*.

---

11 OV C […], […], […] lpp.

12 OV C […], […], […] lpp.

13 OV L 13, 19.1.2000., 12. lpp.

(4) Komisijas sagatavotajā Eiropas digitalizācijas programmā[14] ir konstatēta digitālā tirgus sadrumstalotība, sadarbspējas trūkums un aizvien pieaugoša kibernoziedzība – tie ir galvenie šķēršļi, kas traucē izveidot pozitīvu attīstības ciklu Eiropas digitālajā ekonomikā. Savā 2010. gada ziņojumā par pilsonību Komisija vēl vairāk uzsvēra vajadzību atrisināt galvenās problēmas, kas Eiropas pilsoņiem liedz izmantot digitālā vienotā tirgus un pārrobežu digitālo pakalpojumu sniegtās priekšrocības[15].

(5) Eiropadome aicināja Komisiju izveidot digitālo vienoto tirgu līdz 2015. gadam[16], lai panāktu strauju progresu galvenajās digitālās ekonomikas jomās un veicinātu pilnībā integrētu digitālo vienoto tirgu[17], sekmējot tiešsaistes pakalpojumu pārrobežu izmantošanu un īpašu uzmanību pievēršot drošai elektroniskajai identifikācijai un autentifikācijai.

(6) Padome aicināja Komisiju sniegt ieguldījumu digitālā vienotā tirgus izveidē, radot piemērotus apstākļus tādu svarīgāko katalizatoru savstarpējai pārrobežu atzīšanai kā elektroniska identifikācija, elektroniski dokumenti, elektroniski paraksti un elektroniski piegādes pakalpojumi, kā arī piemērotus apstākļus e-pārvaldes pakalpojumu sadarbspējai visā Eiropas Savienībā[18].

(7) Eiropas Parlaments uzsvēra, cik nozīmīga ir elektronisko pakalpojumu drošība, īpaši elektronisko parakstu drošība, norādot, ka nepieciešams izveidot publiskās atslēgas infrastruktūru (*PKI*) visā Eiropā, un aicināja Komisiju izveidot Eiropas Validācijas iestāžu vārteju, lai nodrošinātu elektronisko parakstu pārrobežu sadarbspēju un palielinātu internetā veikto darījumu drošību[19].

(8) Eiropas Parlamenta un Padomes 2006. gada 12. decembra Direktīvā 2006/123/EK par pakalpojumiem iekšējā tirgū[20] noteikts, ka dalībvalstīm jāizveido vienotie kontaktpunkti, lai visas procedūras un formalitātes saistībā ar piekļuvi pakalpojumiem vai to veikšanu varētu viegli veikt no attāluma un elektroniski attiecīgajā vienotajā kontaktpunktā un ar attiecīgajām iestādēm. Daudziem tiešsaistes pakalpojumiem, attiecībā uz kuriem jāizmanto *PKI*, vajadzīga elektroniskā identifikācija un autentifikācija un elektroniskais paraksts.

(9) Lielākajā daļā gadījumu pakalpojumu sniedzēji no citām dalībvalstīm nevar izmantot savu elektronisko identifikāciju, lai piekļūtu šiem pakalpojumiem, jo attiecīgo valstu elektroniskās identifikācijas shēmas nav atzītas un akceptētas citās dalībvalstīs. Šis šķērslis elektronisko sistēmu jomā liedz pakalpojumu saņēmējiem pilnībā izmantot iekšējā tirgus priekšrocības. Savstarpēji atzīti un akceptēti elektroniskās identifikācijas līdzekļi atvieglos daudzu pārrobežu pakalpojumu sniegšanu iekšējā tirgū un ļaus uzņēmumiem paplašināt savu darbību pāri robežām, neliekot tiem pārvarēt šķēršļus saskarsmē ar publiskā sektora iestādēm.

---

14 COM(2010) 245 galīgā redakcija/2.

15 2010. gada ziņojums par ES pilsonību. Likvidējot šķēršļus ES pilsoņu tiesību īstenošanai, COM(2010) 603 galīgā redakcija, 2.2.2. punkts, 13. lpp.

16 4/2/2011: EUCO 2/1/11.

17 23/10/2011: EUCO 52/1/11.

18 Padomes secinājumi par Eiropas e-pārvaldes rīcības plānu 2011.–2015. gadam, Padomes 3093. sanāksme „Transports, telekomunikācijas un enerģētika", Briselē, 2011. gada 27. maijā.

19 Eiropas Parlamenta 2010. gada 21. septembra rezolūcija par iekšējā tirgus izveidi elektroniskās komercijas jomā (P7_TA(2010)0320) un Eiropas Parlamenta 2010. gada 15. jūnija rezolūcija par interneta pārvaldību – turpmāk veicamajiem pasākumiem (P7_TA(2010)0208).

20 OV L 376, 27.12.2006., 36. lpp.

(10) Pieņemot Eiropas Parlamenta un Padomes 2011. gada 9. marta Direktīvu 2011/24/ES par pacientu tiesību piemērošanu pārrobežu veselības aprūpē[21], ir izveidots tīkls, kurā apvienotas par e-veselību atbildīgās valsts iestādes. Lai palielinātu drošības līmeni un uzlabotu pārrobežu veselības aprūpes nepārtrauktību, šajā tīklā apvienotajām iestādēm ir jāizstrādā vadlīnijas par veselības aprūpes datu un pakalpojumu pārrobežu pieejamību, tostarp atbalstot „*kopīgus identifikācijas un autentifikācijas pasākumus, lai veicinātu datu nodošanu pārrobežu veselības aprūpē*". Elektroniskās identifikācijas un autentifikācijas savstarpēja atzīšana un akceptēšana ir ļoti svarīgs faktors, lai pārrobežu veselības aprūpes pakalpojumus Eiropas iedzīvotāji varētu izmantot praksē. Ja iedzīvotājiem ārstēšanās nolūkā jādodas uz citu valsti, tad medicīniskajiem datiem jābūt pieejamiem valstī, kur notiek ārstniecība. Tādēļ ir jāizveido stabila, droša un uzticama elektroniskās identifikācijas sistēma.

(11) Viens no šīs regulas mērķiem ir likvidēt šķēršļus, kas patlaban kavē to elektroniskās identifikācijas līdzekļu pārrobežu izmantošanu, kuri ieviesti dalībvalstīs, lai piekļūtu vismaz sabiedriskajiem pakalpojumiem. Šīs regulas mērķis nav pārveidot dalībvalstīs jau ieviestās elektroniskās identitātes pārvaldības sistēmas un saistītās infrastruktūras. Šīs regulas mērķis ir nodrošināt, ka dalībvalstu piedāvāto pārrobežu tiešsaistes pakalpojumu piekļuves nolūkā ir iespējams izmantot drošas elektroniskās identifikācijas un autentifikācijas sistēmas.

(12) Dalībvalstīm arī turpmāk vajadzētu būt iespējai brīvi izvēlēties, kādus tiešsaistes pakalpojumu piekļuves līdzekļus tās izmantos, lai nodrošinātu elektronisko identifikāciju. Tām arī vajadzētu būt iespējai izlemt, vai, nodrošinot šo līdzekļu pieejamību, iesaistīt privāto sektoru. Dalībvalstīm nevajadzētu būt pienākumam paziņot par savām elektroniskās identifikācijas shēmām. Dalībvalstis pašas ir tiesīgas izvēlēties, vai paziņot par visām, dažām vai nevienu no tām elektroniskās identifikācijas shēmām, kas tiek izmantotas valsts līmenī, lai piekļūtu vismaz tiešsaistes sabiedriskajiem pakalpojumiem vai īpašiem pakalpojumiem.

(13) Regulā jāparedz daži nosacījumi attiecībā uz to, kuri elektroniskās identifikācijas līdzekļi ir jāakceptē un kā būtu jāpaziņo par shēmām. Šiem nosacījumiem vajadzētu sekmēt dalībvalstu savstarpējo uzticēšanos attiecībā uz elektroniskās identifikācijas shēmām un to elektroniskās identifikācijas līdzekļu savstarpēju atzīšanu un akceptēšanu, kuri ietverti šo valstu paziņotajās shēmās. Ja paziņotāja dalībvalsts ir izpildījusi paziņošanas nosacījumus un paziņojumi ir publicēti *Eiropas Savienības Oficiālajā Vēstnesī*, būtu jāpiemēro savstarpējās atzīšanas un akceptēšanas princips. Taču šo tiešsaistes pakalpojumu piekļuvei un to galīgajai piegādei būtu jābūt cieši saistītai ar tiesībām saņemt šādus pakalpojumus saskaņā ar valsts tiesību aktos paredzētajiem nosacījumiem.

(14) Dalībvalstīm vajadzētu būt iespējai izlemt, vai elektroniskās identifikācijas līdzekļu izsniegšanā iesaistīt privāto sektoru un ļaut privātajam sektoram izmantot paziņotās shēmas elektroniskās identifikācijas līdzekļus identifikācijas nolūkā, ja tas ir vajadzīgs saistībā ar tiešsaistes pakalpojumiem vai elektroniskajiem darījumiem. Ja privātajam sektoram būtu iespēja izmantot šādus elektroniskās identifikācijas līdzekļus, tas varētu paļauties uz elektronisko identifikāciju un autentifikāciju, ko jau tagad daudzās dalībvalstīs plaši izmanto vismaz sabiedrisko pakalpojumu jomā, turklāt līdz ar šādu iespēju uzņēmumiem un iedzīvotājiem būtu vienkāršāk pieejami tiešsaistes

[21] OV L 88, 4.4.2011., 45. lpp.

pakalpojumiem arī citās valstīs. Lai privātajam sektoram būtu vieglāk šādus elektroniskās identifikācijas līdzekļus izmantot citās valstīs, dalībvalstu nodrošinātajai autentifikācijas iespējai vajadzētu būt pieejamai pārbaudītājiem, nepieļaujot publiskā vai privātā sektora diskrimināciju.

(15) Paziņotajā shēmā ietverto elektroniskās identifikācijas līdzekļu pārrobežu izmantošana nozīmē, ka dalībvalstīm ir jāsadarbojas, nodrošinot tehnisko sadarbspēju. Līdz ar to tiek izslēgti jebkādi specifiski valsts tehniskie noteikumi, kuri paredz, ka citu valstu pusēm, piemēram, jāiegādājas īpaša aparatūra vai programmatūra, lai pārbaudītu un validētu paziņoto elektroniskās identifikācijas shēmu. Savukārt no tehniskām prasībām lietotājiem, kuras izriet no jebkādas izmantotās marķierierīces (piem., viedkaršu) attiecīgajām specifikācijām, nav iespējams izvairīties.

(16) Dalībvalstu sadarbībai būtu jāsekmē paziņoto elektroniskās identifikācijas shēmu tehniskā sadarbspēja, lai sekmētu riska pakāpei atbilstošu augsta līmeņa uzticamību un drošību. Informācijas un paraugprakses apmaiņai dalībvalstu starpā ar mērķi panākt savstarpējo atzīšanu būtu jāpalīdz īstenot šādu sadarbību.

(17) Ar šo regulu arī būtu jāievieš vispārējs tiesiskais regulējums elektronisko uzticamības pakalpojumu izmantošanai. Taču ar to nevajadzētu uzlikt vispārēju pienākumu tos izmantot. It īpaši šai regulai nevajadzētu attiekties uz tādu pakalpojumu sniegšanu, par kuriem panākta brīvprātīga vienošanās saskaņā ar privāttiesībām. Tāpat, tai nevajadzētu attiekties uz tiem aspektiem, kas saistīti ar līgumu slēgšanu vai citu juridisku saistību uzņemšanos un derīgumu, ja attiecībā uz to veidu prasības paredzētas valsts vai Savienības tiesību aktos.

(18) Lai veicinātu elektronisko uzticamības pakalpojumu vispārēju pārrobežu izmantošanu, būtu jānodrošina, ka šos pakalpojumus var izmantot kā pierādījumus tiesvedībā visās dalībvalstīs.

(19) Dalībvalstīm arī turpmāk vajadzētu būt iespējai brīvi noteikt citus uzticamības pakalpojumu veidus papildus tiem, kas minēti šajā regulā iekļautajā uzticamības pakalpojumu izsmeļošajā sarakstā, lai valsts līmenī tos varētu atzīt par kvalificētiem uzticamības pakalpojumiem.

(20) Ņemot vērā tehnoloģiju straujo attīstību, šajā regulā būtu jāizmanto pieeja, kas paredz inovācijas iespēju.

(21) Attiecībā uz tehnoloģijām šai regulai vajadzētu būt neitrālai. No tās izrietošās juridiskās sekas varētu panākt ar jebkuriem tehniskajiem līdzekļiem, taču ar nosacījumu, ka ir izpildītas šīs regulas prasības.

(22) Lai stiprinātu iedzīvotāju uzticēšanos iekšējam tirgum un veicinātu uzticamības pakalpojumu un produktu izmantošanu, būtu jāievieš jēdzieni „kvalificēti uzticamības pakalpojumi” un „kvalificēts uzticamības pakalpojumu sniedzējs”, nosakot prasības un pienākumus, kas jāievēro, lai attiecībā uz jebkuru sniegto kvalificētu uzticamības pakalpojumu un lietoto produktu nodrošinātu augsta līmeņa drošību.

(23) Atbilstīgi prasībām, kas noteiktas Eiropas Savienībā spēkā esošajā ANO Konvencijā par personu ar invaliditāti tiesībām, personām ar invaliditāti vajadzētu būt iespējai izmantot uzticamības pakalpojumus un galapatēriņam paredzētos produktus, kas

piedāvāti saistībā ar minētajiem pakalpojumiem, turklāt ar tādiem pašiem nosacījumiem, kādi attiecas uz citiem patērētājiem.

(24) Uzticamības pakalpojumu sniedzējs ir personas datu apstrādātājs, un tādēļ tam ir jāizpilda prasības, kas noteiktas Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvā 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti[22]. Datu vākšana būtu pēc iespējas jāsamazina, ņemot vērā pakalpojuma sniegšanas nolūku.

