2024/1183

30.4.2024.

EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2024/1183

(2024. gada 11. aprīlis),

ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi

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 ([1]),

ņemot vērā Reģionu komitejas atzinumu ([2]),

saskaņā ar parasto likumdošanas procedūru ([3]),

tā kā:

(1) Komisija 2020. gada 19. februāra paziņojumā "Eiropas digitālās nākotnes veidošana" ([4]) paziņoja par Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 pārskatīšanu, lai uzlabotu tās efektivitāti, nodrošinātu, ka tās priekšrocības var izmantot arī privātais sektors, un veicinātu uzticamu digitālo identitāti visiem Eiropas iedzīvotājiem.

(2) Savos 2020. gada 1. un 2. oktobra secinājumos Eiropadome aicināja Komisiju ierosināt izstrādāt Savienības mērogā drošas publiskās elektroniskās identifikācijas, tostarp sadarbspējīgu digitālo parakstu, regulējumu, lai iedzīvotāji varētu kontrolēt savu tiešsaistes identitāti un datus, kā arī piekļūt publiskiem, privātiem un pārrobežu digitālajiem pakalpojumiem.

(3) Ar Eiropas Parlamenta un Padomes Lēmumu (ES) 2022/2481 ([5]) izveidotā politikas programma "Digitālās desmitgades ceļš" 2030. gadam izvirza Savienības satvara mērķus un digitālos mērķrādītājus, ar kuriem līdz 2030. gadam iecerēts panākt, ka tiek plaši izvērsta uzticama, brīvprātīga, lietotāja kontrolēta digitālā identitāte, kuru atzīst visā Savienībā un kura ļauj ikvienam lietotājam kontrolēt savus datus tiešsaistes mijiedarbībā.

(4) Eiropas Parlamenta, Padomes un Komisijas pasludinātā "Eiropas deklarācija par digitālajām tiesībām un principiem digitālajai desmitgadei" ([6]) ("deklarācija") uzsver ikviena tiesības uz piekļuvi digitālām tehnoloģijām, produktiem un pakalpojumiem, kas pēc būtības ir droši, aizsargāti un privātumu aizsargājoši. Tas ietver arī to, ka visiem Savienības iedzīvotājiem tiek piedāvāta pieejama, droša un uzticama digitālā identitāte, kas dod iespēju piekļūt plašam tiešsaistes un bezsaistes pakalpojumu klāstam, kuri ir aizsargāti pret jebkādiem kiberdrošības riskiem un kibernoziegumiem, tai skaitā identitātes zādzību vai manipulācijām. Deklarācijā arī ir norādīts, ka ikvienam ir tiesības uz savu personas datu aizsardzību. Minētās tiesības aptver kontroli pār to, kā dati tiek izmantoti un ar ko tie tiek kopīgoti.

([1]) OV C 105, 4.3.2022., 81. lpp.
([2]) OV C 61, 4.2.2022., 42. lpp.
([3]) Eiropas Parlamenta 2024. gada 29. februāra nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2024. gada 26. marta lēmums.
([4]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp.).
([5]) Eiropas Parlamenta un Padomes Lēmums (ES) 2022/2481 (2022. gada 14. decembris), ar ko izveido politikas programmu "Digitālās desmitgades ceļš" 2030. gadam (OV L 323, 19.12.2022., 4. lpp.).
([6]) OV C 23, 23.1.2023., 1. lpp.

(5) Savienības pilsoņiem un pastāvīgajiem iedzīvotājiem Savienībā vajadzētu būt tiesībām uz digitālo identitāti, kas ir viņu ekskluzīvā kontrolē un kas ļauj viņiem izmantot savas tiesības digitālajā vidē un piedalīties digitālajā ekonomikā. Lai sasniegtu minēto mērķi, būtu jāizveido Eiropas digitālās identitātes satvars, kas ļauj Savienības pilsoņiem un pastāvīgajiem iedzīvotājiem Savienībā piekļūt publiskiem un privātiem tiešsaistes un bezsaistes pakalpojumiem visā Savienībā.

(6) Saskaņotam digitālās identitātes satvaram būtu jāpalīdz izveidot digitāli integrētāku Savienību, samazinot digitālos šķēršļus starp dalībvalstīm un dodot Savienības pilsoņiem un pastāvīgajiem iedzīvotājiem Savienībā iespēju izmantot digitalizācijas sniegtās priekšrocības, vienlaikus palielinot pārredzamību un viņu tiesību aizsardzību.

(7) Saskaņotākai pieejai elektroniskai identifikācijai būtu jāsamazina pašreizējās sadrumstalotības riski un izmaksas, ko rada atšķirīgu valsts risinājumu lietošana vai dažās dalībvalstīs – šādu elektroniskās identifikācijas risinājumu trūkums. Šādai pieejai būtu jāstiprina iekšējais tirgus, ļaujot Savienības pilsoņiem, pastāvīgajiem iedzīvotājiem Savienībā, kas definēti valsts tiesību aktos, un uzņēmumiem identificēties un sniegt savas identitātes autentifikāciju tiešsaistē un bezsaistē drošā, uzticamā, lietotājdraudzīgā, ērtā, pieejamā un saskaņotā veidā visā Savienībā. Eiropas digitālās identitātes makam būtu fiziskām un juridiskām personām visā Savienībā jānodrošina saskaņoti elektroniskās identifikācijas līdzekļi, kas iespējo autentifikācijas veikšanu un ar viņu identitāti saistītu datu kopīgošanu. Ikvienam vajadzētu būt iespējai piekļūt publiskiem un privātiem pakalpojumiem drošā veidā, paļaujoties uz uzlabotu uzticamības pakalpojumu ekosistēmu un verificētiem identitātes pierādījumiem un elektroniskiem atribūtu apliecinājumiem, piemēram, akadēmisko kvalifikāciju, tostarp akadēmisko grādu, vai citu izglītības vai profesionālo statusu, apliecinājumiem. Ar Eiropas digitālās identitātes satvaru iecerēts panākt pāreju no paļaušanās vienīgi uz valstu digitālās identitātes risinājumiem uz tādu atribūtu elektronisko apliecinājumu sniegšanu, kas ir derīgi un juridiski atzīti visā Savienībā. Skaidram un vienotam noteikumu kopumam vajadzētu nest labumu atribūtu elektronisku apliecinājumu sniedzējiem, savukārt valsts iestādēm vajadzētu spēt paļauties uz elektroniskiem dokumentiem attiecīgā formātā.

(8) Vairākas dalībvalstis ir ieviesušas un izmanto elektroniskās identifikācijas līdzekļus, kurus pieņem pakalpojumu sniedzēji Savienībā. Turklāt ir veikti ieguldījumi gan valsts, gan pārrobežu risinājumos, pamatojoties uz Regulu (ES) Nr. 910/2014, tostarp paziņoto elektroniskās identifikācijas shēmu sadarbspējā, ievērojot minēto regulu. Lai nodrošinātu Eiropas digitālās identitātes maku papildināmību un pašreizējie paziņoto elektroniskās identifikācijas līdzekļu lietotāji tos ātri pieņemtu, un lai līdz minimumam samazinātu ietekmi uz esošajiem pakalpojumu sniedzējiem, paredzams, ka Eiropas digitālās identitātes makos balstīsies uz pieredzi, kas gūta ar esošajiem elektroniskās identifikācijas līdzekļiem, un Savienības un valstu līmenī izvērstu paziņotu elektroniskās identifikācijas shēmu infrastruktūru.

(9) Visām Regulā (ES) Nr. 910/2014 paredzētajām personas datu apstrādes darbībām piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([7]) un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([8]). Minētajiem noteikumiem atbilst arī risinājumi, kas noteikti šajā regulā paredzētajā sadarbspējas regulējumā. Savienības datu aizsardzības tiesības paredz datu aizsardzības principus, piemēram, datu minimizēšanas un mērķa ierobežošanas principu, un pienākumus, piemēram, integrētu datu aizsardzību pēc būtības un datu aizsardzību pēc noklusējuma.

(10) Lai atbalstītu Savienības uzņēmumu konkurētspēju, gan tiešsaistes, gan bezsaistes pakalpojumu sniedzējiem vajadzētu būt iespējai paļauties uz digitālās identitātes risinājumiem, kas atzīti visā Savienībā, neatkarīgi no dalībvalsts, kurā minētie risinājumi tiek nodrošināti, tādējādi gūstot labumu no Savienības saskaņotas pieejas uzticamībai, drošībai un sadarbspējai. Gan lietotājiem, gan pakalpojumu sniedzējiem vajadzētu būt iespējai gūt labumu no tāda paša juridiskā spēka, kas visā Savienībā ir paredzēts elektroniskiem atribūtu apliecinājumiem. Iecerēts, ka saskaņots digitālās identitātes satvars radīs ekonomisko vērtību, atvieglojot piekļuvi precēm un pakalpojumiem un būtiski samazinot darbību izmaksas, kas saistītas ar identifikācijas un autentifikācijas procedūrām, piemēram, jaunu klientu pievienošanas laikā, samazinot tādu kibernoziegumu iespējamību kā identitātes zādzība, datu zādzība un krāpšana tiešsaistē, un tādējādi veicinot efektivitātes ieguvumus un drošu Savienības mikrouzņēmumu un mazo un vidējo uzņēmumu (MVU) digitālo pārveidi.

([7]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

([8]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

(11) Digitālās identitātes Eiropas makiem būtu jāsekmē vienreizējas iesniegšanas principa izmantošana, tādējādi mazinot administratīvo slogu Savienības pilsoņiem un pastāvīgajiem iedzīvotājiem Savienībā un uzņēmumiem visā Savienībā un atbalstot to pārrobežu mobilitāti, un veicinot sadarbspējīgu e-pārvaldes pakalpojumu attīstību visā Savienībā.

(12) Personas datu apstrādei, ko veic šīs regulas īstenošanā, piemēro Regulu (ES) 2016/679, Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725 ([9]) un Direktīvu 2002/58/EK. Tāpēc šajā regulā būtu jāparedz konkrēti aizsardzības pasākumi, lai nepieļautu to, ka elektroniskās identifikācijas līdzekļu un elektronisko atribūtu apliecinājumu sniedzēji apvieno no citiem pakalpojumiem iegūtus personas datus ar personas datiem, kurus apstrādā, lai sniegtu pakalpojumus, uz ko attiecas šī regula. Personas datus, kas attiecas uz Eiropas digitālās identitātes maku nodrošināšanu, būtu jāglabā loģiski nošķirti no visiem citiem datiem, kurus tur Eiropas digitālās identitātes maka nodrošinātājs. Šai regulai nebūtu jāliedz Eiropas digitālās identitātes maku nodrošinātājiem piemērot papildu tehniskos pasākumus, kas veicina personas datu aizsardzību, piemēram, fiziski nošķirt ar Eiropas digitālās identitātes maku nodrošināšanu saistītus personas datus no visiem citiem datiem, kurus tur nodrošinātājs. Neskarot Regulu (ES) 2016/679, šī regula sīkāk precizē mērķa ierobežojuma, datu minimizēšanas principu un integrētas datu aizsardzības pēc būtības un datu aizsardzības pēc noklusējuma piemērošanu.

(13) Digitālās identitātes Eiropas makos vajadzētu būt iestrādātai kopīga infopaneļa funkcijai, lai nodrošinātu lielāku pārredzamību, privātumu un lietotāju kontroli pār saviem personas datiem. Minētajai funkcijai būtu jānodrošina vienkārša un lietotājdraudzīga saskarne ar pārskatu par visām atkarīgajām pusēm, ar kurām lietotājs kopīgo datus, tai skaitā atribūtus, un par to datu veidiem, kuri kopīgoti ar katru atkarīgo pusi. Tai būtu jādod lietotājiem iespēja izsekot visus darījumus, kas veikti ar Eiropas digitālās identitātes maka starpniecību, ar vismaz šādiem datiem: darījuma laiks un datums, darījuma partnera identifikācija, pieprasītie personas dati un kopīgotie dati. Minētā informācija būtu jāglabā pat tad, ja darījums nav noslēgts. Nevajadzētu būt iespējamam noliegt darījuma vēsturē ietvertās informācijas autentiskumu. Šādai funkcijai vajadzētu būt aktīvai pēc noklusējuma. Tai būtu jāļauj lietotājiem tieši no digitālās identitātes Eiropas maka vienkāršā veidā pieprasīt atkarīgajai pusei nekavējoties dzēst personas datus, ievērojot Regulas (ES) 2016/679 17. pantu, un vienkāršā veidā ziņot par atkarīgo pusi kompetentajai valsts datu aizsardzības iestādei, ja ir saņemts iespējami nelikumīgs vai aizdomīgs personas datu pieprasījums.