(25) Uzraudzības iestādēm būtu jāsadarbojas un jāapmainās ar informāciju ar datu aizsardzības iestādēm, lai nodrošinātu, ka pakalpojumu sniedzēji pienācīgi pilda tiesību aktus datu aizsardzības jomā. Jo īpaši būtu jāapmainās ar informāciju par drošības incidentiem un personas datu pārkāpumiem.

(26) Visiem uzticamības pakalpojumu sniedzējiem būtu jānosaka pienākums ievērot labu praksi drošības jomā, kas atbilst ar to darbību saistītajiem riskiem, lai tādējādi sekmētu lietotāju uzticēšanos vienotajam tirgum.

(27) Noteikumiem par pseidonīmu izmantošanu sertifikātos nevajadzētu kavēt dalībvalstis pieprasīt personu identifikāciju atbilstīgi Savienības vai valsts tiesību aktiem.

(28) Visām dalībvalstīm būtu jāievēro kopējas būtiskas uzraudzības prasības, lai kvalificētu uzticamības pakalpojumu jomā nodrošinātu līdzvērtīgu drošības līmeni. Lai visā Savienībā būtu vieglāk konsekventi piemērot šīs prasības, dalībvalstīm būtu jāpieņem līdzvērtīgas procedūras un jāapmainās ar informāciju par savu uzraudzības darbību un paraugpraksi šajā jomā.

(29) Drošības pārkāpumu paziņošana un drošības risku izvērtēšana ir būtiski aspekti, kas drošības vai integritātes pārkāpumu gadījumā ļautu sniegt atbilstīgu informāciju attiecīgajām pusēm.

(30) Lai Komisija un dalībvalstis varētu novērtēt ar šo regulu ieviestā pārkāpumu paziņošanas mehānisma efektivitāti, būtu jānosaka, lai uzraudzības iestādes iesniegtu Komisijai un Eiropas Tīklu un informācijas drošības aģentūrai (*ENISA*) informatīvus kopsavilkumus.

(31) Lai Komisija un dalībvalstis varētu novērtēt šīs regulas ietekmi, būtu jāpieprasa uzraudzības iestādēm iesniegt statistikas datus par kvalificētiem uzticamības pakalpojumiem un to izmantošanu.

(32) Lai Komisija un dalībvalstis varētu novērtēt ar šo regulu ieviestā pastiprinātas uzraudzības mehānisma efektivitāti, būtu jāpieprasa uzraudzības iestādēm iesniegt ziņojumus par savu darbību. Šāda pieeja būtu lietderīga, lai sekmētu labas prakses apmaiņu starp uzraudzības iestādēm, turklāt tā nodrošinātu, ka galvenās uzraudzības prasības tiek pārbaudītas konsekventi un efektīvi piemērotas visās dalībvalstīs.

(33) Lai nodrošinātu kvalificētu uzticamības pakalpojumu ilgtspējību un ilglaicīgumu un sekmētu lietotāju uzticēšanos kvalificētu uzticamības pakalpojumu nepārtrauktībai, uzraudzības iestādēm būtu jānodrošina, ka kvalificētu uzticamības pakalpojumu

[22] OV L 281, 23.11.1995., 31. lpp.

sniedzēju dati tiek saglabāti un ir pieejami pienācīgu periodu pat tad, ja kvalificēts uzticamības pakalpojumu sniedzējs ir pārtraucis savu darbību.

(34) Dalībvalstīs būtu jāizveido uzraudzības iestāžu savstarpējas palīdzības sistēma, lai atvieglotu kvalificētu uzticamības pakalpojumu sniedzēju uzraudzību, piemēram, gadījumā, ja pakalpojumu sniedzējs pakalpojumus piedāvā citas dalībvalsts teritorijā un nav pakļauts šīs dalībvalsts uzraudzības iestādēm vai ja pakalpojumu sniedzēja datori atrodas citas dalībvalsts teritorijā, nevis tajā dalībvalstī, kur reģistrēts minētais pakalpojumu sniedzējs.

(35) Uzticamības pakalpojumu sniedzēju pienākums ir izpildīt šajā regulā noteiktās prasības attiecībā uz uzticamības pakalpojumu, it īpaši kvalificētu uzticamības pakalpojumu, sniegšanu. Uzraudzības iestāžu pienākums ir uzraudzīt, kā uzticamības pakalpojumu sniedzēji ievēro šīs prasības.

(36) Lai efektīvi noritētu ieviešanas process, kura noslēgumā kvalificētos uzticamības pakalpojumu sniedzējus un to sniegtos kvalificētos uzticamības pakalpojumus iekļautu uzticamības sarakstos, būtu jāsekmē iepriekšēja apspriešanās starp kvalificētiem uzticamības pakalpojumu sniedzējiem un kompetento uzraudzības iestādi, tādējādi atvieglojot uzticamības pārbaudi, kas jāveic pirms kvalificētu uzticamības pakalpojumu sniegšanas.

(37) Uzticamības saraksti ir būtiski, lai panāktu uzticēšanos tirgus dalībnieku starpā, jo tajos norādīts pakalpojumu sniedzēja kvalifikācijas statuss uzraudzības laikā, taču šādi saraksti nav priekšnoteikums kvalifikācijas statusa piešķiršanai un kvalificētu uzticamības pakalpojumu sniegšanai, jo tā ir atkarīga no šajā regulā paredzēto prasību ievērošanas.

(38) Ja par kvalificētu uzticamības pakalpojumu ir paziņots, tad attiecīgā publiskā sektora iestāde vairs nevar atteikt tā izmantošanu, lai izpildītu administratīvas procedūras vai formalitātes, ar pamatojumu, ka šis pakalpojums nav iekļauts dalībvalstu izveidotajos uzticamības sarakstos. Tādēļ „publiskā sektora iestāde" ir jebkura publiskā sektora iestāde vai cita struktūra, kurai uzticēts sniegt e-pārvaldes pakalpojumus, piemēram, pieņemt tiešsaistē nodokļu deklarācijas, pieņemt dzimšanas apliecību pieteikumus, nodrošināt piedalīšanos publiskā iepirkuma procedūrās elektroniskā veidā u. c.

(39) Lai nodrošinātu elektronisko parakstu savstarpēju atzīšanu, drošības līmenim jābūt augstam, taču īpašos gadījumos, piemēram, saistībā ar Komisijas 2009. gada 16. oktobra Lēmumu 2009/767/EK par pasākumiem, lai veicinātu procedūru veikšanu elektroniski, izmantojot vienotos kontaktpunktus atbilstoši Eiropas Parlamenta un Padomes Direktīvai 2006/123/EK par pakalpojumiem iekšējā tirgū[23], būtu jāakceptē elektroniskie paraksti arī ar zemāku drošības nodrošinājuma līmeni.

(40) Būtu jānodrošina, ka parakstītājs var uzticēt trešai pusei kvalificētas elektroniskā paraksta radīšanas ierīces, ar nosacījumu, ka ir ieviesti attiecīgie mehānismi un procedūras, kas garantē, ka parakstītājs ir vienīgais, kurš kontrolē sava elektroniskā paraksta radīšanas datu izmantošanu, un ka saistībā ar ierīces izmantošanu ir izpildītas kvalificētā paraksta prasības.

---

[23] OV L 274, 20.10.2009., 36. lpp.

(41) Lai nodrošinātu tiesisko noteiktību saistībā ar paraksta derīgumu, ir būtiski precīzi norādīt, kuri kvalificēta elektroniska paraksta dati ir jānovērtē pārbaudītājam, kurš veic validāciju. Turklāt prasību noteikšanai attiecībā uz tādiem kvalificētiem uzticamības pakalpojumu sniedzējiem, kas var sniegt kvalificētus validēšanas pakalpojumus pārbaudītājiem, kuri nevēlas vai nespēj veikt kvalificētu elektronisko parakstu validāciju, būtu jāsekmē privātā vai publiskā sektora ieguldījumi šādos pakalpojumos. Izpildot abus nosacījumus, kvalificēta elektroniskā paraksta validēšanai vajadzētu kļūt par vienkāršu un Savienības līmenī visām pusēm piemērotu procedūru.

(42) Ja, veicot darījumu, vajadzīgs juridiskas personas kvalificēts elektroniskais zīmogs, jāakceptē būtu arī juridiskās personas pilnvarotā pārstāvja kvalificēts elektroniskais paraksts.

(43) Elektroniskie zīmogi būtu jāizmanto kā pierādījums tam, ka elektronisko dokumentu izsniegusi juridiska persona, garantējot dokumenta izcelsmi un integritāti.

(44) Ar šo regulu būtu jānodrošina informācijas ilgtermiņa saglabāšana, proti, elektroniskā paraksta un elektroniskā zīmoga juridiskais derīgums ilgākā laikposmā, garantējot, ka tos var validēt neatkarīgi no turpmākas tehnoloģiju attīstības.

(45) Lai stiprinātu elektronisko dokumentu pārrobežu izmantošanu, šajā regulā būtu jāparedz tādu elektronisko dokumentu juridiskais spēks, kas atbilstīgi riska novērtējumam būtu uzskatāmi par līdzvērtīgiem papīra dokumentiem, ar nosacījumu, ka ir nodrošināts dokumentu autentiskums un integritāte. Lai iekšējā tirgū pārrobežu elektroniskos darījumus varētu veikt plašākā mērogā, būtiski arī nodrošināt, ka elektronisko dokumentu oriģinālus vai apliecinātas kopijas, ko kādas dalībvalsts kompetentās iestādes izsniegušas atbilstīgi savas valsts tiesību aktiem, atzīst un akceptē arī citās dalībvalstīs. Šai regulai nevajadzētu skart dalībvalstu tiesības noteikt, kas uzskatāms par oriģinālu vai kopiju valsts līmenī, tomēr tai vajadzētu nodrošināt, ka oriģinālus un kopijas atzīst un izmanto arī citās valstīs.

(46) Tā kā patlaban dalībvalstu kompetentās iestādes, savus dokumentus parakstot elektroniski, izmanto uzlabotu elektronisko parakstu dažādus formātus, ir jānodrošina, ka dalībvalstis spēj tehniski atbalstīt vismaz daļu uzlabotu elektronisko parakstu formātu tad, kad tās saņem elektroniski parakstītus dokumentus. Tāpat, ja dalībvalstu kompetentās iestādes izmanto uzlabotus elektroniskos zīmogus, būtu jānodrošina, ka tās atbalsta vismaz daļu uzlabotu elektronisko zīmogu formātu.

(47) Elektroniskos zīmogus var izmantot ne vien juridiskas personas izsniegtu dokumentu autentificēšanai, bet arī visu juridiskas personas digitālo aktīvu, piemēram, programmatūru kodu vai serveru, autentificēšanai.

(48) Nodrošinot iespēju autentificēt tīmekļa vietnes un apstiprināt to īpašnieku identitāti, būtu sarežģītāk viltot tīmekļa vietnes, tādējādi samazinot krāpniecību.

(49) Lai elastīgi un ātri papildinātu dažus šajā regulā precīzi noteiktus tehniskos aspektus, pilnvaras pieņemt tiesību aktus saskaņā ar Līguma par Eiropas Savienības darbību 290. pantu būtu jādeleģē Komisijai attiecībā uz elektroniskās identifikācijas sistēmu sadarbspēju; uzticamības pakalpojumu sniedzējiem vajadzīgajiem drošības pasākumiem; atzītām neatkarīgām iestādēm, kas ir atbildīgas par pakalpojumu sniedzēju revīziju; uzticamības sarakstiem; prasībām attiecībā uz elektronisko parakstu drošības līmeni; prasībām attiecībā uz kvalificētiem elektroniskā paraksta

sertifikātiem, to validēšanu un saglabāšanu; par kvalificētu elektroniskā paraksta radīšanas ierīču sertifikāciju atbildīgām iestādēm; prasībām attiecībā uz elektronisko zīmogu drošības līmeni un kvalificētiem elektroniskā zīmoga sertifikātiem; piegādes pakalpojumu sadarbspēju. Īpaši būtiski, lai Komisija, veicot sagatavošanas darbu, laikā rīkotu atbilstīgas apspriešanās, tostarp ekspertu līmenī.

(50) Komisijai, sagatavojot un izstrādājot deleģētos aktus, būtu jānodrošina vienlaicīga, savlaicīga un atbilstīga attiecīgo dokumentu nosūtīšana Eiropas Parlamentam un Padomei.

(51) Lai nodrošinātu vienotus šīs regulas īstenošanas nosacījumus, Komisijai būtu jāpiešķir īstenošanas pilnvaras, it īpaši attiecībā uz to standartu identifikācijas numuru precizēšanu, kuru izmantošana ļautu izdarīt pieņēmumu par dažu šajā regulā vai deleģētajos aktos noteikto prasību ievērošanu. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes 2011. gada 16. februāra Regulu (ES) Nr. 182/2011, ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu[24].

(52) Tiesiskās noteiktības un skaidrības labad Direktīva 1999/93/EK būtu jāatceļ.

(53) Lai nodrošinātu tiesisko noteiktību attiecībā uz tiem tirgus dalībniekiem, kuri jau izmanto kvalificētus sertifikātus, kas izsniegti saskaņā ar Direktīvu 1999/93/EK, ir jāparedz pietiekami ilgs pārejas periods. Turklāt jānodrošina, lai Komisijai būtu līdzekļi, kas tai ļautu īstenošanas aktus un deleģētos aktus pieņemt pirms minētā datuma.

(54) Tā kā rīcības mēroga dēļ šīs regulas mērķus nevar pietiekami labi sasniegt atsevišķās dalībvalstīs un tie labāk sasniedzami Savienības mērogā, Savienība var pieņemt pasākumus saskaņā ar subsidiaritātes principu, kas paredzēts Līguma par Eiropas Savienību 5. pantā. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai, jo īpaši attiecībā uz Komisijas kā dalībvalstu darbību koordinatores lomu,

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets

1. Šajā regulā izklāstīti noteikumi par elektronisko identifikāciju un elektroniskajiem uzticamības pakalpojumiem elektronisko darījumu veikšanai, lai nodrošinātu iekšējā tirgus pienācīgu darbību.

[24] OV L 55, 28.2.2011., 13. lpp.

2. Šajā regulā izklāstīti nosacījumi, saskaņā ar kuriem dalībvalstis atzīst un akceptē fizisku un juridisku personu elektroniskās identifikācijas līdzekļus, kuri ietverti citas dalībvalsts paziņotajā elektroniskās identifikācijas shēmā.