(14) Dalībvalstīm būtu Eiropas digitālās identitātes makā jāintegrē dažādas privātuma saglabāšanas tehnoloģijas, piemēram, patiesuma apliecinājums bez informācijas izpaušanas (*zero knowledge proof*). Minētajām kriptogrāfijas metodēm būtu jādod iespēja atkarīgajai pusei validēt to, vai konkrēts paziņojums, kas balstīts uz personas identifikācijas datiem un atribūtu apliecinājumu, ir patiess, neatklājot nekādus datus, uz kuriem minētais paziņojums ir balstīts, tādējādi saglabājot lietotāja privātumu.

(15) Šī regula paredz saskaņotus nosacījumus to Eiropas digitālās identitātes maku satvara izveidei, kurus nodrošinās dalībvalstis. Visiem Savienības pilsoņiem un pastāvīgajiem iedzīvotājiem Savienībā, kas definēti valstu tiesību aktos, būtu jādod iespēja lietotājdraudzīgā, ērtā veidā, lietotāja ekskluzīvā kontrolē, droši pieprasīt, atlasīt, apvienot, glabāt, dzēst, kopīgot un uzrādīt datus, kas saistīti ar viņu identitāti, un pieprasīt dzēst viņu personas datus, iespējojot selektīvu personas datu izpaušanu. Šī regula atspoguļo kopīgās Eiropas vērtības un tajā ievērotas pamattiesības, tiesiskās garantijas un atbildība, tādējādi aizsargājot demokrātisko sabiedrību un Savienības pilsoņus un pastāvīgos iedzīvotājus Savienībā. Tehnoloģijas, ko izmanto minēto mērķu sasniegšanai, būtu jāattīsta, virzoties uz augstāko drošības līmeni, privātumu, lietotāju ērtību, piekļūstamību, plašu lietojamību un netraucētu sadarbspēju. Dalībvalstīm visiem saviem pilsoņiem un pastāvīgajiem iedzīvotājiem būtu jānodrošina vienlīdzīga piekļuve digitālajai identifikācijai. Dalībvalstīm nebūtu tieši vai netieši jāierobežo tādu fizisku vai juridisku personu piekļuve publiskiem un privātiem pakalpojumiem, kuras neizmanto Eiropas digitālās identitātes makus, un būtu jādara pieejami piemēroti alternatīvi risinājumi.

([9]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

(16) Dalībvalstīm būtu jāpaļaujas uz šīs regulas piedāvātajām iespējām savā atbildībā nodrošināt Eiropas digitālās identitātes makus, ko izmanto fiziskas un juridiskas personas, kas dzīvo vai atrodas to teritorijā. Lai dalībvalstīm piedāvātu elastīgumu un izmantotu modernāko tehnoloģiju, šai regulai būtu jārada iespēja, ka Eiropas digitālās identitātes makus nodrošina tieši dalībvalsts pēc dalībvalsts pilnvarojuma vai neatkarīgi no dalībvalsts, bet tā, ka minētā dalībvalsts tos atzīst.

(17) Reģistrācijas nolūkos atkarīgajām pusēm būtu jāsniedz informācija, kas vajadzīga, lai varētu veikt to elektronisku identifikāciju un autentifikāciju Eiropas digitālās identitātes maku vajadzībām. Deklarējot savu iecerēto Eiropas digitālās identitātes maka lietošanu, atkarīgajām pusēm būtu jāsniedz informācija par datiem, kurus tās pieprasīs – ja tādus pieprasīs –, lai sniegtu savus pakalpojumus, un pieprasīšanas pamatojums. Atkarīgās puses reģistrācija atvieglo dalībvalstu veikto verifikāciju attiecībā uz atkarīgo pušu darbību likumību saskaņā ar Savienības tiesību aktiem. Šajā regulā paredzētajam reģistrācijas pienākumam nevajadzētu skart citos Savienības vai valsts tiesību aktos noteiktos pienākumus, piemēram, informāciju, kas datu subjektiem jāsniedz, ievērojot Regulu (ES) 2016/679. Atkarīgajām pusēm būtu jānodrošina atbilstība minētās regulas 35. un 36. pantā paredzētajām garantijām, jo īpaši veicot novērtējumus par ietekmi uz datu aizsardzību un pirms datu apstrādes apspriežoties ar kompetentajām datu aizsardzības iestādēm, ja novērtējumi par ietekmi uz datu aizsardzību liecina, ka apstrāde radītu augstu risku. Šādām garantijām būtu jāatbalsta likumīga personas datu apstrāde, ko veic atkarīgās puses, jo īpaši attiecībā uz īpašām datu kategorijām, piemēram, veselības datiem. Ar atkarīgo pušu reģistrāciju ir iecerēts uzlabot pārredzamību un uzticēšanos Eiropas digitālās identitātes maku lietošanai. Reģistrācijai vajadzētu būt izmaksu ziņā lietderīgai un samērīgai ar saistītajiem riskiem, lai panāktu, ka pakalpojumu sniedzēji to ievieš. Minētajā sakarībā reģistrācijai būtu jāparedz automatizētu procedūru izmantošana, tostarp dalībvalstu paļaušanās uz esošajiem reģistriem un to izmantošana, un tai nevajadzētu radīt pirmsautorizācijas procesu. Reģistrācijas procesam vajadzētu iespējot dažādus lietošanas gadījumus, kas var būt atšķirīgi attiecībā uz darbības režīmu, tiešsaistē vai bezsaistē, vai attiecībā uz prasību autentificēt ierīces saskarnei ar Eiropas digitālās identitātes maku. Reģistrācija būtu jāpiemēro tikai atkarīgajām pusēm, kas sniedz pakalpojumus, izmantojot digitālu mijiedarbību.

(18) Savienības pilsoņu un Savienībā esošo iedzīvotāju aizsardzība pret neatļautu vai krāpniecisku Eiropas digitālās identitātes maku izmantošanu ir ļoti svarīga, lai panāktu uzticēšanos Eiropas digitālās identitātes makiem un tos plaši ieviestu. Lietotājiem būtu jānodrošina efektīva aizsardzība pret šādu ļaunprātīgu izmantošanu. Jo īpaši, ja faktus, kas ir pamatā krāpnieciskai vai citādi nelikumīgai Eiropas digitālās identitātes maka izmantošanai, valsts tiesu iestāde konstatē citā procedūrā, uzraudzības struktūrām, kas ir atbildīgas par Eiropas digitālās identitātes maka izdevējiem, pēc paziņošanas būtu jāveic vajadzīgie pasākumi, lai nodrošinātu, ka atkarīgās puses reģistrācija un atkarīgo pušu iekļaušana autentifikācijas mehānismā tiek atsaukta vai apturēta līdz brīdim, kad paziņojošā iestāde apstiprina, ka konstatētie pārkāpumi ir novērsti.

(19) Visiem Eiropas digitālās identitātes makiem būtu jādod iespēja lietotājiem elektroniski identificēties un autentificēties tiešsaistē un bezsaistes režīmā pāri robežām, lai piekļūtu plašam publisku un privātu pakalpojumu klāstam. Neskarot dalībvalstu prerogatīvas attiecībā uz savu pilsoņu un pastāvīgo iedzīvotāju identifikāciju, Eiropas digitālās identitātes makus var izmantot arī valstu iestāžu, starptautisku organizāciju un Savienības iestāžu, struktūru, biroju un aģentūru institucionālajām vajadzībām. Autentifikācija bezsaistes režīmā būtu svarīga daudzās nozarēs, tostarp veselības aprūpes nozarē, kur pakalpojumus bieži sniedz, mijiedarbojoties klātienē, un vajadzētu būt iespējai e-receptēm izmantot QR kodus vai līdzīgas tehnoloģijas, lai verificētu autentiskumu. Lai izpildītu šajā regulā noteiktās drošības prasības, Eiropas digitālās identitātes makiem, kuriem attiecībā uz elektroniskās identifikācijas shēmām ir atsauce uz uzticamības līmeni "augsts", būtu jāizmanto potenciāls, ko piedāvā tādi pret viltojumiem droši risinājumi kā aizsardzības elementi. Eiropas digitālās identitātes makiem būtu arī jāļauj lietotājiem izveidot un izmantot kvalificētus elektroniskos parakstus un zīmogus, kas tiek pieņemti visā Savienībā. Tiklīdz fiziskas personas ir pievienotas Eiropas digitālās identitātes makam, tām vajadzētu būt iespējai to lietot, lai pēc noklusējuma un bez maksas parakstītu ar kvalificētiem elektroniskajiem parakstiem, neveicot nekādas papildu administratīvās procedūras. Lietotājiem būtu jāvar parakstīt vai apzīmogot pašpasludinātus apgalvojumus vai atribūtus. Lai panāktu, ka personas un uzņēmumi visā Savienībā varētu gūt labumu no vienkāršošanas un izmaksu samazināšanas, tostarp, iespējojot pārstāvības pilnvaras un e-pilnvaras, dalībvalstīm būtu jānodrošina Eiropas digitālās identitātes maki, kas paļaujas uz kopīgiem standartiem un tehniskajām specifikācijām, lai nodrošinātu netraucētu sadarbspēju un pienācīgi paaugstinātu IT drošības līmeni, stiprinātu noturību pret kiberuzbrukumiem un tādējādi ievērojami samazinātu iespējamos riskus, ko Savienības pilsoņiem, pastāvīgajiem iedzīvotājiem Savienībā un uzņēmumiem rada notiekošā digitalizācija. Tikai dalībvalstu kompetentās iestādes var nodrošināt augstu ticamības līmeni personas

identitātes noskaidrošanā un tādējādi sniegt pārliecību, ka persona, kas apgalvo vai pauž konkrētu identitāti, patiešām ir tā persona, par kuru tā uzdodas. Tāpēc Eiropas digitālās identitātes maku nodrošināšanas pamatā ir jābūt Savienības pilsoņu, Savienības pastāvīgo iedzīvotāju vai juridisko personu juridiskajai identitātei. Tam, ka pamatā ir juridiskā identitāte, nevajadzētu traucēt Eiropas digitālās identitātes maka lietotājiem piekļūt pakalpojumiem, izmantojot pseidonīmus, ja nav juridiskas prasības, ka autentifikācijai ir vajadzīga juridiska identitāte. Uzticēšanās Eiropas digitālās identitātes makiem tiktu vairota, ja to izdevējiem un pārvaldītājiem prasītu īstenot atbilstošus tehniskos un organizatoriskos pasākumus, kas garantē visaugstāko drošības līmeni, kurš ir samērīgs ar riskiem, kas tiek radīti fizisku personu tiesībām un brīvībām, saskaņā ar Regulu (ES) 2016/679.

(20) Kvalificēta elektroniskā paraksta lietošanai vajadzētu būt bez maksas visām fiziskām personām neprofesionālos nolūkos. Dalībvalstīm vajadzētu būt iespējai paredzēt pasākumus, lai novērstu to, ka fiziskas personas bez maksas lieto kvalificētus elektroniskos parakstus profesionālos nolūkos, vienlaikus nodrošinot, ka šādi pasākumi ir samērīgi ar apzinātajiem riskiem un ir pamatoti.

(21) Ir lietderīgi veicināt Eiropas digitālās identitātes maku ieviešanu un izmantošanu, tos vienmērīgi integrējot publiskā un privātā sektora digitālo pakalpojumu ekosistēmā, kas jau ir īstenota valsts, vietējā vai reģionālajā līmenī. Lai sasniegtu šo mērķi, dalībvalstīm vajadzētu būt iespējai paredzēt juridiskus un organizatoriskus pasākumus, ar ko uzlabo Eiropas digitālās identitātes maku nodrošinātāju elastīgumu un Eiropas digitālās identitātes makiem ļauj nodrošināt vēl citas funkcionalitātes papildus tām, kas paredzētas šajā regulā, tostarp, šim nolūkam uzlabojot sadarbspēju ar esošajiem valsts elektroniskās identifikācijas līdzekļiem. Šādām papildu funkcionalitātēm nekādā gadījumā nevajadzētu nelabvēlīgi ietekmēt šajā regulā paredzēto Eiropas digitālās identitātes maku pamatfunkciju nodrošināšanu, nedz arī veicināt esošo valsts risinājumu izmantošanu Eiropas digitālās identitātes maku vietā. Tā kā šādas papildu funkcionalitātes pārsniedz šīs regulas tvērumu, tās negūst labumu no šajā regulā paredzētajiem noteikumiem par Eiropas digitālās identitātes maku izmantošanu pāri robežām.

(22) Eiropas digitālās identitātes makos būtu jāiekļauj funkcionalitāte, kas ģenerē lietotāju izvēlētus un pārvaldītus pseidonīmus, lai autentificētos, piekļūstot tiešsaistes pakalpojumiem.

(23) Lai sasniegtu augstu drošības un uzticamības līmeni, šajā regulā ir noteiktas prasības Eiropas digitālās identitātes makiem. Eiropas digitālās identitātes maku atbilstība minētajām prasībām būtu jāsertificē akreditētām atbilstības novērtēšanas struktūrām, ko izraudzījušās dalībvalstis.

(24) Lai izvairītos no atšķirīgām pieejām un saskaņotu šajā regulā noteikto prasību īstenošanu, Komisijai nolūkā sertificēt Eiropas digitālās identitātes makus būtu jāpieņem īstenošanas akti, lai noteiktu atsauces standartu sarakstu, un, ja nepieciešams, izstrādātu specifikācijas un procedūras ar mērķi formulēt detalizētas minēto prasību tehniskās specifikācijas. Ciktāl Eiropas digitālās identitātes maku atbilstības attiecīgajām kiberdrošības prasībām sertifikāciju neaptver esošās kiberdrošības sertifikācijas shēmas, kas minētas šajā regulā, un attiecībā uz ar kiberdrošību nesaistītām prasībām, kas attiecas uz Eiropas digitālās identitātes makiem, dalībvalstīm būtu jāizveido valsts sertifikācijas shēmas, ievērojot saskaņotas prasības, kas paredzētas šajā regulā un pieņemtas, ievērojot to. Dalībvalstīm savi valstu sertifikācijas shēmu projekti būtu jānosūta Eiropas Digitālās identitātes sadarbības grupai, kurai vajadzētu būt iespējai sniegt atzinumus un ieteikumus.

(25) Sertifikācijas par atbilstību šajā regulā noteiktajām kiberdrošības prasībām pamatā vajadzētu būt attiecīgās Eiropas kiberdrošības sertifikācijas shēmām, ja tādas pieejamas, kuras izveidotas, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2019/881 ([10]), kas izveido brīvprātīgu Eiropas kiberdrošības sertifikācijas satvaru IKT produktiem, procesiem un pakalpojumiem.

([10]) Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

(26) Lai pastāvīgi novērtētu un mazinātu ar drošību saistītus riskus, attiecībā uz sertificētiem Eiropas digitālās identitātes makiem būtu jāveic regulāri ievainojamības novērtējumi, kuru mērķis ir atklāt jebkādu ievainojamību ar sertificētiem produktiem, procesiem un pakalpojumiem saistītos Eiropas digitālās identitātes maka komponentos.

(27) Aizsargājot lietotājus un uzņēmumus no kiberdrošības riskiem, šajā regulā noteiktās kiberdrošības pamatprasības arī palīdz uzlabot personas datu un indivīdu privātuma aizsardzību. Būtu jāapsver sinerģija gan standartizācijas, gan sertifikācijas jomā attiecībā uz kiberdrošības aspektiem, kurā izmantotu sadarbību starp Komisiju, Eiropas standartizācijas organizācijām, Eiropas Savienības Kiberdrošības aģentūru (*ENISA*), ar Regulu (ES) 2016/679 izveidoto Eiropas Datu aizsardzības kolēģiju un valstu datu aizsardzības uzraudzības iestādēm.

(28) Savienības pilsoņu un Savienības pastāvīgo iedzīvotāju pievienošana Eiropas digitālās identitātes makiem būtu jāatvieglo, izmantojot elektroniskās identifikācijas līdzekļus, kas izdoti ar uzticamības līmeni "augsts". Elektroniskās identifikācijas līdzekļi, kas izdoti ar uzticamības līmeni "būtisks", būtu jāizmanto vienīgi tad, ja saskaņotas tehniskās specifikācijas un procedūras, kurās izmanto elektroniskās identifikācijas līdzekļus, kas izdoti ar uzticamības līmeni "būtisks", kopā ar citiem papildu identitātes verifikācijas līdzekļiem ļaus izpildīt šajā regulā izklāstītās prasības attiecībā uz ar uzticamības līmeni "augsts". Šādiem papildu līdzekļiem vai pasākumiem vajadzētu būt uzticamiem un viegli lietojamiem, un to pamatā varētu būt iespēja izmantot attālinātas pievienošanas procedūras, kvalificētus sertifikātus, kas apliecināti ar kvalificētiem elektroniskajiem parakstiem, kvalificētus elektroniskos atribūtu apliecinājumus vai to kombināciju. Lai nodrošinātu, ka Eiropas digitālās identitātes maki tiek pietiekami ieviesti, īstenošanas aktos būtu jāparedz harmonizētas tehniskās specifikācijas un procedūras lietotāju pievienošanai ar elektroniskās identifikācijas līdzekļiem, tostarp tādiem, kas izdoti ar uzticamības līmeni "būtisks".

(29) Šīs regulas mērķis ir lietotājam nodrošināt pilnībā mobilu, drošu un lietotājdraudzīgu Eiropas digitālās identitātes maku. Kā pārejas pasākumu, līdz būs pieejami sertificēti, pret viltojumiem droši risinājumi, piemēram, aizsardzības elementi lietotāju ierīcēs, Eiropas digitālās identitātes makiem būtu jāvar izmantot sertificētus ārējos aizsardzības elementus, lai aizsargātu kriptogrāfijas materiālus un citus sensitīvus datus, vai izmantot paziņotus elektroniskās identifikācijas līdzekļus ar uzticamības līmeni "augsts", lai apliecinātu atbilstību šīs regulas prasībām attiecībā uz Eiropas digitālās identitātes maka uzticamības līmeni. Šai regulai nebūtu jāskar valstu nosacījumi attiecībā uz sertificēta ārēja aizsardzības elementa izdošanu un izmantošanu gadījumā, ja pārejas pasākums ir no tā atkarīgs.

(30) Eiropas digitālās identitātes makiem būtu jāgarantē augstākais datu aizsardzības un drošības līmenis elektroniskās identifikācijas un autentifikācijas nolūkos, lai atvieglotu piekļuvi publiskiem un privātiem pakalpojumiem, neatkarīgi no tā, vai šādi dati tiek glabāti lokāli vai mākoņdatošanas risinājumos, pienācīgi ņemot vērā dažādos riska līmeņus.

(31) Eiropas digitālās identitātes makiem vajadzētu būt integrētā veidā drošiem un tiem būtu jāīsteno uzlaboti drošības elementi, kas aizsargā pret identitātes un citu datu zādzību, pakalpojuma atteikumu un jebkādiem citiem kiberdraudiem. Šādai drošībai būtu jāietver vismodernākās šifrēšanas un glabāšanas metodes, kurām piekļūt un kuras atšifrēt var vienīgi lietotājs, un tajā būtu jāizmanto pilnīgi šifrēti sakari ar citiem Eiropas digitālās identitātes makiem un atkarīgajām pusēm. Turklāt Eiropas digitālās identitātes makiem būtu jāpieprasa drošs, nepārprotams un aktīvs lietotāju apstiprinājums operācijām, kuras veic, izmantojot Eiropas digitālās identitātes makus.

(32) Eiropas digitālās identitātes makulietošanai bez maksas nevajadzētu novest pie datu apstrādes, kas pārsniedz tos datus, kas ir nepieciešami Eiropas digitālās identitātes maka pakalpojumu sniegšanai. Šai regulai nebūtu jāatļauj tādu personas datu apstrāde, kuri glabājas Eiropas digitālās identitātes makā vai izriet no tā, ka Eiropas digitālās identitātes maka nodrošinātājs Eiropas digitālās identitātes maku izmanto citiem nolūkiem nekā Eiropas digitālās identitātes maka pakalpojumu sniegšana. Lai nodrošinātu privātumu, Eiropas digitālās identitātes maka nodrošinātājiem, nevācot datus un negūstot ieskatu par Eiropas digitālās identitātes maka lietotāju darījumiem, būtu jānodrošina neiespējamība novērot. Šāda neiespējamība novērot nozīmē, ka nodrošinātāji neredz sīkāku informāciju par lietotāja veiktajiem darījumiem. Tomēr konkrētos gadījumos, pamatojoties uz lietotāja iepriekš nepārprotami sniegtu piekrišanu katrā šādā konkrētā gadījumā un pilnīgi saskaņā ar Regulu (ES) 2016/679, Eiropas digitālās identitātes

maku nodrošinātājiem varētu atļaut piekļūt informācijai, kas ir nepieciešama konkrēta ar Eiropas digitālās identitātes makiem saistīta pakalpojuma sniegšanai.

(33) Eiropas digitālās identitātes maku pārredzamība un to nodrošinātāju pārskatatbildība ir būtiski elementi tam, lai radītu sabiedrības uzticēšanos un sekmētu satvara pieņemšanu. Tādēļ Eiropas digitālās identitātes maka darbībai vajadzētu būt pārredzamai un jo īpaši būtu jānodrošina verificējama personas datu apstrāde. Lai to panāktu, dalībvalstīm būtu jāizpauž Eiropas digitālās identitātes maku lietotāja lietojumprogrammatūras komponentu pirmkods, tostarp to, kuri ir saistīti ar personas datu un juridisku personu datu apstrādi. Šā pirmkoda publicēšanai saskaņā ar atvērtā pirmkoda licenci būtu jādod iespēja sabiedrībai, tostarp lietotājiem un izstrādātājiem, izprast tā darbību, veikt koda revīziju un pārskatīšanu. Tas palielinātu lietotāju uzticēšanos ekosistēmai un sekmētu Eiropas digitālās identitātes maku drošību, dodot iespēju ikvienam ziņot par ievainojamībām un kļūdām kodā. Kopumā tam būtu jārada stimuls piegādātājiem izstrādāt un uzturēt ļoti drošu produktu. Tomēr atsevišķos gadījumos dalībvalstis, norādot pienācīgi pamatotus iemeslus, jo īpaši sabiedriskās drošības nolūkos, varētu ierobežot pirmkoda izpaušanu izmantotajām bibliotēkām, sakaru kanālam vai citiem elementiem, kas netiek mitināti lietotāja ierīcē.

(34) Eiropas digitālās identitātes maku izmantošanai, kā arī to izmantošanas pārtraukšanai vajadzētu būt ekskluzīvām lietotāju tiesībām un izvēlei. Dalībvalstīm būtu jāizstrādā vienkāršas un drošas procedūras, kā lietotāji pieprasa tūlītēju Eiropas digitālās identitātes maku derīguma atsaukšanu, tostarp pazaudēšanas vai zādzības gadījumā. Lietotāja nāves gadījumā vai juridiskas personas darbības izbeigšanas gadījumā būtu jāizveido mehānisms, kas ļautu iestādei, kura ir atbildīga par fiziskās personas mantojuma kārtošanu vai juridiskās personas aktīviem, pieprasīt tūlītēju Eiropas digitālās identitātes maka atsaukšanu.

(35) Lai veicinātu Eiropas digitālās identitātes maku ieviešanu un plašāku digitālo identitāšu izmantošanu, dalībvalstīm būtu ne tikai jāpopularizē attiecīgo pakalpojumu priekšrocības, bet arī sadarbībā ar privāto sektoru, pētniekiem un akadēmiskajām aprindām būtu jāizstrādā mācību programmas ar mērķi stiprināt dalībvalstu pilsoņu un pastāvīgo iedzīvotāju digitālās prasmes, jo īpaši attiecībā uz neaizsargātām grupām, piemēram, personām ar invaliditāti un vecāka gadagājuma cilvēkiem. Dalībvalstīm, veicot komunikācijas kampaņas, arī būtu jāpalielina informētība par Eiropas digitālās identitātes maku priekšrocībām un riskiem.