3. Ar šo regulu izveido tiesisko regulējumu attiecībā uz elektroniskajiem parakstiem, elektroniskajiem zīmogiem, elektroniskajiem laika zīmogiem, elektroniskajiem dokumentiem, elektroniskajiem piegādes pakalpojumiem un tīmekļa vietņu autentifikāciju.

4. Ar šo regulu nodrošina to, ka uzticamības pakalpojumus un produktus, kas atbilst šīs regulas nosacījumiem, drīkst laist brīvā apritē iekšējā tirgū.

2. pants

Piemērošanas joma

1. Šo regulu piemēro elektroniskās identifikācijas pakalpojumiem, kurus sniedz dalībvalstis vai kuri tiek sniegti šīs dalībvalsts vārdā vai vismaz tai uzņemoties atbildību, kā arī Savienībā reģistrētiem uzticamības pakalpojumu sniedzējiem.

2. Šo regulu nepiemēro tādu elektronisko uzticamības pakalpojumu sniegšanai, par kuriem panākta brīvprātīga vienošanās saskaņā ar privāttiesībām.

3. Šo regulu nepiemēro aspektiem, kas saistīti ar līgumu slēgšanu vai citu juridisku saistību uzņemšanos un to derīgumu, ja attiecībā uz to veidu prasības paredzētas valsts vai Savienības tiesību aktos.

3. pants

Definīcijas

Šajā regulā lieto šādas definīcijas:

1) „elektroniskā identifikācija” ir tādu personas elektronisku identifikācijas datu izmantošana, kas nepārprotami apliecina fiziskās vai juridiskās personas identitāti;

2) „elektroniskās identifikācijas līdzekļi” ir materiāli vai nemateriāli elementi, kas ietver šā panta 1. punktā minētos datus un ko izmanto, lai tiešsaistē piekļūtu pakalpojumiem, kā tas minēts 5. pantā;

3) „elektroniskās identifikācijas shēma” ir elektroniskās identifikācijas sistēma, kurā elektroniskās identifikācijas līdzekļus izsniedz šā panta 1. punktā minētajām personām;

4) „autentifikācija” ir elektronisks process, kurā var validēt fiziskas vai juridiskas personas elektronisko identifikāciju vai elektronisko datu izcelsmi un integritāti;

5) „parakstītājs” ir fiziska persona, kura rada elektronisku parakstu;

6) „elektroniskais paraksts” ir elektroniski dati, kas pievienoti citiem elektroniskajiem datiem vai loģiski saistīti ar tiem un ko parakstītājs izmanto, lai parakstītos;

7) „uzlabots elektroniskais paraksts” ir elektronisks paraksts, kas atbilst šādiem kritērijiem:

(a) tas ir unikāli saistīts ar parakstītāju;

(b) tas spēj identificēt parakstītāju;

(c) tas radīts ar elektroniskā paraksta radīšanas datiem, kuru izmantošanu ar augstu uzticamības līmeni var kontrolēt tikai un vienīgi parakstītājs, un

(d) tas ir saistīts ar attiecīgajiem datiem tādā veidā, lai būtu atklājamas jebkādas turpmākas to izmaiņas;

8) „kvalificēts elektroniskais paraksts" ir uzlabots elektroniskais paraksts, kas radīts ar kvalificētu elektroniskā paraksta radīšanas ierīci, pamatā izmantojot kvalificētu elektroniskā paraksta sertifikātu;

9) „elektroniskā paraksta radīšanas dati" ir unikāli dati, ko parakstītājs izmanto elektroniska paraksta radīšanai;

10) „sertifikāts" ir elektronisks apliecinājums, kas saista attiecīgi fiziskas vai juridiskas personas elektroniskā paraksta vai zīmoga validācijas datus ar sertifikātu un apliecina attiecīgās personas minētos datus;

11) „kvalificēts elektroniskā paraksta sertifikāts" ir apliecinājums, ko izmanto elektronisko parakstu apliecināšanai, ko izsniedz kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst I pielikumā noteiktajām prasībām;

12) „uzticamības pakalpojumi" ir visi elektroniskie pakalpojumi, kas ietver elektronisko parakstu, elektronisko zīmogu, elektronisko laika zīmogu, elektronisko dokumentu, elektronisko piegādes pakalpojumu, tīmekļa vietņu autentifikācijas un elektronisko sertifikātu (tostarp elektroniskā paraksta un elektroniskā zīmoga sertifikātu) radīšanu, pārbaudi, validāciju, apstrādi un saglabāšanu;

13) „kvalificēti uzticamības pakalpojumi" ir uzticamības pakalpojumi, kas atbilst šajā regulā noteiktajām prasībām;

14) „uzticamības pakalpojumu sniedzējs" ir fiziska vai juridiska persona, kas sniedz vienu vai vairākus uzticamības pakalpojumus;

15) „kvalificēts uzticamības pakalpojumu sniedzējs" ir uzticamības pakalpojumu sniedzējs, kas atbilst šajā regulā noteiktajām prasībām;

16) „produkts" ir aparatūra vai programmatūra, vai to attiecīgas sastāvdaļas, ko paredzēts izmantot uzticamības pakalpojumu sniegšanai;

17) „elektroniskā paraksta radīšanas ierīce" ir konfigurēta programmatūra vai aparatūra, ko izmanto elektroniska paraksta radīšanai;

18) „kvalificēta elektroniskā paraksta radīšanas ierīce" ir elektroniskā paraksta radīšanas ierīce, kas atbilst II pielikumā noteiktajām prasībām;

19) „zīmoga radītājs" ir juridiska persona, kas rada elektronisku zīmogu;

20) „elektroniskais zīmogs" ir elektroniski dati, kas pievienoti citiem elektroniskajiem datiem vai loģiski saistīti ar tiem, lai garantētu saistīto datu izcelsmi un integritāti;

21) „uzlabots elektroniskais zīmogs" ir elektronisks zīmogs, kas atbilst šādiem kritērijiem:

(a) tas ir unikāli saistīts ar zīmoga radītāju;

(b) tas spēj identificēt zīmoga radītāju;

(c) tas radīts ar elektroniskā zīmoga radīšanas datiem, kuru izmantošanu ar augstu uzticamības līmeni var kontrolēt tikai un vienīgi zīmoga radītājs elektroniskā zīmoga radīšanai, un

(d) tas ir saistīts ar attiecīgajiem datiem tādā veidā, lai būtu atklājamas jebkādas turpmākas to izmaiņas;

22) „kvalificēts elektroniskais zīmogs" ir uzlabots elektroniskais zīmogs, kas radīts ar kvalificētu elektroniskā zīmoga radīšanas ierīci, pamatā izmantojot kvalificētu elektroniskā zīmoga sertifikātu;

23) „elektroniskā zīmoga radīšanas dati" ir unikāli dati, ko elektroniskā zīmoga radītājs izmanto elektroniska zīmoga radīšanai;

24) „kvalificēts elektroniskā zīmoga sertifikāts" ir apliecinājums, ko izmanto elektronisko zīmogu apliecināšanai, ko izsniedz kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst III pielikumā noteiktajām prasībām;

25) „elektroniskais laika zīmogs" ir elektroniski dati, kas apliecina citu elektronisko datu apzīmogošanu konkrētā laikā un apstiprina to esamību minētajā laikā;

26) „kvalificēts elektroniskais laika zīmogs" ir elektroniskais laika zīmogs, kas atbilst 33. pantā noteiktajām prasībām;

27) „elektroniskais dokuments" ir dokuments jebkādā elektroniskā formātā;

28) „elektroniskie piegādes pakalpojumi" ir pakalpojumi, kurus izmantojot, ar elektroniskiem līdzekļiem tiek nosūtīti dati, sniedzot apliecinājumu par nosūtīto datu apstrādi, tostarp pierādījumu par datu nosūtīšanu vai saņemšanu, un kuri nodrošina nosūtīto datu aizsardzību pret pazušanu, zādzību vai jebkādu neatļautu sagrozīšanu;

29) „kvalificēts elektroniskais piegādes pakalpojums" ir elektroniskais piegādes pakalpojums, kas atbilst 36. pantā noteiktajām prasībām;

30) „kvalificēts tīmekļa vietņu autentifikācijas sertifikāts" ir apliecinājums, kas ļauj autentificēt tīmekļa vietni un apliecina tīmekļa vietnes saikni ar personu, kurai sertifikātu izsniedzis kvalificēts uzticamības pakalpojumu sniedzējs, un kas atbilst IV pielikumā noteiktajām prasībām;

31) „validācijas dati" ir dati, ko izmanto elektroniska paraksta vai elektroniska zīmoga validācijai.

4. pants

Iekšējā tirgus principi

1. Nedrīkst ierobežot tādu uzticamības pakalpojumu sniegšanu kādā dalībvalstī, ko nodrošina citā dalībvalstī reģistrēts uzticamības pakalpojumu sniedzējs tādu iemeslu dēļ, kas izriet no šīs regulas aptvertajām jomām.

2. Produktus, kas atbilst šīs regulas nosacījumiem, drīkst laist brīvā apritē iekšējā tirgū.

II NODAĻA

ELEKTRONISKĀ IDENTIFIKĀCIJA

5. pants

Savstarpējā atzīšana un akceptēšana

Ja saskaņā ar valsts tiesību aktiem vai administratīvo praksi tiešsaistes pakalpojumu piekļuvei ir nepieciešama elektroniskā identifikācija, izmantojot elektroniskās identifikācijas līdzekļus, tad jebkuri elektroniskās identifikācijas līdzekļi, kuri izsniegti citā dalībvalstī un ietverti shēmā, kas atbilstīgi 7. pantā minētajai procedūrai iekļauta Komisijas publicētā sarakstā, tiek atzīti un akceptēti, lai varētu piekļūt šādiem pakalpojumiem.

6. pants

Elektroniskās identifikācijas shēmu paziņošanas nosacījumi

1. Elektroniskās identifikācijas shēmas var paziņot saskaņā ar 7. pantu, ja ir izpildīti visi turpmāk minētie nosacījumi:

(a) elektroniskās identifikācijas līdzekļus izsniedz paziņotāja dalībvalsts, vai arī tie tiek izsniegti šīs dalībvalsts vārdā vai tai uzņemoties atbildību;

(b) elektroniskās identifikācijas līdzekļus var izmantot, lai piekļūtu vismaz tādiem sabiedriskajiem pakalpojumiem, saistībā ar kuriem paziņotājā dalībvalstī jāizmanto elektroniskā identifikācija;

(c) paziņotāja dalībvalsts nodrošina, ka personas identifikācijas dati nepārprotami piešķirti fiziskai vai juridiskai personai, kas minēta 3. panta 1. punktā;

(d) paziņotāja dalībvalsts nodrošina iespēju tiešsaistē izmantot autentifikāciju jebkurā laikā un bez maksas, lai pārbaudītājs varētu validēt elektroniskā formātā saņemtos personas identifikācijas datus. Dalībvalstis neizvirza īpašas tehniskas prasības tiem pārbaudītājiem, kas reģistrēti ārpus to teritorijas un kas plāno veikt šādu autentifikāciju. Ja paziņotajā identifikācijas shēmā vai autentifikācijas iespējā ir konstatēts pārkāpums vai tā ir daļēji apdraudēta, dalībvalstis nekavējoties aptur vai atsauc paziņoto identifikācijas shēmu vai autentifikācijas iespēju, vai attiecīgās apdraudētās daļas, un informē pārējās dalībvalstis un Komisiju atbilstīgi 7. pantam;

(e) paziņotāja dalībvalsts uzņemas atbildību par:

– i) šā panta c) apakšpunktā minēto personas identifikācijas datu nepārprotamu sasaistīšanu ar personu un

– ii) šā panta d) apakšpunktā minēto autentifikācijas iespēju.

2. Šā panta 1. punkta e) apakšpunkts neskar to pušu atbildību, kas veic darījumu, izmantojot elektroniskās identifikācijas līdzekļus, kuri ietverti paziņotajā shēmā.

7. pants

Paziņošana

1. Dalībvalstis, kuras paziņo elektroniskās identifikācijas shēmu, Komisijai nosūta turpmāk minēto informāciju un bez liekas kavēšanās jebkādas turpmākas izmaiņas, kas attiecas uz:

(a) paziņotās elektroniskās identifikācijas shēmas aprakstu;

(b) par paziņoto elektroniskās identifikācijas shēmu atbildīgajām iestādēm;

(c) informāciju par to, kurš veic personas nepārprotamo identifikatoru reģistrāciju;

(d) autentifikācijas iespējas aprakstu;

(e) paziņotās elektroniskās identifikācijas shēmas vai autentifikācijas iespējas vai attiecīgo apdraudēto daļu apturēšanas vai atsaukšanas kārtību.

2. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī* to elektroniskās identifikācijas shēmu sarakstu, par kurām iesniegts paziņojums saskaņā ar 1. punktu, un pamatinformāciju par attiecīgajām shēmām.

3. Ja Komisija paziņojumu saņem pēc 2. punktā minētā termiņa, tā veic grozījumus sarakstā trīs mēnešu laikā.

4. Pieņemot īstenošanas aktus, Komisija var noteikt tos nosacījumus, formātus un procedūras, kas jāievēro saistībā ar 1. un 3. punktā minēto paziņošanu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

8. pants

Koordinācija

1. Dalībvalstis sadarbojas, lai nodrošinātu paziņotajā shēmā ietverto elektroniskās identifikācijas līdzekļu sadarbspēju un palielinātu to drošības līmeni.

2. Pieņemot īstenošanas aktus, Komisija nosaka vajadzīgo kārtību, lai atvieglotu 1. punktā minēto dalībvalstu sadarbību ar mērķi sekmēt riska pakāpei atbilstošu augsta līmeņa uzticamību un drošību. Minētie īstenošanas akti it īpaši attiecas uz informācijas, pieredzes un labas prakses apmaiņu attiecībā uz elektroniskās identifikācijas shēmām, paziņoto elektroniskās identifikācijas shēmu salīdzinošo izvērtēšanu un tādu attiecīgo izmaiņu novērtējumu, ko elektroniskās identifikācijas nozarē veikušas dalībvalstu kompetentās iestādes. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

3. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz elektroniskās identifikācijas līdzekļu pārrobežu sadarbspējas sekmēšanu, nosakot prasību minimumu.