(36) Lai nodrošinātu Eiropas digitālās identitātes satvara pieejamību inovācijām, tehnoloģiju attīstībai un atbilst nākotnes prasībām, dalībvalstis tiek mudinātas kopīgi izveidot "smilškastes", lai kontrolētā un drošā vidē testētu novatoriskus risinājumus, jo īpaši, lai uzlabotu risinājumu funkcionalitāti, personas datu aizsardzību, drošību un sadarbspēju un informētu par turpmākiem tehnisko atsauču un juridisko prasību atjauninājumiem. Minētajai videi būtu jāveicina MVU, jaunuzņēmumu un individuālu novatoru un pētnieku, kā arī attiecīgo nozares ieinteresēto personu iekļaušana. Šādām iniciatīvām būtu jāsekmē un jāstiprina Eiropas digitālās identitātes maku, ko paredzēts nodrošināt Savienības pilsoņiem un pastāvīgajiem iedzīvotājiem Savienībā, atbilstība satvaram un tehniskā noturība, tādējādi nepieļaujot tādu risinājumu izstrādi, kuri neatbilst Savienības tiesību aktiem par datu aizsardzību vai kuros varētu rasties ievainojamības drošības jomā.

(37) Eiropas Parlamenta un Padomes Regula (ES) 2019/1157 ([11]) līdz 2021. gada augustam pastiprina personas apliecību drošību ar uzlabotiem drošības elementiem. Dalībvalstīm būtu jāapsver iespēja tās paziņot saskaņā ar elektroniskās identifikācijas shēmām, lai paplašinātu elektroniskās identifikācijas līdzekļu pieejamību pāri robežām.

(38) Elektroniskās identifikācijas shēmu paziņošanas process būtu jāvienkāršo un jāpaātrina, lai veicinātu piekļuvi ērtiem, uzticamiem, drošiem un novatoriskiem autentifikācijas un identifikācijas risinājumiem un attiecīgā gadījumā mudinātu privātus identitātes nodrošinātājus piedāvāt elektroniskās identifikācijas shēmas dalībvalstu iestādēm, lai par tām paziņotu kā par valsts elektroniskās identifikācijas shēmām atbilstoši Regulai (ES) Nr. 910/2014.

([11]) Eiropas Parlamenta un Padomes Regula (ES) 2019/1157 (2019. gada 20. jūnijs) par Savienības pilsoņu personas apliecību un Savienības pilsoņiem un viņu ģimenes locekļiem, kuri izmanto tiesības brīvi pārvietoties, izsniegto uzturēšanās dokumentu drošības uzlabošanu (OV L 188, 12.7.2019., 67. lpp.).

(39) Pašreizējo paziņošanas un mācīšanās no līdzbiedriem procedūru racionalizēšana novērsīs dažādas pieejas dažādu paziņoto elektroniskās identifikācijas shēmu novērtēšanā un veicinās dalībvalstu savstarpējo uzticēšanos. Jauni, vienkāršoti mehānismi paredzēti, lai veicinātu dalībvalstu sadarbību to paziņoto elektroniskās identifikācijas shēmu drošības un sadarbspējas jomā.

(40) Dalībvalstīm būtu jāgūst labums no jauniem, elastīgiem rīkiem, ar kuriem nodrošina atbilstību šīs regulas un saskaņā ar to pieņemto attiecīgo īstenošanas aktu prasībām. Šai regulai būtu jāļauj dalībvalstīm izmantot ziņojumus un novērtējumus, ko veikušas akreditētas atbilstības novērtēšanas struktūras, kā paredzēts saistībā ar sertifikācijas shēmām, kas saskaņā ar Regulu (ES) 2019/881 jāizveido Savienības līmenī, lai atbalstītu savas prasības par shēmu vai to daļu saskaņošanu ar regulu (ES) Nr. 910/2014.

(41) Publisko pakalpojumu sniedzēji izmanto personas identifikācijas datus, kas pieejami no elektroniskajiem identifikācijas līdzekļiem, ievērojot Regulu (ES) Nr. 910/2014, lai saskaņotu citu dalībvalstu lietotāju elektronisko identitāti ar personas identifikācijas datiem, kas minētajiem lietotājiem ir piešķirti dalībvalstī, kura veic pārrobežu identitātes saskaņošanas procesu. Tomēr daudzos gadījumos, neraugoties uz to, ka tiek izmantoti minimuma datu kopumi, kas sniegti paziņoto elektroniskās identifikācijas shēmu ietvaros, lai nodrošinātu pareizu identitātes saskaņošanu tad, kad dalībvalstis rīkojas kā atkarīgās puses, ir vajadzīga papildu informācija par lietotāju un konkrētas papildinošas unikālās identifikācijas procedūras, kas jāveic valstu līmenī. Lai vēl vairāk atbalstītu elektroniskās identifikācijas līdzekļu lietojamību, nodrošinātu labākus publiskos pakalpojumus tiešsaistē un vairotu juridisko noteiktību saistībā ar lietotāju elektronisko identitāti, Regulai (ES) Nr. 910/2014 būtu jāprasa dalībvalstīm veikt konkrētus tiešsaistes pasākumus, lai nodrošinātu nekļūdīgu identitātes saskaņošanu, kad lietotāji ir iecerējuši piekļūt pārrobežu publiskajiem tiešsaistes pakalpojumiem.

(42) Izstrādājot Eiropas digitālās identitātes makus, ir svarīgi ņemt vērā lietotāju vajadzības. Vajadzētu būt pieejamiem jēgpilnas izmantošanas gadījumiem un tiešsaistes pakalpojumiem, kuros tiek izmantoti Eiropas digitālās identitātes maki. Lietotāju ērtībai un nolūkā nodrošināt šādu pakalpojumu pieejamību pārrobežu mērogā, ir svarīgi veikt darbības, ar kurām tiek sekmēta līdzīga pieeja tiešsaistes pakalpojumu projektēšanā, izstrādē un ieviešanā visās dalībvalstīs. Lai sasniegtu minēto mērķi, par lietderīgu instrumentu var kļūt nesaistošas pamatnostādnes, kā projektēt, izstrādāt un ieviest tiešsaistes pakalpojumus, kuros tiek izmantoti Eiropas digitālās identitātes maki. Šādas pamatnostādnes būtu jāsagatavo, ņemot vērā Savienības sadarbspējas regulējumu. Dalībvalstīm vajadzētu būt vadošai lomai minēto pamatnostādņu pieņemšanā.

(43) Saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2019/882 ([12]) personām ar invaliditāti būtu jāspēj vienlīdzīgi ar citiem lietotājiem lietot Eiropas digitālās identitātes makus, uzticamības pakalpojumus un tiešo lietotāju produktus, ko izmanto šo pakalpojumu sniegšanā.

(44) Lai nodrošinātu efektīvu šīs regulas izpildi, būtu jānosaka administratīvo naudas sodu maksimālā apmēra minimums gan kvalificētiem, gan nekvalificētiem uzticamības pakalpojumu sniedzējiem. Dalībvalstīm būtu jāparedz iedarbīgi, samērīgi un atturoši sodi. Nosakot sankcijas, būtu pienācīgi jāņem vērā skarto subjektu lielums, to uzņēmējdarbības modeļi un pārkāpumu smagums.

(45) Dalībvalstīm būtu jāparedz noteikumi attiecībā uz sankcijām par pārkāpumiem, piemēram, par tiešu vai netiešu praksi, kas rada nekvalificētu un kvalificētu uzticamības pakalpojumu sajaukšanu vai ļaunprātīgu ES uzticamības zīmes izmantošanu, ko veic nekvalificēti uzticamības pakalpojumu sniedzēji. ES uzticamības zīmi nevajadzētu izmantot apstākļos, kas tieši vai netieši liek uzskatīt, ka minēto pakalpojumu sniedzēju piedāvātie nekvalificētie uzticamības pakalpojumi ir kvalificēti.

(46) Šai regulai nebūtu jāattiecas uz tiem aspektiem, kas ir saistīti ar līgumu slēgšanu vai citu juridisku saistību uzņemšanos un šādu līgumu vai saistību derīgumu, ja attiecībā uz to veidu prasības noteiktas Savienības vai valsts tiesību aktos. Turklāt tai nebūtu jāietekmē valstu formātam izvirzītās prasības, kas attiecas uz publiskiem reģistriem, jo īpaši komercreģistriem un zemes reģistriem.

([12]) Eiropas Parlamenta un Padomes Direktīva (ES) 2019/882 (2019. gada 17. aprīlis) par produktu un pakalpojumu piekļūstamības prasībām (OV L 151, 7.6.2019., 70. lpp.).

(47) Uzticamības pakalpojumu sniegšana un lietošana un to sniegtie ieguvumi ērtības un juridiskās noteiktības ziņā pārrobežu darījumu kontekstā, jo īpaši tad, ja tiek izmantoti kvalificēti uzticamības pakalpojumi, kļūst arvien nozīmīgāki starptautiskajā tirdzniecībā un sadarbībā. Savienības starptautiskie partneri veido uzticamības regulējumus, iedvesmojoties no Regulas (ES) Nr. 910/2014. Lai atvieglotu kvalificētu uzticamības pakalpojumu un to sniedzēju atzīšanu, Komisija var pieņemt īstenošanas aktus, lai paredzētu nosacījumus, saskaņā ar kuriem trešo valstu uzticamības regulējumus varētu uzskatīt par līdzvērtīgiem šajā regulā paredzētajam kvalificētu uzticamības pakalpojumu un to sniedzēju satvaram. Šādai pieejai būtu jāpapildina Savienībā un trešās valstīs iedibinātu uzticamības pakalpojumu un to sniedzēju savstarpējās atzīšanas iespēja saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 218. pantu. Paredzot nosacījumus, saskaņā ar kuriem trešo valstu uzticamības regulējumus varētu uzskatīt par līdzvērtīgiem regulā (ES) Nr. 910/2014 paredzētajam kvalificētu uzticamības pakalpojumu un to sniedzēju satvaram, būtu jānodrošina, ka tiek ievēroti attiecīgie Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2555 ([13]) un Regulas (ES) 2016/679 noteikumi un ka uzticamības saraksti tiek izmantoti kā būtiski elementi, lai panāktu uzticēšanos.

(48) Šai regulai būtu jāveicina izvēle un iespēja pāriet no viena Eiropas digitālās identitātes maka uz citu, ja dalībvalsts savā teritorijā ir apstiprinājusi vairāk nekā vienu Eiropas digitālās identitātes maka risinājumu. Lai šādās situācijās nepieļautu iesīkstes efektu, Eiropas digitālās identitātes maku nodrošinātājiem, ja tas ir tehniski iespējams, būtu jānodrošina efektīva datu pārnesamība pēc Eiropas digitālās identitātes maka lietotāju pieprasījuma, un tiem nevajadzētu būt atļautam izmantot līgumiskus, ekonomiskus vai tehniskus šķēršļus, lai nepieļautu reālu pāriešanu no viena Eiropas digitālās identitātes maka uz citu vai lai atturētu no šādas pāriešanas.

(49) Lai nodrošinātu pareizu Eiropas digitālās identitātes maku darbību, Eiropas digitālās identitātes makunodrošinātājiem ir vajadzīga efektīva sadarbspēja un taisnīgi, saprātīgi un nediskriminējoši nosacījumi Eiropas digitālās identitātes maku piekļuvei konkrētām mobilo ierīču aparatūras un programmatūras funkcijām. Minētie komponenti varētu ietvert jo īpaši tuvā lauka sakaru antenas un aizsardzības elementus, tostarp universālās integrālshēmas kartes, iegultus aizsardzības elementus, mikroSD kartes un *Bluetooth Low Energy*. Piekļuve minētajiem komponentiem varētu būt mobilo tīklu operatoru un aprīkojuma ražotāju kontrolē. Tāpēc, ja tas nepieciešams Eiropas digitālās identitātes maku pakalpojumu sniegšanai, mobilo ierīču oriģinālā aprīkojuma ražotājiem vai elektronisko sakaru pakalpojumu sniedzējiem nebūtu jāatsaka piekļuve šādiem komponentiem. Turklāt uz uzņēmumiem, kas izraudzīti par platformas pamatpakalpojumu vārtziņiem, kurus Komisija uzskaitījusi, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2022/1925 ([14]), būtu joprojām jāattiecas minētās regulas konkrētajiem nosacījumiem, balstoties uz tās 6. panta 7. punktu.