III NODAĻA

UZTICAMĪBAS PAKALPOJUMI

1. iedaļa

Vispārīgi noteikumi

9. pants

Atbildība

1. Ja vien uzticamības pakalpojumu sniedzējs nevar pierādīt, ka tas nav darbojies nolaidīgi, tas ir atbildīgs par tiešiem zaudējumiem, kas nodarīti fiziskai vai juridiskai personai un kas radušies 15. panta 1. punktā minēto saistību neizpildes dēļ.

2. Ja vien kvalificēts uzticamības pakalpojumu sniedzējs nevar pierādīt, ka tas nav darbojies nolaidīgi, tas ir atbildīgs par tiešiem zaudējumiem, kas nodarīti fiziskai vai juridiskai personai un kas radušies šajā regulā, it īpaši tās 19. pantā, noteikto prasību neievērošanas dēļ.

10. pants

Trešās valstīs reģistrēti uzticamības pakalpojumu sniedzēji

1. Ja trešās valsts izcelsmes kvalificētie uzticamības pakalpojumi un kvalificētie sertifikāti ir atzīti saskaņā ar nolīgumu, kas saskaņā ar LESD 218. pantu noslēgts starp Savienību un trešām valstīm vai starptautiskām organizācijām, tad kvalificētus uzticamības pakalpojumus un kvalificētus sertifikātus, ko sniedz trešās valstīs reģistrēti kvalificēti uzticamības pakalpojumu sniedzēji, akceptē kā tādus kvalificētus uzticamības pakalpojumus un kvalificētus sertifikātus, ko sniedz Savienībā reģistrēti kvalificēti uzticamības pakalpojumu sniedzēji.

2. Atsaucoties uz 1. punktu, šādi nolīgumi nodrošina, ka prasības, kuras piemērojamas kvalificētiem uzticamības pakalpojumiem un kvalificētiem sertifikātiem, ko sniedz Savienībā reģistrēti kvalificēti uzticamības pakalpojumu sniedzēji, ievēro arī uzticamības pakalpojumu sniedzēji trešās valstīs vai starptautiskās organizācijās, it īpaši attiecībā uz personas datu aizsardzību, drošību un uzraudzību.

11. pants

Datu apstrāde un aizsardzība

1. Uzticamības pakalpojumu sniedzēji un uzraudzības iestādes, apstrādājot personas datus, nodrošina likumīgu un godprātīgu datu apstrādi saskaņā ar Direktīvu 95/46/EK.

2. Uzticamības pakalpojumu sniedzēji personas datus apstrādā saskaņā ar Direktīvu 95/46/EK. Šādā apstrādē izmanto stingri ierobežotu tādu datu minimumu, kuri vajadzīgi, lai izsniegtu un uzturētu sertifikātu vai sniegtu uzticamības pakalpojumus.

3. Uzticamības pakalpojumu sniedzēji garantē tās personas datu konfidencialitāti un integritāti, kura izmanto uzticamības pakalpojumu.

4. Neskarot juridisko spēku, kas atbilstīgi valsts tiesību aktiem piešķirtas pseidonīmiem, dalībvalstis neliedz uzticamības pakalpojumu sniedzējiem elektroniskā paraksta sertifikātā parakstītāja vārda vietā norādīt pseidonīmu.

12. pants

Pieejamība personām ar invaliditāti

Piedāvātie uzticamības pakalpojumi un minēto pakalpojumu sniegšanā izmantotie galapatēriņam paredzētie produkti ir pieejami personām ar invaliditāti.

2. iedaļa

Uzraudzība

13. pants

Uzraudzības iestāde

1. Dalībvalsts izraugās piemērotu iestādi, kas reģistrēta tās teritorijā vai, pēc savstarpējas vienošanās, citā dalībvalstī, atbildību uzņemoties izraudzītājai dalībvalstij. Uzraudzības iestādēm piešķir visas uzraudzības un izmeklēšanas pilnvaras, kas tām nepieciešamas savu uzdevumu izpildē.

2. Uzraudzības iestāde ir atbildīga par šādu uzdevumu izpildi:

(a) pārraudzīt uzticamības pakalpojumu sniedzējus, kuri reģistrēti izraudzītājā dalībvalstī, lai nodrošinātu, ka tie atbilst 15. pantā noteiktajām prasībām;

(b) uzraudzīt kvalificētus uzticamības pakalpojumu sniedzējus, kuri reģistrēti izraudzītājā dalībvalstī, un to sniegtos kvalificētos uzticamības pakalpojumus, lai nodrošinātu, ka tie un to sniegtie kvalificētie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām;

(c) nodrošināt, ka uz attiecīgu laikposmu, garantējot pakalpojumu nepārtrauktību, attiecīgā informācija un dati, kas minēti 19. panta 2. punkta g) apakšpunktā un ko reģistrējuši kvalificēti uzticamības pakalpojumu sniedzēji, tiek saglabāti un ir pieejami arī pēc tam, kad kvalificēts uzticamības pakalpojumu sniedzējs ir pārtraucis savu darbību.

3. Visas uzraudzības iestādes līdz nākamā gada pirmā ceturkšņa beigām iesniedz Komisijai un dalībvalstīm gada pārskatu par uzraudzības pasākumiem iepriekšējā kalendārā gada laikā. Tajā ietver vismaz:

(a) informāciju par uzraudzības pasākumiem;

(b) kopsavilkumu par pārkāpumiem, par kuriem uzticamības pakalpojumu sniedzēji paziņojuši saskaņā ar 15. panta 2. punktu;

(c) statistikas datus par kvalificētu uzticamības pakalpojumu tirgu un izmantošanu, tostarp informāciju par pašiem kvalificētiem uzticamības pakalpojumu sniedzējiem, to sniegtajiem kvalificētajiem uzticamības pakalpojumiem un izmantotajiem produktiem, kā arī klientu vispārēju aprakstu.

4. Dalībvalstis paziņo Komisijai un pārējām dalībvalstīm to attiecīgo uzraudzības iestāžu nosaukumus un adreses, ko tās ir izraudzījušās.

5. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz 2. punktā minēto uzdevumu izpildē izmantojamo procedūru noteikšanu.

6. Pieņemot īstenošanas aktus, Komisija var noteikt tos nosacījumus, formātus un procedūras, kas jāievēro saistībā ar 3. punktā minēto ziņojumu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

14. pants

Savstarpējā palīdzība

1. Uzraudzības iestādes sadarbojas, lai apmainītos ar labu praksi un viena otrai iespējami īsākā laikā sniegtu attiecīgo informāciju un savstarpēju palīdzību, tādējādi panākot pasākumu konsekventu īstenošanu. Savstarpējā palīdzība it īpaši ietver informācijas pieprasījumus un uzraudzības pasākumus, piemēram, pieprasījumus veikt ar drošības revīziju saistītas pārbaudes, kā minēts 15., 16. un 17. pantā.

2. Uzraudzības iestāde, kurai ir lūgta palīdzība, nevar atteikties izpildīt pieprasījumu izņemot, ja vien:

(a) tā nav pilnvarota izskatīt pieprasījumu; vai

(b) pieprasījuma izpilde ir pretrunā šīs regulas noteikumiem.

3. Attiecīgā gadījumā uzraudzības iestādes var veikt kopīgu izmeklēšanu, kurā piedalās citu dalībvalstu uzraudzības iestāžu darbinieki.

Tās dalībvalsts uzraudzības iestāde, kurā tiek veikta izmeklēšana, atbilstīgi savas valsts tiesību aktiem, izmeklēšanas uzdevumus var uzticēt tās uzraudzības iestādes darbiniekiem, kam tiek sniegta palīdzība. Šādas pilnvaras var izmantot vienīgi uzņemošās uzraudzības iestādes darbinieku vadībā un klātbūtnē. Tās uzraudzības iestādes darbiniekiem, kam tiek sniegta palīdzība, piemēro valsts tiesību aktus, kuri attiecas uz uzņemošo uzraudzības iestādi. Uzņemošā uzraudzības iestāde uzņemas atbildību par tās uzraudzības iestādes darbinieku darbību, kam tiek sniegta palīdzība.

4. Pieņemot īstenošanas aktus, Komisija var noteikt tos formātus un procedūras, kas jāievēro saistībā ar šajā pantā paredzēto savstarpējo palīdzību. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

15. pants

Uzticamības pakalpojumu sniedzējiem piemērojamās drošības prasības

1. Savienībā reģistrēti uzticamības pakalpojumu sniedzēji veic atbilstīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu to sniegto uzticamības pakalpojumu drošības riskus. Ar šiem pasākumiem nodrošina riska pakāpei atbilstošu drošības līmeni, ņemot vērā jaunākās tehniskās iespējas. Jo īpaši veic pasākumus, lai novērstu un mazinātu drošības incidentu ietekmi un informētu ieinteresētās personas par jebkura incidenta negatīvo ietekmi.

Neskarot 16. panta 1. punktu, ikviens uzticamības pakalpojumu sniedzējs var uzraudzības iestādei iesniegt ziņojumu par drošības revīziju, ko veikusi atzīta neatkarīga iestāde, lai apstiprinātu, ka ir veikti atbilstīgi drošības pasākumi.

2. Uzticamības pakalpojumu sniedzēji bez liekas kavēšanās un, ja iespējams, ne vēlāk kā 24 stundas pēc attiecīgās informācijas saņemšanas, paziņo kompetentajai uzraudzības iestādei, informācijas drošības jomā kompetentajai valsts iestādei un citām attiecīgām trešām personām, piemēram, datu aizsardzības iestādēm, par jebkuru tādu drošības vai integritātes pārkāpumu, kas būtiski ietekmē sniegtos uzticamības pakalpojumus un ar tiem saistītos personas datus.

Attiecīgā gadījumā, jo īpaši tad, ja drošības vai integritātes pārkāpums skar divas vai vairākas dalībvalstis, attiecīgā uzraudzības iestāde informē citu dalībvalstu uzraudzības iestādes un Eiropas Tīklu un informācijas drošības aģentūru (*ENISA*).

Ja attiecīgā uzraudzības iestāde uzskata, ka pārkāpuma publiskošana ir sabiedrības interesēs, tā var arī informēt sabiedrību vai pieprasīt, lai to izdarītu uzticamības pakalpojumu sniedzējs.

3. Uzraudzības iestāde reizi gadā Komisijai un *ENISA* iesniedz kopsavilkumu par pārkāpumiem, par kuriem paziņojuši uzticamības pakalpojumu sniedzēji.

4. Lai īstenotu 1. un 2. punktu, kompetentajai uzraudzības iestādei ir pilnvaras izdot saistošus norādījumus uzticamības pakalpojumu sniedzējiem.

5. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz precīzāk definētiem 1. punktā minētajiem pasākumiem.

6. Pieņemot īstenošanas aktus, Komisija var noteikt tos nosacījumus, formātus un procedūras, tostarp termiņus, kas jāievēro saistībā ar 1.–3. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

16. pants

Kvalificētu uzticamības pakalpojumu sniedzēju uzraudzība

1. Kvalificētu uzticamības pakalpojumu sniedzēju revīziju reizi gadā veic atzīta neatkarīga iestāde, lai apstiprinātu, ka tie un to sniegtie kvalificētie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām, un tie iesniedz uzraudzības iestādei drošības revīzijas ziņojumu.

2. Neskarot 1. punktu, pēc savas iniciatīvas vai pēc Komisijas pieprasījuma uzraudzības iestāde var jebkurā laikā veikt revīziju, pārbaudot kvalificētos uzticamības pakalpojumu sniedzējus, lai apstiprinātu, ka tie un to sniegtie kvalificētie uzticamības pakalpojumi joprojām atbilst šajā regulā noteiktajiem nosacījumiem. Ja personas datu aizsardzības noteikumi, iespējams, ir pārkāpti, uzraudzības iestāde par revīzijas rezultātiem informē datu aizsardzības iestādes.

3. Uzraudzības iestādei ir pilnvaras izdot saistošus norādījumus kvalificētiem uzticamības pakalpojumu sniedzējiem, lai labotu jebkuru drošības revīzijas ziņojumā minētu prasību neizpildi.

4. Atsaucoties uz 3. punktu, ja kvalificētais uzticamības pakalpojumu sniedzējs neizlabo šādu neizpildi termiņā, ko noteikusi uzraudzības iestāde, tas zaudē savu kvalifikācijas statusu, un uzraudzības iestāde to informē, ka tā statuss tiks mainīts 18. pantā minētajos uzticamības sarakstos.

5. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz precizētiem nosacījumiem, atbilstīgi kuriem tiek atzīta neatkarīgā iestāde, kas veic šā panta 1. punktā, 15. panta 1. punktā un 17. panta 1. punktā minēto revīziju.

6. Pieņemot īstenošanas aktus, Komisija var noteikt tos nosacījumus, procedūras un formātus, kas jāievēro saistībā ar 1., 2. un 4. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

17. pants

Kvalificētu uzticamības pakalpojumu sniegšanas uzsākšana

1. Kvalificēti uzticamības pakalpojumu sniedzēji paziņo uzraudzības iestādei par savu nodomu sākt kvalificētu uzticamības pakalpojumu sniegšanu un iesniedz uzraudzības iestādei drošības revīzijas ziņojumu, ko sagatavojusi atzīta neatkarīga iestāde, kā noteikts 16. panta 1. punktā. Kvalificēti uzticamības pakalpojumu sniedzēji var sākt sniegt kvalificētos uzticamības pakalpojumus pēc tam, kad tie uzraudzības iestādei ir iesnieguši paziņojumu un drošības revīzijas ziņojumu.

2. Ja saskaņā ar 1. punktu uzraudzības iestādē ir iesniegti attiecīgie dokumenti, kvalificētos pakalpojumu sniedzējus iekļauj 18. pantā minētajos uzticamības sarakstos, norādot, ka paziņojums ir iesniegts.

3. Uzraudzības iestāde pārbauda, vai kvalificētais uzticamības pakalpojumu sniedzējs un tā sniegtie kvalificētie uzticamības pakalpojumi atbilst šīs regulas prasībām.