(50) Lai racionalizētu uzticamības pakalpojumu sniedzējiem uzliktos kiberdrošības pienākumus, kā arī ļautu minētajiem pakalpojumu sniedzējiem un to attiecīgajām kompetentajām iestādēm gūt labumu no tiesiskā satvara, kas izveidots ar Direktīvu (ES) 2022/2555, uzticamības pakalpojumiem ir jāveic atbilstoši tehniski un organizatoriski pasākumi saskaņā ar minēto Direktīvu, piemēram, pasākumi, kas vērsti uz sistēmas kļūmēm, cilvēku kļūdām, ļaunprātīgām darbībām vai dabas parādībām, lai pārvaldītu riskus, ko rada tāda tīkla un informācijas sistēmu drošība, ko šie pakalpojumu sniedzēji izmanto, lai saskaņā ar minēto Direktīvu sniegtu savus pakalpojumus un ziņotu par nozīmīgiem incidentiem un kiberdraudiem. Attiecībā uz ziņošanu par incidentiem uzticamības pakalpojumu sniedzējiem būtu jāpaziņo par jebkādiem incidentiem, kuriem ir būtiska ietekme uz to pakalpojumu sniegšanu, tostarp par tādiem, ko izraisījusi ierīču zādzība vai nozaudēšana, tīkla kabeļa bojājumi vai incidenti, kas radušies saistībā ar personu identificēšanu. Kiberdrošības riska pārvaldības prasības un ziņošanas pienākumi saskaņā ar Direktīvu (ES) 2022/2555 būtu jāuzskata par tādiem, kuri papildina prasības, kas uzticamības pakalpojumu sniedzējiem noteiktas saskaņā ar šo regulu. Attiecīgā gadījumā saskaņā ar Direktīvu (ES) 2022/2555 izraudzītajām kompetentajām iestādēm arī turpmāk būtu jāpiemēro iedibinātā valsts prakse vai norādījumi par drošības un ziņošanas prasību īstenošanu un šādu prasību ievērošanas pārraudzību, kā paredzēts Regulā (ES) Nr. 910/2014. Šī regula neietekmē pienākumu ziņot par personas datu pārkāpumiem, ievērojot Regulu (ES) 2016/679.

([13]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).

([14]) Eiropas Parlamenta un Padomes Regula (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) (OV L 265, 12.10.2022., 1. lpp.).

(51) Pienācīgi būtu jāapsver efektīvas sadarbības nodrošināšanai starp uzraudzības iestādēm, kas izraudzītas, ievērojot Regulas (ES) Nr. 910/2014 46.b pantu, un kompetentajām iestādēm, kas izraudzītas vai izveidotas, ievērojot Direktīvas (ES) 2022/2555 8. panta 1. punktu. Gadījumos, kad uzraudzības iestāde atšķiras no kompetentās iestādes, tām būtu cieši un laikus jāsadarbojas, apmainoties ar attiecīgo informāciju, lai nodrošinātu efektīvu uzraudzību un uzticamības pakalpojumu sniedzēju atbilstību Regulā (ES) Nr. 910/2014 un Direktīvā (ES) 2022/2555 noteiktajām prasībām. Jo īpaši uzraudzības iestādēm, kas izraudzītas, ievērojot Regulu (ES) Nr. 910/2014, vajadzētu būt tiesībām lūgt kompetentās iestādes, kas izraudzītas vai izveidotas, ievērojot Direktīvu (ES) 2022/2555, sniegt attiecīgo informāciju, kas vajadzīga kvalificēta statusa piešķiršanai, un veikt uzraudzības darbības, lai pārbaudītu uzticamības pakalpojumu sniedzēju atbilstību attiecīgajām Direktīvā (ES) 2022/2555 paredzētajām prasībām, vai likt viņiem novērst neatbilstību.

(52) Ir būtiski izveidot tiesisko regulējumu, kas atvieglo pārrobežu atzīšanu starp esošajām valstu tiesību sistēmām attiecībā uz elektroniski reģistrētiem piegādes pakalpojumiem. Minētais satvars varētu arī radīt jaunas tirgus iespējas Savienības uzticamības pakalpojumu sniedzējiem piedāvāt jaunus elektroniski reģistrētus piegādes pakalpojumus visā Savienībā. Lai nodrošinātu, ka dati ar kvalificētu elektroniski reģistrētu piegādes pakalpojumu tiek piegādāti pareizajam adresātam, kvalificētiem elektroniski reģistrētiem piegādes pakalpojumiem būtu jānodrošina pilnīga adresāta identifikācijas precizitāte, savukārt attiecībā uz sūtītāja identifikāciju būtu pietiekama identifikācija ar augstu ticamības līmeni. Dalībvalstīm būtu jāmudina kvalificētu elektroniski reģistrētu piegādes pakalpojumu sniedzēji nodrošināt savu pakalpojumu sadarbspēju ar kvalificētiem elektroniski reģistrētiem piegādes pakalpojumiem, kurus sniedz citi kvalificētu uzticamības pakalpojumu sniedzēji, lai atvieglotu elektroniski reģistrētu datu nosūtīšanu starp diviem vai vairākiem kvalificētiem uzticamības pakalpojumu sniedzējiem un veicinātu godprātīgu praksi iekšējā tirgū.

(53) Vairumā gadījumu Savienības pilsoņi un Savienības pastāvīgie iedzīvotāji nevar pāri robežām, droši un ar augstu datu aizsardzības līmeni apmainīties ar digitālu informāciju, kas saistīta ar viņu identitāti, piemēram, adresi, vecumu, profesionālo kvalifikāciju, transportlīdzekļa vadītāja apliecību un citām atļaujām un maksājumu datiem.

(54) Vajadzētu būt iespējai izdot un apstrādāt uzticamus elektroniskus atribūtus un palīdzēt samazināt administratīvo slogu, dodot Savienības pilsoņiem un pastāvīgajiem iedzīvotājiem Savienībā iespēju tos izmantot savos privātajos un publiskajos darījumos. Savienības pilsoņiem un Savienības pastāvīgajiem iedzīvotājiem, piemēram, vajadzētu būt iespējai pierādīt, ka viņiem ir derīga kādas dalībvalsts iestādes izsniegta transportlīdzekļa vadītāja apliecība, ko var verificēt un uz ko var paļauties attiecīgās iestādes citās dalībvalstīs, iespējai paļauties uz sava sociālā nodrošinājuma akreditācijas datiem vai uz turpmākiem digitālajiem ceļošanas dokumentiem pārrobežu kontekstā.

(55) Visi pakalpojumu sniedzēji, kas izdod apliecinātus atribūtus elektroniskā formā, piemēram, diplomus, apliecības, dzimšanas apliecības vai pilnvaras un pilnvarojumus pārstāvēt fiziskas vai juridiskas personas vai rīkoties to vārdā, būtu uzskatāmi par elektroniskā atribūtu apliecinājuma uzticamības pakalpojumu sniedzējiem. Atribūtu elektroniskam apliecinājumam nevajadzētu liegt juridisko spēku tādēļ, ka tas ir elektroniskā formātā vai neatbilst kvalificēta elektroniska atribūtu apliecinājuma prasībām. Būtu jānosaka vispārīgas prasības, lai nodrošinātu, ka kvalificētam atribūtu elektroniskajam apliecinājumam ir līdzvērtīgs juridisks spēks kā likumīgi izdotiem papīra formāta apliecinājumiem. Tomēr šīs prasības būtu jāpiemēro, neskarot Savienības vai valstu tiesību aktus, kuros ir noteiktas papildu, nozarei specifiskas prasības attiecībā uz formātu ar tam pamatā esošu juridisku spēku, un jo īpaši attiecīgā gadījumā attiecībā uz kvalificēta atribūtu elektroniskā apliecinājuma atzīšanu pāri robežām.

(56) Plašai Eiropas digitālās identitātes maku pieejamībai un lietojamībai būtu jāstiprina to pieņemšana un uzticēšanās tiem no privātu indivīdu un privātu pakalpojumu sniedzēju puses. Tādēļ privātām atkarīgajām personām, kuras sniedz pakalpojumus, piemēram, transporta, enerģētikas, banku un finanšu pakalpojumu, sociālā nodrošinājuma, veselības, dzeramā ūdens, pasta pakalpojumu, digitālās infrastruktūras, telesakaru vai izglītības jomā, būtu jāpieņem Eiropas digitālās identitātes maku lietošana pakalpojumu sniegšanas vajadzībām, ja Savienības vai valsts tiesību aktos vai līgumsaistībās tiek prasīta droša lietotāja autentifikācija identifikācijai tiešsaistē. Visiem Eiropas digitālās identitātes maka lietotājam adresētiem atkarīgās puses informācijas pieprasījumiem vajadzētu būt nepieciešamiem un samērīgiem ar paredzēto lietojumu konkrētā gadījumā, tiem vajadzētu atbilst datu minimizēšanas principam un būtu jānodrošina pārredzamība attiecībā uz to, kuri dati tiek kopīgoti un kādos nolūkos. Lai sekmētu Eiropas digitālās identitātes maku lietošanu un pieņemšanu, to ieviešanā būtu jāņem vērā plaši pieņemti nozares standarti un specifikācijas.

(57) Ja ļoti lielas tiešsaistes platformas Eiropas Parlamenta un Padomes Regulas (ES) 2022/2065 ([15]) 33. panta 1. punkta nozīmē prasa lietotājiem pašiem autentificēties, lai tie varētu piekļūt tiešsaistes pakalpojumiem, būtu jāprasa minētajām platformām pieņemt Eiropas digitālās identitātes maku lietošanu pēc lietotāja brīvprātīgi izteikta lūguma. Lietotājiem nevajadzētu būt pienākumam lietot Eiropas digitālās identitātes maku, lai piekļūtu privātiem pakalpojumiem, un nebūtu jāierobežo vai jākavē viņu piekļuve pakalpojumiem tāpēc, ka viņi nelieto Eiropas digitālās identitātes maku. Tomēr, ja lietotāji vēlas to darīt, ļoti lielām platformām būtu tie jāpieņem minētajā nolūkā, vienlaikus ievērojot datu minimizēšanas principu un lietotāju tiesības izmantot brīvi izvēlētus pseidonīmus. Tā kā lielas tiešsaistes platformas to pieejamības dēļ ir ļoti nozīmīgas, jo īpaši pakalpojuma saņēmēju un ekonomisko darījumu skaita izteiksmē, pienākums pieņemt Eiropas digitālās identitātes makus ir nepieciešams, lai pastiprinātu lietotāju aizsardzību pret krāpšanu un nodrošinātu augstu datu aizsardzības līmeni.

(58) Savienības līmenī būtu jāizstrādā rīcības kodeksi, lai palīdzētu darīt plaši pieejamus un izmantot elektroniskās identifikācijas līdzekļus, tostarp Eiropas digitālās identitātes makus, kas ir šīs regulas darbības jomā. Rīcības kodeksiem būtu jāveicina tas, ka elektroniskos identifikācijas līdzekļus, tostarp Eiropas digitālās identitātes makus, plaši pieņem tie pakalpojumu sniedzēji, kuri nav kvalificējami kā ļoti lielas platformas un kuri lietotāju autentifikācijā paļaujas uz trešo personu elektroniskās identifikācijas pakalpojumiem.

(59) Selektīva izpaušana ir jēdziens, kas datu īpašniekam dod iespēju izpaust tikai dažas daļas no plašākas datu kopas, lai saņēmējs subjekts saņemtu vienīgi tādu informāciju, kāda nepieciešama lietotāja pieprasītā pakalpojuma sniegšanai. Eiropas digitālās identitātes makam tehniski būtu jādod iespēja selektīvi izpaust atribūtus atkarīgām personām. Vajadzētu būt tehniski iespējamam, ka lietotājs var selektīvi izpaust atribūtus, tostarp no vairākiem atšķirīgiem elektroniskajiem apliecinājumiem, un tos apvienot un netraucēti uzrādīt atkarīgajām personām. Šai funkcijai būtu jākļūst par Eiropas digitālās identitātes maku struktūras pamatelementu, tādējādi uzlabojot ērtības un personas datu aizsardzību, tostarp datu minimizēšanu.

(60) Ja vien konkrēti Savienības vai valstu tiesību aktu noteikumi neprasa lietotājiem identificēties, nebūtu jāaizliedz piekļūt pakalpojumiem, izmantojot pseidonīmu.