Ja pārbaudes rezultāti ir pozitīvi, tad ne vēlāk kā mēnesi pēc paziņošanas, kas veikta saskaņā ar 1. punktu, uzraudzības iestāde uzticamības sarakstos norāda kvalificēto pakalpojumu sniedzēju un to sniegto kvalificēto uzticamības pakalpojumu kvalifikācijas statusu.

Ja mēneša laikā pārbaude nav pabeigta, uzraudzības iestāde informē kvalificēto uzticamības pakalpojumu sniedzēju, norādot kavēšanās iemeslus un termiņu, līdz kuram pārbaude tiks pabeigta.

4. Kvalificētu uzticamības pakalpojumu, par kuru iesniegts 1. punktā minētais paziņojums, attiecīgajā publiskā sektora iestādē veicot administratīvu procedūru vai formalitātes, nevar atteikt ar pamatojumu, ka šis pakalpojums nav iekļauts 3. punktā minētajos sarakstos.

5. Pieņemot īstenošanas aktus, Komisija var noteikt tos nosacījumus, formātus un procedūras, kas jāievēro saistībā ar 1., 2. un 3. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

18. pants

Uzticamības saraksti

1. Katra dalībvalsts izveido, atjaunina un publicē uzticamības sarakstus, kur sniegta informācija par kvalificētajiem uzticamības pakalpojumu sniedzējiem, kuri ietilpst attiecīgās dalībvalsts kompetencē, kā arī informācija par to sniegtajiem kvalificētajiem uzticamības pakalpojumiem.

2. Dalībvalstis drošā veidā izveido, atjaunina un publicē 1. punktā minētos uzticamības sarakstus, kuri ir elektroniski parakstīti vai apzīmogoti, turklāt sagatavoti automatizētai apstrādei piemērotā formātā.

3. Dalībvalstis bez liekas kavēšanās paziņo Komisijai informāciju par iestādi, kura ir atbildīga par valsts uzticamības sarakstu izveidi, atjaunināšanu un publicēšanu, un sīku informāciju par to, kur šādi saraksti ir publicēti, par sertifikātu, kas izmantots uzticamības sarakstu parakstīšanai vai apzīmogošanai, kā arī par visām attiecīgajām izmaiņām.

4. Izmantojot drošu kanālu, Komisija publisko 3. punktā minēto informāciju, kura ir elektroniski parakstīta vai apzīmogota, turklāt sagatavota automatizētai apstrādei piemērotā formātā.

5. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz 1. punktā minētās informācijas noteikšanu.

6. Pieņemot īstenošanas aktus, Komisija var noteikt uzticamības sarakstu tehniskās specifikācijas un formātus, kas jāievēro saistībā ar 1.–4. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

19. pants

Prasības kvalificētajiem uzticamības pakalpojumu sniedzējiem

1. Izsniedzot kvalificētu sertifikātu, ar piemērotiem līdzekļiem un saskaņā ar valsts tiesību aktiem kvalificēts uzticamības pakalpojumu sniedzējs pārbauda tās fiziskās vai juridiskās personas identitāti, kurai izsniegts kvalificēts sertifikāts, un, ja vajadzīgs, šīs personas īpašās raksturīgās pazīmes.

Atbildību uzņemoties kvalificētam pakalpojumu sniedzējam, kvalificētais pakalpojumu sniedzējs vai pilnvarota trešā persona šādu informāciju pārbauda:

(a) pēc fiziskas personas izskata vai juridiskas personas pilnvarotā pārstāvja izskata, vai

(b) attālināti, izmantojot paziņotajā shēmā ietvertos elektroniskās identifikācijas līdzekļus, kuri izsniegti saskaņā ar a) apakšpunktu.

2. Kvalificēti uzticamības pakalpojumu sniedzēji, nodrošinot kvalificētus uzticamības pakalpojumus:

(a) nodarbina darbiniekus, kuriem ir vajadzīgās zināšanas, pieredze un kvalifikācija, kuri veic Eiropas vai starptautiskiem standartiem atbilstīgas administratīvās un vadības procedūras un ir atbilstīgi apmācīti par drošības un personas datu aizsardzības noteikumiem;

(b) uzņemas risku sakarā ar atbildību par zaudējumiem, nodrošinot pietiekamus finanšu resursus vai izmantojot piemērotu atbildības apdrošināšanas shēmu;

(c) pirms iesaistīšanās līgumsaistībās informē personu, kura vēlas izmantot kvalificētus uzticamības pakalpojumus, par precīziem noteikumiem attiecībā uz minētā pakalpojuma izmantošanu;

(d) izmanto uzticamas sistēmas un produktus, kas ir aizsargāti pret izmaiņām un nodrošina to piedāvātā procesa tehnisko drošību un uzticamību;

(e) izmanto uzticamas sistēmas tiem iesniegto datu uzglabāšanai pārbaudāmā formā, lai:

– šie dati būtu publiski pieejami izguves nolūkā tikai tad, ja tam piekrīt persona, kurai šie dati ir izsniegti,

– ierakstus un izmaiņas varētu izdarīt tikai pilnvarotas personas,

– varētu pārbaudīt informācijas autentiskumu;

(f) veic pasākumus pret datu viltošanu un zādzību;

(g) uz attiecīgu laikposmu reģistrē visu attiecīgo informāciju par kvalificētā uzticamības pakalpojumu sniedzēja izsniegtajiem un saņemtajiem datiem, jo īpaši tādēļ, lai sniegtu pierādījumus tiesvedībā. Šādu reģistrāciju var veikt elektroniski;

(h) ir sagatavojuši atjauninātu plānu par pakalpojumu pārtraukšanu, lai nodrošinātu pakalpojumu nepārtrauktību saskaņā ar noteikumiem, ko saskaņā ar 13. panta 2. punkta c) apakšpunktu izdevusi uzraudzības iestāde;

(i) nodrošina personas datu likumīgu apstrādi saskaņā ar 11. pantu.

3. Kvalificēti uzticamības pakalpojumu sniedzēji, kas izsniedz kvalificētus sertifikātus, savā sertifikātu datubāzē reģistrē atsauktos sertifikātus desmit minūšu laikā pēc šādas atsaukšanas.

4. Attiecībā uz 3. punktu kvalificēti uzticamības pakalpojumu sniedzēji, kas izsniedz kvalificētus sertifikātus, ikvienam pārbaudītājam sniedz informāciju par tiem izsniegto kvalificēto sertifikātu derīgumu vai atsaukšanu. Šī informācija ir pieejama jebkurā laikā, vismaz tad, ja to pieprasa, izmantojot sertifikātu automatizētā veidā, kas ir uzticams, bez maksas un efektīvs.

5. Pieņemot īstenošanas aktus, Komisija var ieviest uzticamu sistēmu un produktu standartu identifikācijas numurus. Uzskata, ka atbilstība 19. pantā noteiktajām prasībām ir panākta tad, ja uzticamas sistēmas un produkti atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

3. iedaļa

Elektroniskais paraksts

20. pants

Elektroniskā paraksta juridiskais spēks un akceptēšana

1. Elektronisks paraksts var radīt juridiskais spēks, tas ir pieņemams kā pierādījums tiesvedībā, un to nedrīkst noraidīt tikai elektroniskā formāta dēļ.

2. Kvalificēts elektronisks paraksts juridiskā spēka ziņā ir līdzvērtīgs parakstam ar roku.

3. Kvalificētus elektroniskos parakstus atzīst un akceptē visās dalībvalstīs.

4. Ja ir vajadzīgs elektronisks paraksts ar tādu drošības nodrošinājuma līmeni, kas ir zemāks nekā kvalificētajam elektroniskam parakstam – jo īpaši tad, kad to pieprasa dalībvalsts nolūkā piekļūt publiskā sektora iestādes piedāvātam tiešsaistes pakalpojumam, pamatojoties uz atbilstīgu tādu risku novērtējumu, kuri saistīti ar šādiem pakalpojumiem, – tiek atzīti un akceptēti visi elektroniskie paraksti, kas atbilst vismaz tādam pašam drošības nodrošinājuma līmenim.

5. Saistībā ar publiskā sektora iestādes piedāvātu tiešsaistes pakalpojumu pārrobežu piekļuvi dalībvalstis nepieprasa elektronisku parakstu ar tādu drošības nodrošinājuma līmeni, kas ir augstāks nekā kvalificētajam elektroniskam parakstam.

6. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz elektroniskā paraksta 4. punktā minēto dažādo drošības līmeņu noteikšanu.

7. Pieņemot īstenošanas aktus, Komisija var ieviest elektroniskā paraksta drošības līmeņu standartu identifikācijas numurus. Uzskata, ka atbilstība drošības līmenim, kas noteikts atbilstīgi 6. punktam pieņemtā deleģētajā aktā, ir panākta tad, ja elektroniskais paraksts atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

21. pants

Kvalificēti elektroniskā paraksta sertifikāti

1. Kvalificēti elektroniskā paraksta sertifikāti atbilst I pielikumā noteiktajām prasībām.

2. Uz kvalificētiem elektroniskā paraksta sertifikātiem neattiecas neviena obligātā prasība, kas pārsniedz I pielikumā noteiktās prasības.

3. Ja kvalificēts elektroniskā paraksta sertifikāts ir atsaukts pēc sākotnējas aktivizēšanas, tas vairs nav derīgs, un tā statusu nekādā gadījumā nevar mainīt, atjaunojot tā derīgumu.

4. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz precīzāk definētām I pielikumā noteiktajām prasībām.

5. Pieņemot īstenošanas aktus, Komisija var ieviest kvalificētu elektroniskā paraksta sertifikātu standartu identifikācijas numurus. Uzskata, ka atbilstība I pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā paraksta sertifikāts atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

22. pants

Prasības kvalificētām elektroniskā paraksta radīšanas ierīcēm

1. Kvalificētas elektroniskā paraksta radīšanas ierīces atbilst II pielikumā noteiktajām prasībām.

2. Pieņemot īstenošanas aktus, Komisija var ieviest kvalificētu elektroniskā paraksta radīšanas ierīču standartu identifikācijas numurus. Uzskata, ka atbilstība II pielikumā noteiktajām prasībām ir panākta tad, ja kvalificētas elektroniskā paraksta radīšanas ierīces atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

23. pants

Kvalificētu elektroniskā paraksta radīšanas ierīču sertifikācija

1. Kvalificētas elektroniskā paraksta radīšanas ierīces var sertificēt dalībvalstu izraudzītas kompetentās publiskā vai privātā sektora iestādes, ar nosacījumu, ka minētās ierīces ir izvērtētas drošības novērtēšanas procedūrā saskaņā ar kādu no standartiem, kuri noteikti attiecībā uz tādu informācijas tehnoloģiju produktu drošības novērtēšanu, kurus Komisija, pieņemot īstenošanas aktus, iekļāvusi sarakstā. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

2. Dalībvalstis paziņo Komisijai un pārējām dalībvalstīm izraudzīto publiskā vai privātā sektora iestāžu nosaukumus un adreses, kā minēts 1. punktā.

3. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz tādu īpašu kritēriju izstrādi, kuri jāievēro izraudzītajām iestādēm, kas minētas 1. punktā.

24. pants

Sertificēto kvalificēto elektroniskā paraksta radīšanas ierīču saraksta publicēšana

1. Dalībvalstis bez liekas kavēšanās paziņo Komisijai informāciju par kvalificētām elektroniskā paraksta radīšanas ierīcēm, ko sertificējušas 23. pantā minētās iestādes. Dalībvalstis bez liekas kavēšanās Komisijai paziņo arī informāciju par tām elektroniskā paraksta radīšanas ierīcēm, kas vairs netiks sertificētas.

2. Pamatojoties uz saņemto informāciju, Komisija izveido, publicē un atjaunina sarakstu, kurā uzskaitītas sertificētās kvalificētās elektroniskā paraksta radīšanas ierīces.

3. Pieņemot īstenošanas aktus, Komisija var noteikt tos nosacījumus, formātus un procedūras, kas jāievēro saistībā ar 1. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

25. pants

Prasības kvalificētu elektronisko parakstu validācijai

1. Kvalificētu elektronisko parakstu uzskata par derīgu, ja to var radīt ar augstu drošības pakāpi un parakstīšanas brīdī:

(a) sertifikāts, kas apliecina parakstu, ir kvalificēts elektroniskā paraksta sertifikāts atbilstīgi I pielikumā izklāstītajiem noteikumiem;

(b) pieprasītais kvalificētais sertifikāts ir autentisks un derīgs;

(c) paraksta validācijas dati atbilst datiem, kuri nosūtīti pārbaudītājam;

(d) datu kopums, kas nepārprotami apliecina parakstītāja identitāti, ir pareizi nosūtīts pārbaudītājam;

(e) ja tiek izmantots pseidonīms, tas ir skaidri norādīta pārbaudītājam;

(f) elektroniskais paraksts ir izveidots ar kvalificētu elektroniskā paraksta radīšanas ierīci;

(g) parakstīto datu integritāte nav apdraudēta;

(h) ir izpildītas 3. panta 7. punktā noteiktās prasības;

(i) ar paraksta validēšanai izmantoto sistēmu pārbaudītājam nosūtīti precīzi validēšanas rezultāti, ļaujot pārbaudītājam noskaidrot jebkādus ar drošību saistītus jautājumus.

2. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz precīzāk definētām 1. punktā noteiktajām prasībām.

3. Pieņemot īstenošanas aktus, Komisija var ieviest kvalificētu elektronisko parakstu validācijas standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu validācija atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

26. pants

Kvalificētu elektronisko parakstu kvalificēti validēšanas pakalpojumi

1. Kvalificētu elektronisko parakstu kvalificētus validēšanas pakalpojumus sniedz kvalificēts uzticamības pakalpojumu sniedzējs, kurš:

(a) veic validāciju atbilstīgi 25. panta 1. punktam un

(b) ļauj pārbaudītājiem saņemt validēšanas rezultātus automatizētā veidā, kas ir uzticams un efektīvs, turklāt nodrošinot, ka uz šā dokumenta ir kvalificēto validēšanas pakalpojumu sniedzēja uzlabotais elektroniskais paraksts vai uzlabotais elektroniskais zīmogs.

2. Pieņemot īstenošanas aktus, Komisija var ieviest 1. punktā minēto kvalificētu validēšanas pakalpojumu standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punkta b) apakšpunktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu validēšanas pakalpojumi atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

27. pants

Kvalificētu elektronisko parakstu saglabāšana

1. Kvalificētu elektronisko parakstu saglabāšanas pakalpojumus sniedz kvalificēts uzticamības pakalpojumu sniedzējs, izmantojot tādas procedūras un tehnoloģijas, ar kurām var nodrošināt kvalificētā elektroniskā paraksta validācijas datu uzticamību ilgāk par to tehnoloģiskā derīguma termiņu.

2. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz precīzāk definētām 1. punktā noteiktajām prasībām.

3. Pieņemot īstenošanas aktus, Komisija var ieviest kvalificētu elektronisko parakstu saglabāšanas standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu saglabāšanas kārtība atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

4. iedaļa

Elektroniskais zīmogs

28. pants

Elektroniskā zīmoga juridiskais spēks

1. Elektroniskajam zīmogam ir juridiskais spēks, tas ir pieņemams kā pierādījums tiesvedībā, un to nedrīkst noraidīt tikai elektroniskā formāta dēļ.

2. Attiecībā uz kvalificētu elektronisko zīmogu pastāv juridiskā prezumpcija par to, ka ir nodrošināta to datu izcelsme un integritāte, ar kuriem tas ir saistīts.

3. Kvalificētu elektronisko zīmogu atzīst un akceptē visās dalībvalstīs.

4. Ja ir vajadzīgs elektronisks zīmogs ar tādu drošības nodrošinājuma līmeni, kas ir zemāks nekā kvalificētajam elektroniskam zīmogam, – jo īpaši tad, kad to pieprasa dalībvalsts, lai varētu piekļūt publiskā sektora iestādes piedāvātam tiešsaistes pakalpojumam, pamatojoties uz atbilstīgu tādu risku novērtējumu, kuri saistīti ar šādiem pakalpojumiem, – tiek atzīti un akceptēti visi elektroniskie zīmogi, kas atbilst vismaz tādam pašam drošības nodrošinājuma līmenim.

5. Lai varētu piekļūt publiskā sektora iestādes piedāvātam tiešsaistes pakalpojumam, dalībvalstis nepieprasa elektronisku zīmogu ar tādu drošības nodrošinājuma līmeni, kas ir augstāks nekā kvalificētajam elektroniskam zīmogam.

6. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz elektroniskā zīmoga 4. punktā minēto dažādo drošības līmeņu noteikšanu.

7. Pieņemot īstenošanas aktus, Komisija var ieviest elektroniskā zīmoga drošības līmeņu standartu identifikācijas numurus. Uzskata, ka atbilstība drošības nodrošinājuma līmenim, kas noteikts atbilstīgi 6. punktam pieņemtā deleģētajā aktā, ir panākta tad, ja elektronisks zīmogs atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

29. pants

Prasības kvalificētiem elektroniskā zīmoga sertifikātiem

1. Kvalificēti elektroniskā zīmoga sertifikāti atbilst III pielikumā noteiktajām prasībām.

2. Uz kvalificētiem elektroniskā zīmoga sertifikātiem neattiecas neviena obligātā prasība, kas pārsniedz III pielikumā noteiktās prasības.

3. Ja kvalificēts elektroniskā zīmoga sertifikāts ir atsaukts pēc sākotnējas aktivizēšanas, tas vairs nav derīgs, un tā statusu nekādā gadījumā nevar mainīt, atjaunojot tā derīgumu.

4. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz precīzāk definētām III pielikumā noteiktajām prasībām.

5. Pieņemot īstenošanas aktus, Komisija var ieviest kvalificētu elektroniskā zīmoga sertifikātu standartu identifikācijas numurus. Uzskata, ka atbilstība III pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā zīmoga sertifikāts atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

30. pants

Kvalificētas elektroniskā zīmoga radīšanas ierīces

1. Prasībām, kas noteiktas attiecībā uz kvalificētām elektroniskā zīmoga radīšanas ierīcēm, 22. pantu piemēro *mutatis mutandis*.

2. Attiecībā uz kvalificēto elektroniskā zīmoga radīšanas ierīču sertifikāciju 23. pantu piemēro *mutatis mutandis*.

3. Attiecībā uz tāda saraksta publicēšanu, kurā uzskaitītas kvalificētas elektroniskā zīmoga radīšanas ierīces, kas ir sertificētas, 24. pantu piemēro *mutatis mutandis*.

31. pants

Kvalificētu elektronisko zīmogu validācija un saglabāšana

Attiecībā uz kvalificētu elektronisko zīmogu validāciju un saglabāšanu 25., 26. un 27. pantu piemēro *mutatis mutandis*.

5. iedaļa

Elektroniskais laika zīmogs

32. pants

Elektronisko laika zīmogu juridiskais spēks

1. Elektroniskajam laika zīmogam ir juridisks spēks, tas ir pieņemams kā pierādījums tiesvedībā, un to nedrīkst noraidīt tikai elektroniskā formāta dēļ.

2. Attiecībā uz kvalificētu elektronisko laika zīmogu pastāv juridiskā prezumpcija par to, ka ir nodrošināts zīmogā norādītais laiks un to datu integritāte, ar kuriem ir saistīts minētais laiks.

3. Kvalificētu elektronisko laika zīmogu atzīst un akceptē visās dalībvalstīs.

33. pants

Prasības kvalificētiem elektroniskajiem laika zīmogiem

1. Kvalificēts elektroniskais laika zīmogs atbilst šādām prasībām:

(a) tas ir precīzi sasaistīts ar universālo koordinēto laiku (*UTC*), lai nepieļautu iespēju veikt datos neatklājamas izmaiņas;

(b) tas ir balstīts uz precīzu laika avotu;

(c) to ir izsniedzis kvalificēts uzticamības pakalpojumu sniedzējs;

(d) tas ir parakstīts, izmantojot kvalificētā uzticamības pakalpojumu sniedzēja uzlabotu elektronisko parakstu vai uzlabotu elektronisko zīmogu, vai citu līdzvērtīgu metodi.

2. Pieņemot īstenošanas aktus, Komisija var ieviest laika un datu precīzas sasaistes un precīza laika avota standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja laika un datu precīza sasaiste un precīzs laika avots atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī.*

6. iedaļa

Elektroniskie dokumenti

34. pants

Elektronisko dokumentu juridiskais spēks un akceptēšana

1. Elektronisku dokumentu uzskata par līdzvērtīgu papīra dokumentam, un tas ir pieņemams kā pierādījums tiesvedībā, ņemot vērā tā autentiskuma un integritātes drošības nodrošinājuma līmeni.

2. Attiecībā uz dokumentu, ko persona, kura pilnvarota izsniegt attiecīgo dokumentu, parakstījusi ar kvalificētu elektronisko parakstu vai apzīmogojusi ar kvalificētu elektronisko zīmogu, pastāv juridiskā prezumpcija par šā dokumenta autentiskumu un integritāti, ar nosacījumu, ka dokumentā nav tādu dinamisku elementu, kas spēj automātiski mainīt dokumentu.

3. Ja publiskā sektora iestādes piedāvāta tiešsaistes pakalpojuma sniegšanas nolūkā ir vajadzīgs dokumenta oriģināls vai apliecināta kopija, tad citās dalībvalstīs bez papildu prasībām akceptē vismaz tādus elektroniskos dokumentus, ko izsniegušas personas, kuras ir pilnvarotas izsniegt attiecīgos dokumentus, un kas atzīti par oriģināliem vai apliecinātām kopijām saskaņā ar izcelsmes dalībvalsts tiesību aktiem.

4. Pieņemot īstenošanas aktus, Komisija var noteikt tos elektroniskā paraksta un elektroniskā zīmoga formātus, kas jāakceptē, ja publiskā sektora iestādes piedāvāta tiešsaistes pakalpojuma sniegšanas nolūkā dalībvalsts ir pieprasījusi parakstītu vai apzīmogotu dokumentu, kurš minēts 2. punktā. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

7. iedaļa

Kvalificēti elektroniskie piegādes pakalpojumi

35. pants

Elektronisko piegādes pakalpojumu juridiskais spēks

1. Dati, kas nosūtīti vai saņemti, izmantojot elektroniskos piegādes pakalpojumus, ir pieņemami kā pierādījums tiesvedībā attiecībā uz datu integritāti un pārliecību par datumu un laiku, kad norādītais adresāts nosūtījis vai saņēmis datus.

2. Attiecībā uz datiem, kas nosūtīti vai saņemti, izmantojot elektroniskos piegādes pakalpojumus, pastāv juridiskā prezumpcija par to datu nosūtīšanas vai saņemšanas datuma un laika precizitāti, kuri norādīti kvalificētā elektroniskās piegādes sistēmā.

3. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz precizētiem datu nosūtīšanas vai saņemšanas mehānismiem, kurus izmantojot, tiek sniegti elektroniskie piegādes pakalpojumi, un kuru mērķis ir sekmēt elektronisko piegādes pakalpojumu sadarbspēju.

36. pants

Prasības kvalificētiem elektroniskajiem piegādes pakalpojumiem

1. Kvalificēti elektroniskie piegādes pakalpojumi atbilst šādām prasībām:

(a) tos sniedz viens vai vairāki kvalificēti uzticamības pakalpojumu sniedzēji;

(b) tiem jānodrošina iespēja nepārprotami identificēt nosūtītāju un, ja vajadzīgs, adresātu;

(c) datu nosūtīšanas vai saņemšanas procesa drošība jāapliecina ar kvalificēta uzticamības pakalpojumu sniedzēja uzlabotu elektronisko parakstu vai uzlabotu elektronisko zīmogu tādā veidā, lai nepieļautu iespēju veikt datos neatklājamas izmaiņas;

(d) visas izmaiņas datos, kuras jāveic datu saņemšanas vai nosūtīšanas nolūkā, skaidri jānorāda datu nosūtītājam un adresātam;

(e) datu nosūtīšanas, saņemšanas un jebkuru izmaiņu datums jānorāda ar kvalificētu elektronisko laika zīmogu;

(f) ja datus pārsūta divu vai vairāku kvalificētu uzticamības pakalpojumu sniedzēju starpā, tad visiem kvalificētajiem uzticamības pakalpojumu sniedzējiem piemēro a)–e) apakšpunktā minētās prasības.

2. Pieņemot īstenošanas aktus, Komisija var ieviest datu nosūtīšanas un saņemšanas standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja datu nosūtīšana un saņemšana atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

8. iedaļa

Tīmekļa vietņu autentifikācija

37. pants

Prasības kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem

1. Kvalificēti tīmekļa vietņu autentifikācijas sertifikāti atbilst IV pielikumā noteiktajām prasībām.

2. Kvalificētus tīmekļa vietņu autentifikācijas sertifikātus atzīst un akceptē visās dalībvalstīs.

3. Saskaņā ar 38. pantu Komisija ir pilnvarota pieņemt deleģētos aktus attiecībā uz precīzāk definētām IV pielikumā noteiktajām prasībām.

4. Pieņemot īstenošanas aktus, Komisija var ieviest kvalificētu tīmekļa vietņu autentifikācijas sertifikātu standartu identifikācijas numurus. Uzskata, ka atbilstība IV pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēti tīmekļa vietņu autentifikācijas sertifikāti atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā. Šos aktus Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

IV NODAĻA

DELEĢĒTIE AKTI

38. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.

2. Pilnvaras pieņemt 8. panta 3. punktā, 13. panta 5. punktā, 15. panta 5. punktā, 16. panta 5. punktā, 18. panta 5. punktā, 20. panta 6. punktā, 21. panta 4. punktā, 23. panta 3. punktā, 25. panta 2. punktā, 27. panta 2. punktā, 28. panta 6. punktā, 29. panta 4. punktā, 30. panta 2. punktā, 31. pantā, 35. panta 3. punktā un 37. panta 3. punktā minētos deleģētos aktus Komisijai piešķir uz nenoteiktu laiku no šīs regulas spēkā stāšanās dienas.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 8. panta 3. punktā, 13. panta 5. punktā, 15. panta 5. punktā, 16. panta 5. punktā, 18. panta 5. punktā, 20. panta 6. punktā, 21. panta 4. punktā, 23. panta 3. punktā, 25. panta 2. punktā, 27. panta 2. punktā, 28. panta 6. punktā, 29. panta 4. punktā, 30. panta 2. punktā, 31. pantā, 35. panta 3. punktā un 37. panta 3. punktā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošo deleģēto aktu derīgumu.

4. Tiklīdz tā pieņem deleģētu aktu, Komisija par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

5. Saskaņā ar 8. panta 3. punktu, 13. panta 5. punktu, 15. panta 5. punktu, 16. panta 5. punktu, 18. panta 5. punktu, 20. panta 6. punktu, 21. panta 4. punktu, 23. panta 3. punktu, 25. panta 2. punktu, 27. panta 2. punktu, 28. panta 6. punktu, 29. panta 4. punktu, 30. panta 2. punktu, 31. pantu, 35. panta 3. punktu un 37. panta 3. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus, vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

V NODAĻA

ĪSTENOŠANAS AKTI

39. pants

Komiteju procedūra

1. Komisijai palīdz komiteja. Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011 nozīmē.

2. Ja ir atsauce uz šo punktu, piemēro Regulas Nr. 182/2011 5. pantu.

VI NODAĻA

NOBEIGUMA NOTEIKUMI

40. pants

Ziņojums

Komisija iesniedz ziņojumu Eiropas Parlamentam un Padomei par šīs regulas piemērošanu. Pirmo ziņojumu iesniedz ne vēlāk kā četrus gadus pēc regulas stāšanās spēkā. Turpmākos ziņojumus iesniedz reizi četros gados.

41. pants

Atcelšana

1. Direktīvu 1999/93/EK atceļ.

2. Atsauces uz atcelto direktīvu uzskata par atsaucēm uz šo regulu.

3. Drošās paraksta radīšanas ierīces, kuru atbilstība noteikta saskaņā ar Direktīvas 1999/93/EK 3. panta 4. punktu, uzskata par kvalificētām paraksta radīšanas ierīcēm saskaņā ar šo regulu.