(61) Atribūti, ko kvalificēti uzticamības pakalpojumu sniedzēji nodrošina kā kvalificētas atribūtu apliecināšanas daļu, būtu jāverificē, salīdzinot ar autentiskiem avotiem, vai nu tieši kvalificētam uzticamības pakalpojumu sniedzējam, vai izmantojot izraudzītus starpniekus, kas atzīti valsts līmenī saskaņā ar Savienības vai valsts tiesību aktiem, nolūkā veikt drošu apliecinātu atribūtu apmaiņu starp identitātes vai atribūtu apliecināšanas pakalpojumu sniedzējiem un atkarīgajām personām. Dalībvalstīm valstu līmenī būtu jāizveido pienācīgi mehānismi, lai nodrošinātu, ka kvalificēti uzticamības pakalpojumu sniedzēji, kuri izdod kvalificētus atribūtu elektroniskos apliecinājumus, var uz tās personas piekrišanas pamata, kurai apliecinājums izdots, verificēt atribūtu autentiskumu, izmantojot autentiskus avotus. Vajadzētu būt iespējamam pienācīgos mehānismos iekļaut konkrētu starpnieku vai tehnisku risinājumu izmantošanu saskaņā ar valsts tiesību aktiem, kas ļauj piekļūt autentiskiem avotiem. Mehānisma pieejamības nodrošināšanai, kas dod iespēju verificēt atribūtus, salīdzinot tos ar autentiskiem avotiem, vajadzētu sekmēt to, ka kvalificēti uzticamības pakalpojumu sniedzēji, kuri izsniedz kvalificētu elektronisko atribūtu apliecinājumu, ievēro savus pienākumus atbilstoši Regulai (ES) Nr. 910/2014. Minētās regulas jaunā pielikumā būtu jāiekļauj saraksts ar atribūtu kategorijām, attiecībā uz kurām dalībvalstīm būtu jānodrošina, ka tiek veikti pasākumi, kas ļauj kvalificētiem atribūtu elektronisko apliecinājumu sniedzējiem pēc lietotāja pieprasījuma ar elektroniskiem līdzekļiem verificēt to autentiskumu salīdzinājumā ar attiecīgo autentisko avotu.

(62) Drošai elektroniskai identifikācijai un atribūtu apliecinājuma nodrošināšanai būtu jāsniedz papildu elastība un risinājumi finanšu pakalpojumu nozarē, lai varētu identificēt klientus un apmainīties ar konkrētiem atribūtiem, kas vajadzīgi, lai izpildītu, piemēram, klientu uzticamības pārbaudes prasības saskaņā ar Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas regulu [atsauce jāpievieno pēc priekšlikuma pieņemšanas], piemērotības prasības, kas izriet no ieguldītāju aizsardzības tiesību aktiem, vai lai atbalstītu drošu klientu autentifikācijas prasību izpildi attiecībā uz tiešsaistes identifikāciju, ko veic, lai pieteiktos kontā un lai uzsāktu darījumu maksājumu pakalpojumu jomā.

(63) Elektroniskā paraksta juridisko spēku nevar apstrīdēt, pamatojoties uz to, ka tas ir elektroniskā formātā vai ka tas neatbilst kvalificētā elektroniskā paraksta prasībām. Tomēr elektronisko parakstu juridiskais spēks ir jānosaka valstu tiesību aktos, izņemot šajā regulā paredzētās prasības, saskaņā ar kurām kvalificēta elektroniskā paraksta juridiskās

([15]) Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (OV L 277, 27.10.2022., 1. lpp.).

sekas ir uzskatāmas par līdzvērtīgām ar roku rakstītam parakstam. Nosakot elektronisko parakstu juridisko spēku, dalībvalstīm būtu jāņem vērā samērīguma princips starp parakstāmā dokumenta juridisko vērtību un drošības līmeni un izmaksām, ko prasa elektroniskais paraksts. Lai palielinātu elektronisko parakstu pieejamību un izmantošanu, dalībvalstis tiek mudinātas apsvērt uzlabotu elektronisko parakstu izmantošanu ikdienas darījumos, attiecībā uz kuriem tie nodrošina pietiekamu drošības un ticamības līmeni.

(64) Lai nodrošinātu konsekventu sertifikācijas praksi visā Savienībā, Komisijai vajadzētu izdot pamatnostādnes par kvalificēta elektroniskā paraksta radīšanas ierīču un kvalificēta elektroniskā zīmoga radīšanas ierīču sertifikāciju un resertifikāciju, tostarp par to derīgumu un termiņiem. Šī regula neliedz publiskām vai privātām struktūrām, kurām ir sertificētas kvalificēta elektroniskā paraksta radīšanas ierīces, uz laiku atkārtoti sertificēt šādas ierīces uz īstermiņa sertifikācijas periodu, pamatojoties uz iepriekšējā sertifikācijas procesa rezultātiem, ja šādu atkārtotu sertifikāciju nevar veikt juridiski noteiktā termiņā cita iemesla dēļ, kas nav pārkāpums vai drošības incidents, un neskarot pienākumu veikt neaizsargātības novērtējumu un neskarot piemērojamo sertifikācijas praksi.

(65) Tīmekļa vietņu autentifikācijas sertifikātu izdošanas mērķis ir sniegt lietotājiem augsta līmeņa ticamību attiecībā uz tā subjekta identitāti, kas atbild par tīmekļa vietni, neatkarīgi no platformas, kas tiek izmantota minētās identitātes attēlošanai. Minētajiem pakalpojumiem būtu jāpalīdz veidot uzticēšanos darījumu kārtošanai tiešsaistē, jo lietotāji uzticētos autentificētai tīmekļa vietnei. Šādu tīmekļa vietņu sertifikātu lietošanai tīmekļa vietnēs vajadzētu būt brīvprātīgai. Lai tīmekļa vietņu autentifikācija kļūtu par veidu, kā palielināt uzticēšanos, sniegt labāku pieredzi lietotājam un veicināt izaugsmi iekšējā tirgū, šī regula nosaka uzticamības satvaru, tostarp minimālos drošības un atbildības pienākumus kvalificētu tīmekļa vietņu autentifikācijas sertifikātu sniedzējiem un prasības minēto sertifikātu izsniegšanai. Valstu uzticamības sarakstiem būtu jāapstiprina tīmekļa vietņu autentifikācijas pakalpojumu un to uzticamības pakalpojumu sniedzēju kvalificētais statuss, tostarp to pilnīga atbilstība šīs regulas prasībām attiecībā uz kvalificētu tīmekļa vietņu autentifikācijas sertifikātu izdošanu. Kvalificētu tīmekļa vietņu autentifikācijas sertifikātu atzīšana nozīmē, ka tīmekļa pārlūkprogrammu nodrošinātājiem nebūtu jānoliedz kvalificētu sertifikātu autentiskums tīmekļa vietnes autentifikācijai vienīgi nolūkā apliecināt saikni starp tīmekļa vietnes domēna nosaukumu un fizisko vai juridisko personu, kurai sertifikāts ir izdots, vai apstiprināt minētās personas identitāti. Tīmekļa pārlūkprogrammu nodrošinātājiem būtu pārlūkprogrammas vidē lietotājdraudzīgā veidā jāparāda tiešajam lietotājam sertificētie identitātes dati un citi apliecinātie atribūti, izmantojot pašu izvēlētu tehnisko īstenošanu. Minētajā nolūkā tīmekļa pārlūkprogrammu nodrošinātājiem būtu jānodrošina atbalsts un sadarbspēja ar kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem, kuri izdoti pilnīgi saskaņā ar šo regulu. Kvalificētu tīmekļa vietņu autentifikācijas sertifikātu atzīšanas, sadarbspējas un atbalsta pienākums neietekmē tīmekļa pārlūkprogrammu nodrošinātāju brīvību nodrošināt tīmekļa drošību, domēna autentifikāciju un tīmekļa datplūsmas šifrēšanu tādā veidā un ar tādām tehnoloģijām, kādas tie uzskata par vispiemērotākajām. Lai sekmētu tiešo lietotāju drošību tiešsaistē, tīmekļa pārlūkprogrammu nodrošinātājiem būtu izņēmuma apstākļos jāspēj veikt piesardzības pasākumus, kas ir gan nepieciešami, gan samērīgi reakcijā uz pamatotām bažām par drošības pārkāpumiem vai identificēta sertifikāta vai sertifikātu kopuma integritātes zudumu. Tīmekļa pārlūkprogrammu nodrošinātājiem, ja tie veic šādus piesardzības pasākumus, būtu bez liekas kavēšanās jāpaziņo Komisijai, valsts uzraudzības struktūrai un subjektam, kuram sertifikāts tika izdots, un kvalificētajam uzticamības pakalpojuma sniedzējam, kas izsniedza minēto sertifikātu vai sertifikātu kopumu, par visām bažām attiecībā uz šādu drošības pārkāpumu vai integritātes zudumu, kā arī par pasākumiem, kas veikti saistībā ar atsevišķu sertifikātu vai sertifikātu kopumu. Minētajiem pasākumiem nebūtu jāskar tīmekļa pārlūkprogrammu nodrošinātāju pienākums atzīt kvalificētus tīmekļa vietņu autentifikācijas sertifikātus saskaņā ar valstu uzticamības sarakstiem. Lai vēl vairāk aizsargātu Savienības pilsoņus un Savienības pastāvīgos iedzīvotājus un lai veicinātu kvalificētu tīmekļa vietņu autentifikācijas sertifikātu lietošanu, dalībvalstu publiskajām iestādēm būtu jāapsver kvalificētu tīmekļa vietņu autentifikācijas sertifikātu iekļaušana savās tīmekļa vietnēs. Šajā regulā paredzētie pasākumi, kuru mērķis ir panākt lielāku saskaņotību starp dalībvalstu atšķirīgajām pieejām un praksi attiecībā uz uzraudzības procedūrām, ir iecerēti, lai sekmētu lielāku uzticēšanos un paļāvību uz kvalificētu tīmekļa vietņu autentifikācijas sertifikātu drošību, kvalitāti un pieejamību.

(66) Daudzas dalībvalstis ir ieviesušas valsts prasības drošas un uzticamas elektroniskās arhivēšanas pakalpojumiem, lai ilgtermiņā saglabātu elektroniskos datus un elektroniskos dokumentus, un ar tiem saistītiem uzticamības pakalpojumiem. Lai nodrošinātu juridisko noteiktību, uzticēšanos un saskaņošanu visās dalībvalstīs, būtu jāizveido tiesisks satvars kvalificētiem elektroniskās arhivēšanas pakalpojumiem, iedvesmojoties no citu šajā regulā paredzēto uzticamības pakalpojumu satvara. Kvalificētu elektroniskās arhivēšanas pakalpojumu satvaram būtu jāpiedāvā uzticamības pakalpojumu sniedzējiem un lietotājiem efektīvs instrumentu kopums, kurā ir iekļautas funkcionālas prasības elektroniskās arhivēšanas pakalpojumam, kā arī skaidras tiesiskās sekas, ja tiek izmantots kvalificēts elektroniskās arhivēšanas pakalpojums. Minētie noteikumi būtu jāpiemēro elektroniskiem datiem un elektroniskiem dokumentiem, kuri radīti elektroniskā formā, kā arī papīra dokumentiem, kas ir ieskenēti un digitalizēti. Vajadzības

gadījumā minētajiem noteikumiem būtu jāatļauj saglabātos elektroniskos datus un elektroniskos dokumentus pārnest uz citādiem nesējiem vai formātiem, lai pagarinātu to ilglaicīgumu un lasāmību pēc tehniskā derīguma termiņa beigām, vienlaikus pēc iespējas novēršot zudumus un izmaiņas. Ja elektroniskie dati un elektroniskie dokumenti, kas iesniegti elektroniskās arhivēšanas pakalpojumam, satur vienu vai vairākus kvalificētus elektroniskos parakstus vai kvalificētus elektroniskos zīmogus, pakalpojumam būtu jāizmanto procedūras un tehnoloģijas, kas spēj pagarināt to uzticamību šādu datu saglabāšanas periodā, iespējams, paļaujoties uz citu kvalificētu elektronisko uzticamības pakalpojumu izmantošanu, kuri izveidoti ar šo regulu. Lai izveidotu saglabāšanas pierādījumus, kuros izmanto elektroniskos parakstus, elektroniskos zīmogus vai elektroniskos laika zīmogus, būtu jāizmanto kvalificēti uzticamības pakalpojumi. Tiktāl, ciktāl šī regula nesaskaņo elektroniskās arhivēšanas pakalpojumus, dalībvalstīm vajadzētu būt iespējai saglabāt vai ieviest valsts noteikumus, saskaņā ar Savienības tiesību aktiem, attiecībā uz minētajiem pakalpojumiem, piemēram, konkrētus noteikumus attiecībā uz pakalpojumiem, kuri ir integrēti organizācijā un kurus izmanto vienīgi minētās organizācijas iekšējiem arhīviem. Šai regulai nevajadzētu nošķirt elektroniskus datus un elektroniskus dokumentus, kas radīti elektroniskā formā, no fiziskiem dokumentiem, kas ir digitalizēti.