4. Kvalificētus sertifikātus, kas izsniegti saskaņā ar Direktīvu 1999/93/EK, saskaņā ar šo regulu uzskata par kvalificētiem elektroniskā paraksta sertifikātiem līdz to derīguma termiņa beigām, bet ne ilgāk par pieciem gadiem no šīs regulas stāšanās spēkā.

42. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē,

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētājs*

I PIELIKUMS

Prasības kvalificētiem elektroniskā paraksta sertifikātiem

Kvalificēti elektroniskā paraksta sertifikāti ietver:

(a) norādi, vismaz automatizētai apstrādei piemērotā formātā, par to, ka sertifikāts izsniegts kā kvalificēts elektroniskā paraksta sertifikāts;

(b) tādu datu kopumu, kas nepārprotami apliecina tā kvalificētā uzticamības pakalpojumu sniedzēja identitāti, kurš izsniedz kvalificētos sertifikātus, ietverot vismaz informāciju par dalībvalsti, kurā pakalpojumu sniedzējs ir reģistrēts, un

– juridiskai personai – nosaukumu un reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai,

– fiziskai personai – personas vārdu;

(c) tādu datu kopumu, kas nepārprotami apliecina tā parakstītāja identitāti, kam izsniegts sertifikāts, ietverot vismaz parakstītāja vārdu vai pseidonīmu, kuru kā tādu identificē;

(d) elektroniskā paraksta validācijas datus, kas atbilst elektroniskā paraksta radīšanas datiem;

(e) precīzu informāciju par sertifikāta derīguma termiņa sākumu un beigām;

(f) sertifikāta identifikācijas kodu, kam jābūt kā kvalificētā uzticamības pakalpojumu sniedzēja unikālam kodam;

(g) tā kvalificētā uzticamības pakalpojumu sniedzēja uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu, kurš izsniedz sertifikātu;

(h) vietu, kur bez maksas pieejams sertifikāts, kas apliecina g) apakšpunktā minēto uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu;

(i) vietu, kur pieejami ar sertifikāta derīgumu saistīti pakalpojumi, ko var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu;

(j) ja elektroniskā paraksta radīšanas dati, kas saistīti ar elektroniskā paraksta validācijas datiem, atrodas kvalificētā elektroniskā paraksta radīšanas ierīcē – atbilstīgu norādi vismaz automatizētai apstrādei piemērotā formātā.

II PIELIKUMS

Prasības kvalificētām paraksta radīšanas ierīcēm

1. Ar kvalificētām elektroniskā paraksta radīšanas ierīcēm, izmantojot atbilstīgus tehniskos un procesuālos līdzekļus, nodrošina vismaz to, ka:

(a) ir nodrošināta elektroniskā paraksta radīšanā izmantoto elektroniskā paraksta radīšanas datu slepenība;

(b) elektroniskā paraksta radīšanā izmantotie elektroniskā paraksta radīšanas dati var parādīties tikai vienu reizi;

(c) ir pietiekama pārliecība par to, ka elektroniskā paraksta radīšanā izmantotos elektroniskā paraksta radīšanas datus nevar izgūt un elektroniskais paraksts ir aizsargāts pret viltošanu, izmantojot patlaban pieejamās tehnoloģijas;

(d) elektroniskā paraksta radīšanā izmantotos elektroniskā paraksta radīšanas datus likumīgais parakstītājs var droši aizsargāt pret to, ka tos izmanto citi.

2. Kvalificētās elektroniskā paraksta radīšanas ierīces nemaina parakstāmos datus vai nekavē šo datu parādīšanu parakstītājam pirms parakstīšanas.

3. Elektroniskā paraksta radīšanas datus parakstītāja vārdā rada vai pārvalda kvalificēts uzticamības pakalpojumu sniedzējs.

4. Kvalificēti uzticamības pakalpojumu sniedzēji, kuri pārvalda elektroniskā paraksta radīšanas datus, parakstītāja vārdā var nokopēt elektroniskā paraksta radīšanas datus rezerves kopijas izveides nolūkā, ja ir ievērotas šādas prasības:

(a) nokopēto datu kopu drošības līmenim jābūt tādam pašam, kāds tas ir oriģinālajām datu kopām;

(b) nokopēto datu kopu skaits nedrīkst pārsniegt minimālo skaitu, kāds nepieciešams, lai nodrošinātu pakalpojumu nepārtrauktību.

III PIELIKUMS

Prasības kvalificētiem elektroniskā zīmoga sertifikātiem

Kvalificēti elektroniskā zīmoga sertifikāti ietver:

(a) norādi, vismaz automatizētai apstrādei piemērotā formātā, par to, ka sertifikāts izsniegts kā kvalificēts elektroniskā zīmoga sertifikāts;

(b) tādu datu kopumu, kas nepārprotami apliecina tā kvalificētā uzticamības pakalpojumu sniedzēja identitāti, kurš izsniedz kvalificētos sertifikātus, ietverot vismaz informāciju par dalībvalsti, kurā pakalpojumu sniedzējs ir reģistrēts, un

– juridiskai personai – nosaukumu un reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai,

– fiziskai personai – personas vārdu;

(c) tādu datu kopumu, kas nepārprotami apliecina tās juridiskās personas identitāti, kam izsniegts sertifikāts, ietverot vismaz nosaukumu un reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai;

(d) elektroniskā zīmoga validācijas datus, kas atbilst elektroniskā zīmoga radīšanas datiem;

(e) precīzu informāciju par sertifikāta derīguma termiņa sākumu un beigām;

(f) sertifikāta identifikācijas kodu, kam jābūt kā kvalificētā uzticamības pakalpojumu sniedzēja unikālam kodam;

(g) tā kvalificētā uzticamības pakalpojumu sniedzēja uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu, kurš izsniedz sertifikātu;

(h) vietu, kur bez maksas pieejams sertifikāts, kas apliecina g) apakšpunktā minēto uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu;

(i) vietu, kur pieejami ar sertifikāta derīgumu saistīti pakalpojumi, ko var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu;

(j) ja elektroniskā zīmoga radīšanas dati, kas saistīti ar elektroniskā zīmoga validācijas datiem, atrodas kvalificētā elektroniskā zīmoga radīšanas ierīcē – atbilstīgu norādi vismaz automatizētai apstrādei piemērotā formātā.

IV PIELIKUMS

Prasības kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem

Kvalificēti tīmekļa vietņu autentifikācijas sertifikāti ietver:

(a) norādi, vismaz automatizētai apstrādei piemērotā formātā, par to, ka sertifikāts izsniegts kā kvalificēts tīmekļa vietņu autentifikācijas sertifikāts;

(b) tādu datu kopumu, kas nepārprotami apliecina tā kvalificētā uzticamības pakalpojumu sniedzēja identitāti, kurš izsniedz kvalificētos sertifikātus, ietverot vismaz informāciju par dalībvalsti, kurā pakalpojumu sniedzējs ir reģistrēts, un

– juridiskai personai – nosaukumu un reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai,

– fiziskai personai – personas vārdu;

(c) tādu datu kopumu, kas nepārprotami apliecina tās juridiskās personas identitāti, kam izsniegts sertifikāts, ietverot vismaz nosaukumu un reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai;

(d) tās juridiskās personas adresi, norādot vismaz pilsētu un dalībvalsti, kam izsniegts sertifikāts, turklāt atbilstīgi oficiālos avotos norādītajai informācijai;

(e) domēna vārdu vai vārdus, ko izmanto juridiskā persona, kurai izsniegts sertifikāts;

(f) precīzu informāciju par sertifikāta derīguma termiņa sākumu un beigām;

(g) sertifikāta identifikācijas kodu, kam jābūt kā kvalificētā uzticamības pakalpojumu sniedzēja unikālam kodam;

(h) tā kvalificētā uzticamības pakalpojumu sniedzēja uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu, kurš izsniedz sertifikātu;

(i) vietu, kur bez maksas pieejams sertifikāts, kas apliecina h) apakšpunktā minēto uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu;

(j) vietu, kur pieejami ar sertifikāta derīgumu saistīti pakalpojumi, ko var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu.

TIESĪBU AKTA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

Šajā finanšu pārskatā sīki izklāstītas prasības attiecībā uz administratīvajiem izdevumiem, lai īstenotu ierosināto regulu *par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū*.

Saskaņā ar likumdošanas procedūru pēc apspriedēm par ierosinātās regulas pieņemšanu Eiropas Parlamentā un Padomē tika nolemts, ka Komisijai būs vajadzīgi 12 pilnslodzes ekvivalenti, lai sagatavotu saistītos deleģētos un īstenošanas aktus, lai nodrošinātu organizatorisko un tehnisko standartu pieejamību, lai apstrādātu dalībvalstu paziņoto informāciju (it īpaši atjauninot ar uzticamības sarakstiem saistīto informāciju), lai informētu ieinteresētās personas (it īpaši iedzīvotājus un MVU) par elektroniskās identifikācijas un autentifikācijas, elektronisko parakstu un saistīto uzticamības pakalpojumu (*eIAS*) priekšrocībām un lai noorganizētu apspriedes ar trešām valstīm ar mērķi panākt *eIAS* sadarbspēju pasaules mērogā.

1.1. Priekšlikuma/iniciatīvas nosaukums

Komisijas priekšlikums regulai par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū

1.2. Attiecīgās politikas jomas *ABM*/*ABB* struktūrā[25]

09 INFORMĀCIJAS SABIEDRĪBA

1.3. Priekšlikuma/iniciatīvas būtība

☐ Priekšlikums/iniciatīva attiecas uz **jaunu darbību**

☐ Priekšlikums/iniciatīva attiecas uz **jaunu darbību, pamatojoties uz izmēģinājuma projektu/sagatavošanas darbību**[26]

☐ Priekšlikums/iniciatīva attiecas uz **esošas darbības pagarināšanu**

☑ Priekšlikums/iniciatīva attiecas uz **darbību, kas pārveidota jaunā darbībā**

1.4. Mērķi

1.4.1. Komisijas daudzgadu stratēģiskie mērķi, kurus plānots sasniegt ar priekšlikumu/iniciatīvu

Priekšlikuma vispārīgie mērķi ir to vispārējo ES politikas jomu mērķi, uz kurām attiecas priekšlikums, piemēram, stratēģija „Eiropa 2020”. Stratēģijas mērķis ir „padarīt ES par gudru, ilgtspējīgu un integrējošu ekonomiku ar augstu nodarbinātības, ražīguma un sociālās kohēzijas līmeni”.

25 *ABM*: budžeta vadība pa darbības jomām; *ABB*: budžeta līdzekļu sadale pa darbības jomām.

26 Kā paredzēts Finanšu regulas 49. panta 6. punkta attiecīgi a) un b) apakšpunktā.

1.4.2. Konkrētie mērķi un attiecīgās ABM/ABB *darbības*

Stiprināt Eiropas mēroga elektronisko darījumu uzticamību un nodrošināt elektroniskās identifikācijas un autentifikācijas un elektronisko parakstu, kā arī saistīto uzticamības pakalpojumu juridisku atzīšanu pārrobežu līmenī, kā arī augsta līmeņa datu aizsardzību un lietotāju tiesību nostiprināšanu vienotajā tirgū (skatīt Eiropas digitalizācijas programmu, 3. un 16. pamatpasākumu). Attiecīgās *ABM*/*ABB* darbības 09 02 - tiesiskais regulējums Eiropas digitalizācijas programmai

1.4.3. Paredzamie rezultāti un ietekme

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz finansējuma saņēmējiem/mērķgrupām.

Izveidot skaidru normatīvo vidi *eIAS* pakalpojumu jomā, kas sekmētu lietotājiem ērti izmantojamas digitālās tehnoloģijas un uzticēšanos tām.

1.4.4. Rezultātu un ietekmes rādītāji

Norādīt priekšlikuma/iniciatīvas īstenošanas uzraudzībā izmantojamos rādītājus.

1. Tādu *eIAS* pakalpojumu sniedzēju esamība, kuri veic darbību vairākās ES dalībvalstīs. 2. Ierīču (piemēram, viedkaršu lasītāju) savstarpējās izmantojamības līmenis dažādās nozarēs un valstīs. 3. *eIAS* izmantošana visās sabiedrības grupās. 4. Tas, cik lielā mērā *eIAS* izmanto tiešie lietotāji, veicot darījumus valsts un starptautiskā (pārrobežu) līmenī. 5. *eIAS* jomā ieviesto tiesību aktu harmonizācijas pakāpe dalībvalstīs. 6. Komisijai paziņotās elektroniskās identifikācijas shēmas. 7. Pakalpojumi, kuriem var piekļūt izmantojami ar elektroniskās identifikācijas līdzekļiem publiskajā sektorā (piemēram, e-pārvalde, e-veselība, e-tiesiskums, e-iepirkums). 8. Pakalpojumi, kuriem var piekļūt ar elektroniskās identifikācijas līdzekļiem privātajā sektorā (piemēram, internetbanka, e-komercija, e-azartspēles, pieslēgšanās tīmekļa vietnēm, drošāki interneta pakalpojumi).

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņa vai ilgtermiņa vajadzības

Tā kā dalībvalstis ir atšķirīgi interpretējušas Elektroniskā paraksta direktīvu un valstu līmenī tā ir dažādi īstenota, ir radušās pārrobežu sadarbspējas problēmas, tādējādi Eiropas Savienībā veidojot fragmentāciju un iekšējā tirgus izkropļojumus. Turklāt konstatēts uzticēšanās trūkums un nepietiekama paļāvība uz elektroniskajām sistēmām, kas neļauj Eiropas iedzīvotājiem digitālajā vidē pilnībā izmantot tos pašus pakalpojumus, ko viņi var izmantot fiziskajā pasaulē.