(67) Pasākumus, ko veic valstu arhīvi un atmiņas institūcijas kā organizācijas, kas nodarbojas ar dokumentārā mantojuma saglabāšanu sabiedrības interesēs, parasti reglamentē valsts tiesību akti, un tās ne vienmēr sniedz uzticamības pakalpojumus šīs regulas izpratnē. Ciktāl šādas iestādes nesniedz šādus uzticamības pakalpojumus, šī regula neskar to darbību.

(68) Elektroniskas virsgrāmatas ir elektronisko datu ierakstu sekvence, kam būtu jānodrošina to integritāte un to hronoloģiskās secības precizitāte. Elektroniskajām virsgrāmatām būtu jāizveido datu ierakstu hronoloģiskā secība. Kopā ar citām tehnoloģijām tām būtu jāpalīdz rast risinājumus efektīvākiem un transformatīviem publiskajiem pakalpojumiem, tādiem kā e-balsošana, pārrobežu sadarbība starp muitas iestādēm, pārrobežu sadarbība starp akadēmiskajām iestādēm un nekustamā īpašuma īpašumtiesību reģistrēšana decentralizētos zemes reģistros. Kvalificētām elektroniskajām virsgrāmatām būtu jārada juridiska prezumpcija attiecībā uz unikālu un precīzu virsgrāmatā iekļauto datu ierakstu hronoloģisko secību un integritāti. Elektroniskās virsgrāmatas to specifisko iezīmju dēļ, piemēram, ierakstu hronoloģiskās secības dēļ, būtu jānošķir no citiem uzticamības pakalpojumiem, piemēram, elektroniskiem laika zīmogiem un elektroniski reģistrētiem piegādes pakalpojumiem. Lai nodrošinātu juridisko noteiktību un veicinātu inovāciju, būtu jāizveido Savienības mēroga tiesiskais satvars, kas paredz pāri robežām atzīt uzticamības pakalpojumus attiecībā uz datu reģistrēšanu elektroniskajās virsgrāmatās. Tam būtu pietiekami jānovērš tas, ka viens un tas pats digitālais aktīvs tiek kopēts un pārdots vairāk nekā vienu reizi dažādām pusēm. Elektroniskās virsgrāmatas izveides un atjaunināšanas process ir atkarīgs no izmantotās virsgrāmatas veida, proti, vai tā ir centralizēta vai izkliedēta. Šai regulai būtu jānodrošina tehnoloģiskā neitralitāte, proti, ka nevienai tehnoloģijai, ko izmanto, lai īstenotu jauno elektronisko virsgrāmatu uzticamības pakalpojumu, netiek dota nedz priekšroka, nedz arī tā tiek diskriminēta. Turklāt, sagatavojot īstenošanas aktus, kuros konkrēti nosaka prasības attiecībā uz kvalificētām elektroniskajām virsgrāmatām, Komisijai, izmantojot atbilstīgas metodikas, būtu jāņem vērā ilgtspējas rādītāji attiecībā uz jebkādu nelabvēlīgu ietekmi uz klimatu vai citu ar vidi saistītu nelabvēlīgu ietekmi.

(69) Elektronisko virsgrāmatu uzticamības pakalpojumu sniedzēju lomai vajadzētu būt pārliecināties par secīgu datu reģistrēšanu virsgrāmatā. Šī regula neskar elektronisko virsgrāmatu lietotāju juridiskos pienākumus saskaņā ar Savienības vai valstu tiesībām. Piemēram, lietošanas gadījumiem, kuros iesaistīta personas datu apstrāde, būtu jāatbilst Regulai (ES) 2016/679, un lietošanas gadījumiem, kas saistīti ar finanšu pakalpojumiem, būtu jāatbilst attiecīgajiem Savienības tiesību aktiem finanšu pakalpojumu jomā.

(70) Lai izvairītos no sadrumstalotības un šķēršļiem iekšējā tirgū atšķirīgo standartu un tehnisko ierobežojumu dēļ un lai nodrošinātu koordinētu procesu nolūkā izvairīties no tā, ka tiek ietekmēta Eiropas digitālās identitātes satvara īstenošana, ir vajadzīga cieša un strukturēta Komisijas, dalībvalstu, pilsoniskās sabiedrības, akadēmisko aprindu un privātā sektora sadarbība. Lai sasniegtu minēto mērķi, dalībvalstīm un Komisijai būtu jāsadarbojas atbilstīgi Komisijas Ieteikumā (ES) 2021/946 ([16]) paredzētajam satvaram nolūkā noteikt kopīgu Savienības rīkkopu Eiropas digitālās identitātes satvaram. Minētajā sakarā dalībvalstīm būtu jāvienojas par visaptverošu tehnisko arhitektūru un atsauču satvaru, kopīgu standartu un tehnisko atsauču kopumu, tostarp atzītiem esošiem standartiem, kā arī pamatnostādņu un paraugprakses aprakstu kopumu, kas aptver vismaz visas Eiropas digitālās identitātes maku, tostarp e-parakstus un kvalificēta atribūtu elektroniskas apliecināšanas uzticamības pakalpojuma sniedzēju funkcionalitātes un sadarbspēju, kā noteikts šajā regulā. Minētajā sakarā dalībvalstīm būtu arī jāvienojas par elementiem attiecībā uz Eiropas digitālās identitātes maku uzņēmējdarbības modeļa elementiem un maksājumu

([16]) Komisijas Ieteikums (ES) 2021/946 (2021. gada 3. jūnijs) par kopīgu Savienības rīkkopu koordinētai pieejai Eiropas digitālās identitātes satvaram (OV L 210, 14.6.2021., 51. lpp.)

struktūru, lai pārrobežu kontekstā atvieglotu to ieviešanu, jo īpaši to, kuru veic MVU. Rīkkopas saturam būtu jāattīstās vienlaikus ar Eiropas digitālās identitātes satvara apspriešanas un pieņemšanas procesa rezultātu un tas jāatspoguļo.

(71) Šī regula paredz kvalificētu uzticamības pakalpojumu saskaņotu kvalitātes, uzticamības un drošības līmeni neatkarīgi no darbības veikšanas vietas. Tādējādi kvalificētam uzticamības pakalpojumu sniedzējam būtu jāļauj izmantot ārpakalpojumus savām darbībām, kas saistītas ar kvalificēta uzticamības pakalpojuma sniegšanu trešā valstī, ja šī trešā valsts sniedz pienācīgas garantijas, nodrošinot, ka uzraudzības darbības un revīzijas var īstenot tā, it kā tās tiktu veiktas Savienībā. Ja nav iespējams pilnībā nodrošināt atbilstību šai regulai, uzraudzības iestādēm būtu jāspēj pieņemt samērīgus un pamatotus pasākumus, tostarp atsaukt kvalificēto statusu sniegtajam uzticamības pakalpojumam.

(72) Lai nodrošinātu juridisko noteiktību attiecībā uz tādu uzlabotu elektronisko parakstu derīgumu, kuru pamatā ir kvalificēti sertifikāti, ir svarīgi precizēt novērtējumu, ko veic atkarīgā puse, kura veic minētā uz kvalificētiem sertifikātiem balstīta uzlabota elektroniskā paraksta validāciju.

(73) Uzticamības pakalpojumu sniedzējiem būtu jāizmanto kriptogrāfijas metodes, kas atspoguļo pašreizējo paraugpraksi un uzticamu minēto algoritmu īstenošanu savu uzticamības pakalpojumu drošības un uzticamības nodrošināšanai.

(74) Šī regula nosaka kvalificētu uzticamības pakalpojumu sniedzēju pienākumu verificēt tās fiziskās vai juridiskās personas identitāti, kurai ir izdots kvalificētais sertifikāts vai kvalificēts atribūta elektroniskais apliecinājums, pamatojoties uz dažādām saskaņotām metodēm visā Savienībā. Lai nodrošinātu, ka kvalificēti sertifikāti un kvalificēti atribūtu elektroniskie apliecinājumi tiek izdoti personām, kurām tie pieder, un ka tie apliecina pareizu un unikālu datu kopumu, kas atspoguļo minētās personas identitāti, kvalificētajiem uzticamības pakalpojumu sniedzējiem, kuri izdod kvalificētus sertifikātus vai izdod kvalificētus atribūtu elektroniskos apliecinājumus, būtu minēto sertifikātu un apliecinājumu izsniegšanas brīdī ar pilnīgu noteiktību jānodrošina minētās personas identifikācija. Turklāt papildus obligātai personas identitātes verifikācijai, ja tā ir piemērojama kvalificētu sertifikātu izdošanai un kad tiek izdots kvalificēts atribūtu elektroniskais apliecinājums, kvalificētiem uzticamības pakalpojumu sniedzējiem būtu ar pilnīgu noteiktību jānodrošina personas, kurai tiek izdots kvalificētais sertifikāts vai kvalificētais atribūtu elektroniskais apliecinājums, apliecināto atribūtu pareizība un precizitāte. Minētos pienākumus attiecībā uz rezultātu un pilnīgu noteiktību apliecināto datu verifikācijā būtu jāatbalsta ar pienācīgiem līdzekļiem, tostarp, izmantojot vienu konkrētu šajā regulā noteiktu metodi vai, vajadzības gadījumā, to kombināciju. Vajadzētu būt iespējai kombinēt minētās metodes, lai nodrošinātu pienācīgu pamatu tās personas identitātes verifikācijai, kurai izdod kvalificētu sertifikātu vai kvalificētu atribūtu elektronisko apliecinājumu. Šādā kombinācijā vajadzētu varēt ietvert paļaušanos uz elektroniskiem identifikācijas līdzekļiem, kuri atbilst uzticamības līmeņa "būtisks" prasībām, apvienojumā ar citiem identitātes verifikācijas līdzekļiem. Šāda elektroniskā identifikācija nodrošinātu šajā regulā paredzēto saskaņoto prasību izpildi attiecībā uz uzticamības līmeni "augsts", kā daļu no saskaņotām attālinātām procedūrām, kas nodrošina identifikāciju ar augstu ticamības līmeni. Minētajām metodēm vajadzētu ietvert iespēju, ka kvalificētu uzticamības pakalpojumu sniedzējs, kas izsniedz kvalificētu atribūtu elektronisko apliecinājumu, pēc lietotāja pieprasījuma un saskaņā ar Savienības vai valsts tiesību aktiem verificē ar elektroniskiem līdzekļiem apliecināmos atribūtus, tostarp, salīdzinot ar autentiskiem avotiem.

(75) Lai nodrošinātu šīs regulas atbilstību pasaules norisēm un ņemtu vērā paraugpraksi iekšējā tirgū, Komisijas pieņemtie deleģētie un īstenošanas akti būtu regulāri jāpārskata un vajadzības gadījumā jāatjaunina. Minēto atjauninājumu nepieciešamības novērtējumā būtu jāņem vērā jaunās tehnoloģijas, prakse, standarti vai tehniskās specifikācijas.

(76) Ņemot vērā to, ka šīs regulas mērķus, proti, Savienības līmeņa Eiropas digitālās identitātes satvara un uzticamības pakalpojumu satvara izstrādi, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet rīcības mēroga un ietekmes dēļ tos var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minēto mērķu sasniegšanai.

(77) Saskaņā ar Regulas (ES) 2018/1725 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju.