1.5.2. ES iesaistīšanās pievienotā vērtība

Rīcība ES līmenī dotu acīmredzamus ieguvumus salīdzinājumā ar rīcību dalībvalstu līmenī. Pieredze patiešām ir apliecinājusi, ka valsts mēroga pasākumi ir nepietiekami, lai nodrošinātu elektronisko darījumu pārrobežu pieejamību, gluži otrādi, ir radījuši šķēršļus elektronisko parakstu sadarbspējai ES mērogā, un patlaban tie tieši tādā pašā veidā ietekmē elektronisko identifikāciju, elektronisko autentifikāciju un saistītos uzticamības pakalpojumus.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

Izstrādājot priekšlikumu, ņemta vērā pieredze saistībā ar E-paraksta direktīvu un problēmas, ko radīja minētās direktīvas fragmentētā transponēšana un īstenošana, kas liedza sasniegt tajā paredzētos mērķus.

1.5.4. Saderība un iespējamā sinerģija ar citiem attiecīgajiem instrumentiem

Elektroniskā paraksta direktīvā ir iekļautas atsauces uz vairākām citām ES iniciatīvām, kuru mērķis ir atrisināt sadarbspējas problēmas un pārrobežu atzīšanas un akceptēšanas jautājumus saistībā ar dažiem elektronisko darījumu veidiem (piemēram, Pakalpojumu direktīva, publiskā iepirkuma direktīvas, pārskatītā PVN direktīva (e-rēķini) vai Eiropas pilsoņu iniciatīvas regula). Turklāt ar ierosināto regulu tiks izveidots tiesiskais regulējums, ļaujot vērienīgi īstenot plaša mēroga izmēģinājuma projektus, kuri ieviesti ES līmenī, lai atbalstītu sadarbspējīgus un uzticamus elektroniskās saziņas līdzekļus (tostarp tādus projektus kā *SPOCS*, kas sekmē Pakalpojumu direktīvas īstenošanu; *STORK*, kas sekmē sadarbspējīgu elektroniskās identifikācijas sistēmu izveidi un izmantošanu; *PEPPOL*, kas sekmē sadarbspējīgu e-iepirkuma risinājumu izstrādi un izmantošanu; *epSOS*, kas sekmē sadarbspējīgu e-veselības risinājumu izstrādi un izmantošanu; *eCodex*, kas sekmē sadarbspējīgu e-tiesiskuma risinājumu izstrādi un izmantošanu).

1.6. Ilgums un finansiālā ietekme

☐ **Ierobežota ilguma** priekšlikums/iniciatīva

– ☐ Priekšlikuma/iniciatīvas darbības laiks: [DD.MM.]GGGG.–[DD.MM.]GGGG.

– ☐ Finansiālā ietekme: GGGG.– GGGG.

☑ **Beztermiņa** priekšlikums/iniciatīva

1.7. Paredzētie pārvaldības veidi[27]

☑ Komisijas īstenota **centralizēta tieša pārvaldība**

☐ **Centralizēta netieša pārvaldība**, izpildes uzdevumus deleģējot:

– ☐ izpildaģentūrām

[27] Skaidrojumus par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt *BudgWeb* tīmekļa vietnē: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

– ☐ Kopienu izveidotām struktūrām[28]

– ☐ valstu publiskā sektora struktūrām vai struktūrām, kas veic valsts pārvaldes uzdevumus

– ☐ personām, kurām ir uzticēts veikt īpašas darbības saskaņā ar Līguma par Eiropas Savienību V sadaļu un kuras ir noteiktas attiecīgā pamataktā Finanšu regulas 49. panta nozīmē

☐ **Dalīta pārvaldība** kopā ar dalībvalstīm

☐ **Decentralizēta pārvaldība** kopā ar trešām valstīm

☐ **Pārvaldība kopā** ar starptautiskām organizācijām ***(precizēt)***

Ja norādīti vairāki pārvaldības veidi, sniedziet papildu informāciju iedaļā „Piezīmes”.

Piezīmes

[//]

[28] Kā paredzēts Finanšu regulas 185. pantā.

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

Norādīt periodiskumu un nosacījumus.

Pirmā izvērtēšana notiks 4 gadus pēc regulas stāšanās spēkā. Regulā ir skaidri iekļauts noteikums par ziņošanu, kam atbilstīgi Komisija ziņos Eiropas Parlamentam un Padomei par regulas piemērošanu. Turpmākos ziņojumus iesniegs ik pēc 4 gadiem. Piemēros Komisijas izvērtēšanas metodoloģiju. Šī izvērtēšana tiks veikta, izmantojot mērķtiecīgus pētījumus par tiesību aktu īstenošanu, aptaujājot valsts iestādes, rīkojot ekspertu diskusijas, darbsemināru, Eirobarometra aptaujas u.tml.

2.2. Pārvaldības un kontroles sistēma

2.2.1. Apzinātie riski

Ir veikts ietekmes novērtējums, kas pievienots regulas priekšlikumam. Jaunais tiesību akts nodrošinās elektroniskās identifikācijas savstarpēju atzīšanu un akceptēšanu pārrobežu līmenī, uzlabos pašreizējo regulējumu elektronisko parakstu jomā, nostiprinās valsts uzraudzību attiecībā uz uzticamības pakalpojumu sniedzējiem, piešķirs juridisku spēku saistītajiem uzticamības pakalpojumiem un nodrošinās to atzīšanu. Ar minēto tiesību aktu arī ieviests deleģēto un īstenošanas aktu izmantošanas mehānisms, nodrošinot elastīgumu attiecībā uz tehnoloģiju attīstību.

2.2.2. Paredzētās kontroles metodes

Esošās un Komisijas piemērotās kontroles metodes attieksies uz papildu apropriācijām.

2.3. Krāpšanas un pārkāpumu apkarošanas pasākumi

Norādīt esošos vai plānotos novēršanas un aizsardzības pasākumus.

Esošās un Komisijas piemērotās krāpšanas novēršanas metodes attieksies arī uz papildu apropriācijām.

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

- Esošās budžeta izdevumu pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām.

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Numurs [Izdevumu kategorija…...….]	Dif./nedif. (29)	no EBTA valstīm[30]	no kandidātvalstīm[31]	no trešām valstīm	Finanšu regulas 18. panta 1. punkta aa) apakšpunkta nozīmē
5	09 01 01 01 Izdevumi, kas saistīti ar Informācijas sabiedrības un plašsaziņas līdzekļu ģenerāldirektorātā aktīvi nodarbināto personālu	Nedif.	NĒ	NĒ	NĒ	NĒ
5	09 01 02 01 Ārštata darbinieki	Nedif.	NĒ	NĒ	NĒ	NĒ

29 Dif. – diferencētās apropriācijas / nedif. – nediferencētās apropriācijas.

30 EBTA: Eiropas Brīvās tirdzniecības asociācija.

31 Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Paredzamās ietekmes uz izdevumiem kopsavilkums

Daudzgadu finanšu shēmas izdevumu kategorija:	Numurs	[Izdevumu kategorija 1 **Gudra un iekļaujoša izaugsme** ……...……]

ĢD: INFSO			**2014.** gads	**2015.** gads	**2016.** gads	**2017.** gads	**2018.** gads	**2019.** gads	**2020.** gads	**KOPĀ**
• Darbības apropriācijas										
Budžeta pozīcijas numurs - N.A.	Saistības	(1)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Maksājumi	(2)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Budžeta pozīcijas numurs - N.A.	Saistības	(1a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Maksājumi	(2a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem[32]			0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Budžeta pozīcijas numurs		(3)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
KOPĀ – INFSO ĢD apropriācijas	Saistības	=1+1a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Maksājumi	=2+2a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**

Daudzgadu finanšu shēmas izdevumu	**5**	„Administratīvie izdevumi”

[32] Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās „*BA*” pozīcijas), netiešā pētniecība, tiešā pētniecība.

kategorija:		

Miljonos EUR (3 zīmes aiz komata)

		2014. gads	**2015.** gads	**2016.** gads	**2017.** gads	**2018.** gads	**2019.** gads	**2020.** gads	**KOPĀ**
		ĢD: INFSO							
• Cilvēkresursi		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Pārējie administratīvie izdevumi									
KOPĀ – INFSO ĢD	Apropriācijas	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

KOPĀ – Daudzgadu finanšu shēmas **5. IZDEVUMU KATEGORIJAS apropriācijas**	(Saistību summa = maksājumu summa)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Miljonos EUR (3 zīmes aiz komata)

		2014. gads	**2015.** gads	**2016.** gads	**2017.** gads	**2018.** gads	**2019.** gads	**2020.** gads	**KOPĀ**
KOPĀ – Daudzgadu finanšu shēmas **1.–5. IZDEVUMU KATEGORIJAS apropriācijas**	Saistības	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Maksājumi	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2. Paredzamā ietekme uz darbības apropriācijām

– ☑ Priekšlikums/iniciatīva neparedz darbības apropriāciju izmantošanu

– ☐ Priekšlikums/iniciatīva paredz darbības apropriāciju izmantošanu šādā veidā:

3.2.3. Paredzamā ietekme uz administratīvajām apropriācijām

3.2.3.1. Kopsavilkums

– ☐ Priekšlikums/iniciatīva neparedz administratīvo apropriāciju izmantošanu

– ☑ Priekšlikums/iniciatīva paredz administratīvo apropriāciju izmantošanu šādā veidā:

Miljonos EUR (3 zīmes aiz komata)

	N 2014. gads	**2015.** gads	**2016.** gads	**2017.** gads	**2018.** gads	**2019.** gads	**2020.** gads	**KOPĀ**
Daudzgadu finanšu shēmas 5. IZDEVUMU KATEGORIJA								
Cilvēkresursi	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Pārējie administratīvie izdevumi								
Starpsumma – Daudzgadu finanšu shēmas 5. IZDEVUMU KATEGORIJA	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Ārpus daudzgadu finanšu shēmas 5. IZDEVUMU KATEGORIJAS[33]								
Cilvēkresursi								
Citi administratīvie izdevumi								
Starpsumma – Ārpus daudzgadu finanšu shēmas 5. IZDEVUMU KATEGORIJAS								
KOPĀ	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās „*BA*" pozīcijas), netiešā pētniecība, tiešā pētniecība.

3.2.3.2. Paredzamās cilvēkresursu vajadzības

– ☐ Priekšlikums/iniciatīva neparedz cilvēkresursu izmantošanu
– ☑ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Paredzamais apjoms izsakāms veselos skaitļos (vai maksimāli ar vienu zīmi aiz komata)

		2014. gads	**2015.** gads	**2016.** gads	**2017.** gads	**2018.** gads	**2019.** gads	**2020.** gads
• Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)								
09 01 01 01 (Galvenā mītne un Komisijas pārstāvniecības)		9	9	9	9	9	9	9
XX 01 01 02 (Delegācijas)								
XX 01 05 01 (Netiešā pētniecība)								
10 01 05 01 (Tiešā pētniecība)								
• Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu – *FTE*)[34]								
09 01 02 01 (*CA*, *INT*, *SNE*, ko finansē no vispārīgajām apropriācijām)		3	3	3	3	3	3	3
XX 01 02 02 (*CA*, *INT*, *JED*, *LA* un *SNE* delegācijās)								
XX 01 04 ***yy*** [35]	- Galvenā mītne[36]							
	- Delegācijas							
XX 01 05 02 (*CA*, *INT*, *SNE* – netiešā pētniecība)								
10 01 05 02 (*CA*, *INT*, *SNE* – tiešā pētniecība)								
Citas budžeta pozīcijas (precizēt)								
KOPĀ		**12**	**12**	**12**	**12**	**12**	**12**	**12**

Cilvēkresursu vajadzības tiks nodrošinātas, izmantojot attiecīgā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ģenerāldirektorātā, vajadzības gadījumā izmantojot vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

Veicamo uzdevumu apraksts

Ierēdņi un pagaidu darbinieki	Organizēt likumdošanas procedūras ar mērķi Eiropas Parlamentā un Padomē pieņemt ierosināto regulu un saistītos deleģētos/īstenošanas aktus. Prioritārās jomas: 1. Izveidot jaunu tiesisko regulējumu elektronisko uzticamības pakalpojumu jomā 2. Veicināt elektronisko uzticamības pakalpojumu ieviešanu, palielinot MVU un iedzīvotāju informētību par šo pakalpojumu iespējām 3. Pārskats par Direktīvu 1999/93/EK, arī tās starptautiskajiem aspektiem

34 *CA* – līgumdarbinieki, *INT* – pagaidu darbinieki, *JED* – jaunākie eksperti delegācijās, *LA* – vietējie darbinieki, *SNE* –valstu norīkotie eksperti.

35 Saskaņā ar robežlielumiem attiecībā uz ārštata darbiniekiem, ko finansē no darbības apropriācijām (kādreizējām „*BA*" pozīcijām).

36 Galvenokārt struktūrfondiem, Eiropas Lauksaimniecības fondam lauku attīstībai (ELFLA) un Eiropas Zivsaimniecības fondam (EZF).

	4. Līdzsvaroti ieviest plaša mēroga izmēģinājuma projektus, lai paātrinātu jaunā tiesiskā regulējuma mērķa konkrētu īstenošanu
Ārštata darbinieki	Tāpat kā iepriekš

3.2.4. Saderība ar kārtējo daudzgadu finanšu shēmu

– ☑ Priekšlikums/iniciatīva atbilst kārtējai daudzgadu finanšu shēmai

– ☐ Pieņemot priekšlikumu/iniciatīvu, jāpārplāno attiecīgā izdevumu kategorija daudzgadu finanšu shēmā

Aprakstīt, kas jāpārplāno, norādot attiecīgās budžeta pozīcijas un summas.

– ☐ Pieņemot priekšlikumu/iniciatīvu, jāpiemēro elastības instruments vai jāpārskata daudzgadu finanšu shēma[37]

Aprakstīt, kas jādara, norādot attiecīgās izdevumu kategorijas, budžeta pozīcijas un summas.

3.2.5. Trešo personu iemaksas

– ☑ Priekšlikums/iniciatīva neparedz trešo personu līdzfinansējumu

– ☐ Priekšlikums/iniciatīva paredz šādu līdzfinansējumu:

3.3. Paredzamā ietekme uz ieņēmumiem

– ☑ Priekšlikums/iniciatīva finansiāli neietekmē ieņēmumus

– ☐ Priekšlikums/iniciatīva finansiāli ietekmē:

- ☐ pašu resursus
- ☐ dažādus ieņēmumus

[37] Skatīt Iestāžu nolīguma 19. un 24. punktu.