(78) Tāpēc Regula (ES) Nr. 910/2014 būtu attiecīgi jāgroza,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Grozījumi Regulā (ES) Nr. 910/2014

Regulu (ES) Nr. 910/2014 groza šādi:

1) regulas 1. pantu aizstāj ar šādu:

"*1. pants*

Priekšmets

Šīs regulas mērķis ir nodrošināt pienācīgu iekšējā tirgus darbību un pienācīga drošības līmeņa panākšanu elektroniskās identifikācijas līdzekļiem un uzticamības pakalpojumiem, kurus izmanto visā Savienībā, lai fiziskām un juridiskām personām dotu un atvieglotu iespēju izmantot tiesības droši piedalīties digitālā sabiedrībā un piekļūt publiskiem un privātiem tiešsaistes pakalpojumiem visā Savienībā. Minētajā nolūkā šī regula:

a) nosaka nosacījumus, saskaņā ar kuriem dalībvalstis nodrošina un atzīst fizisku un juridisku personu elektroniskās identifikācijas līdzekļus, kuri ietilpst citas dalībvalsts paziņotajā elektroniskās identifikācijas shēmā, un paredz un atzīst Eiropas digitālās identitātes makus;

b) nosaka noteikumus par uzticamības pakalpojumiem, jo īpaši attiecībā uz elektroniskiem darījumiem;

c) izveido tiesisko regulējumu attiecībā uz elektroniskajiem parakstiem, elektroniskajiem zīmogiem, elektroniskajiem laika zīmogiem, elektroniskajiem dokumentiem, elektroniski reģistrētiem piegādes pakalpojumiem, sertifikācijas pakalpojumiem tīmekļa vietņu autentifikācijai, elektronisko arhivēšanu, atribūtu elektronisko apliecinājumu, elektroniskā paraksta radīšanas ierīcēm, elektroniskā zīmoga radīšanas ierīču pārvaldību un elektroniskajām virsgrāmatām.";

2) regulas 2. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Šo regulu piemēro elektroniskās identifikācijas shēmām, par kurām dalībvalsts ir paziņojusi Eiropas digitālās identitātes makiem, kurus nodrošina dalībvalsts, un uzticamības pakalpojumu sniedzējiem, kuri iedibināti Savienībā.";

b) panta 3. punktu aizstāj ar šādu:

"3. Šī regula neskar Savienības vai valstu tiesību aktus, kas saistīti ar līgumu slēgšanu un derīgumu vai citu juridisku vai procesuālu saistību uzņemšanos attiecībā uz formātu vai specifiskām nozares prasībām attiecībā uz formātu.

4. Šī regula neskar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (*).

(*) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).";

3) regulas 3. pantu groza šādi:

a) panta 1.–5. punktu aizstāj ar šādiem:

"1) "elektroniskā identifikācija" ir tādu elektronisku personas identifikācijas datu izmantošanas process, kas unikālā veidā apliecina fiziskās vai juridiskās personas identitāti vai tādas fiziskas personas identitāti, kas pārstāv citu fizisku vai kādu juridisku personu;

2) “elektroniskās identifikācijas līdzekļi” ir materiāls un/vai nemateriāls elements, kas satur personas identifikācijas datus un ko izmanto, lai autentificētos tiešsaistes pakalpojumam vai, attiecīgā gadījumā, bezsaistes pakalpojumam;

3) “personas identifikācijas dati” ir datu kopums, kas izdots saskaņā ar Savienības vai valstu tiesību aktiem un kas ļauj noskaidrot fiziskas vai juridiskas personas identitāti, vai tādas fiziskas personas identitāti, kas pārstāv citu fizisku personu vai juridisku personu;

4) “elektroniskās identifikācijas shēma” ir elektroniskās identifikācijas sistēma, kurā elektroniskās identifikācijas līdzekļus izdod fiziskām vai juridiskām personām vai tādām fiziskām personām, kas pārstāv citas fiziskas personas vai juridiskas personas;

5) “autentifikācija” ir elektronisks process, kas dara iespējamu fiziskas vai juridiskas personas elektroniskās identifikācijas apstiprināšanu vai elektronisko datu izcelsmes un integritātes apstiprināšanu;”;

b) iekļauj šādu punktu:

“5.a) “lietotājs” ir fiziska vai juridiska persona, vai fiziska persona, kas pārstāv citu fizisku vai juridisku personu, kura izmanto uzticamības pakalpojumus vai elektroniskās identifikācijas līdzekļus, kas sniegti saskaņā ar šo regulu;”;

c) panta 6. punktu aizstāj ar šādu:

“6) “atkarīgā puse” ir fiziska vai juridiska persona, kas paļaujas uz elektronisku identifikāciju, Eiropas digitālās identitātes makiem vai elektroniskās identifikācijas līdzekļiem, vai uz uzticamības pakalpojumu;”;

d) panta 16. punktu aizstāj ar šādu:

“16) “uzticamības pakalpojums” ir elektronisks pakalpojums, parasti par atlīdzību, kas ietver jebko no tālāk minētā:

a) elektronisko parakstu sertifikātu, elektronisko zīmogu sertifikātu, tīmekļa vietņu autentifikācijas sertifikātu vai citu uzticamības pakalpojumu sniegšanas sertifikātu izsniegšanu;

b) elektronisko parakstu sertifikātu, elektronisko zīmogu sertifikātu, tīmekļa vietņu autentifikācijas sertifikātu vai citu uzticamības pakalpojumu sniegšanas sertifikātu validāciju;

c) elektronisko parakstu vai elektronisko zīmogu radīšanu;

d) elektronisko parakstu vai elektronisko zīmogu validāciju;

e) elektronisko parakstu, elektronisko zīmogu, elektronisko parakstu sertifikātu vai elektronisko zīmogu sertifikātu saglabāšanu;

f) attālinātas elektroniskā paraksta radīšanas ierīču vai attālinātas elektroniskā zīmoga radīšanas ierīču pārvaldību;

g) atribūtu elektronisko apliecinājumu izsniegšanu;

h) atribūtu elektroniskā apliecinājuma validāciju;

i) elektronisko laika zīmogu izveidi;

j) elektronisko laika zīmogu validāciju;

k) elektroniski reģistrētu piegādes pakalpojumu sniegšanu;

l) to datu validāciju, kas nosūtīti, izmantojot elektroniski reģistrētus piegādes pakalpojumus, un ar tiem saistītus pierādījumus;

m) elektronisko datu un elektronisko dokumentu elektronisko arhivēšanu;

n) elektronisko datu reģistrēšanu elektroniskajā virsgrāmatā;";

e) panta 18. punktu aizstāj ar šādu:

"18) "atbilstības novērtēšanas struktūra" ir atbilstības novērtēšanas struktūra, kā definēts Regulas (EK) Nr. 765/2008 2. panta 13. punktā, kas saskaņā ar minēto regulu ir akreditēta kā kompetenta veikt kvalificēta uzticamības pakalpojumu sniedzēja un tā sniegtu kvalificētu uzticamības pakalpojumu atbilstības novērtēšanu vai veikt Eiropas digitālās identitātes maku vai elektroniskās identifikācijas līdzekļu sertifikāciju;";

f) panta 21. punktu aizstāj ar šādu:

"21) "produkts" ir aparatūra vai programmatūra, vai attiecīgās aparatūras vai programmatūras sastāvdaļas, ko paredzēts izmantot elektroniskās identifikācijas un uzticamības pakalpojumu sniegšanai;";

g) pantam pievieno šādus apakšpunktus:

"23.a) "attālinātas kvalificēta elektroniskā paraksta radīšanas ierīce" ir kvalificēta elektroniskā paraksta radīšanas ierīce, ko parakstītāja vārdā pārvalda kvalificēts uzticamības pakalpojumu sniedzējs saskaņā ar 29.a pantu;

23.b)" attālinātas kvalificēta elektroniskā zīmoga radīšanas ierīce" ir kvalificēta elektroniskā zīmoga radīšanas ierīce, ko zīmoga radītāja vārdā pārvalda kvalificēts uzticamības pakalpojumu sniedzējs saskaņā ar 39.a pantu;";

h) panta 38. punktu aizstāj ar šādu:

"38) "tīmekļa vietņu autentifikācijas sertifikāts" ir elektronisks apliecinājums, kas ļauj autentificēt tīmekļa vietni un saista tīmekļa vietni ar fizisko vai juridisko personu, kurai sertifikāts ir izdots;";

i) panta 41. punktu aizstāj ar šādu:

"41) "validācija" ir process, kurā verificē un apstiprina, ka dati elektroniskā formātā ir derīgi saskaņā ar šo regulu;";

j) pievieno šādus punktus:

"42) "Eiropas digitālās identitātes maks" ir elektroniskās identifikācijas līdzeklis, kas ļauj lietotājam droši glabāt, pārvaldīt un validēt personas identifikācijas datus un atribūtu elektroniskos apliecinājumus, lai sniegtu tos atkarīgajām pusēm un citiem Eiropas digitālās identitātes maku lietotājiem, un parakstītu ar kvalificētu elektronisko parakstu vai apzīmogotu ar kvalificētiem elektroniskiem zīmogiem;

43) "atribūts" ir fiziskas vai juridiskas personas vai priekšmeta īpašība, kvalitāte, tiesības vai atļauja;

44) "atribūtu elektroniskais apliecinājums" ir apliecinājums elektroniskā formātā, kas ļauj atribūtiem tikt autentificētiem;

45) "kvalificēts atribūtu elektroniskais apliecinājums" ir atribūtu elektroniskais apliecinājums, ko izdod kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst V pielikumā noteiktajām prasībām;

46) "atribūtu elektroniskais apliecinājums, ko izdevusi par autentisku avotu atbildīga publiskā sektora struktūra vai kas izdots tās vārdā" ir elektronisks atribūtu apliecinājums, ko izdevusi publiskā sektora struktūra, kura ir atbildīga par autentisku avotu, vai publiskā sektora struktūra, kuru dalībvalsts izraudzījusies, lai izdotu šādus atribūtu apliecinājumus to publiskā sektora struktūru vārdā, kuras ir atbildīgas par autentiskiem avotiem saskaņā ar 45.f pantu un VII pielikumu;

47) "autentisks avots" ir repozitorijs vai sistēma, kas ir publiskas iestādes vai privāta subjekta atbildībā un satur un sniedz atribūtus, kuri attiecas uz fizisku vai juridisku personu vai objektu, un ko uzskata par minētās informācijas primāro avotu vai kas atzīts par autentisku saskaņā ar Savienības vai valstu tiesību aktiem, tostarp administratīvo praksi;

48) “elektroniska arhivēšana” ir pakalpojums, kas nodrošina elektronisku datu un elektronisku dokumentu saņemšanu, glabāšanu, izguvi un dzēšanu, lai garantētu to ilglaicīgumu un lasāmību, kā arī saglabātu to integritāti, konfidencialitāti un izcelsmes apliecinājumu visā saglabāšanas periodā;

49) “kvalificēts elektroniskās arhivēšanas pakalpojums” ir elektroniskās arhivēšanas pakalpojums, ko sniedz kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst 45.j pantā noteiktajām prasībām;

50) “ES digitālās identitātes maka uzticamības marķējums” ir pārbaudāma, vienkārša un atpazīstama norāde, kas darīta zināma skaidrā veidā un kas apliecina, ka Eiropas digitālās identitātes maks ir nodrošināts saskaņā ar šo regulu;

51) “droša lietotāja autentifikācija” ir autentifikācija, kurai ir vismaz divi autentifikācijas faktori no dažādām kategorijām, proti, no zināšanu kategorijas (kaut kas, kas ir tikai lietotājam zināms), valdījuma kategorijas (kaut kas, kas ir tikai lietotāja valdījumā) vai neatņemamas īpašības kategorijas (lietotājam raksturīgas īpašības), un šie faktori ir savstarpēji neatkarīgi, proti, neatbilstība vienam kritērijam neapdraud pārējo elementu uzticamību, un ir izstrādāti tā, lai nodrošinātu autentificēšanas datu konfidencialitātes aizsardzību;

52) “elektroniskā virsgrāmata” ir elektronisko datu ierakstu sekvence, kas nodrošina minēto ierakstu integritāti un minēto ierakstu hronoloģiskās secības precizitāti;

53) “kvalificēta elektroniskā virsgrāmata” ir elektroniskā virsgrāmata, ko sniedz kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst 45.l pantā noteiktajām prasībām;

54) “personas dati” ir jebkura informācija, kā definēts Regulas (ES) 2016/679 4. panta 1. punktā;

55) “identitātes saskaņošana” ir process, kurā personas identifikācijas dati vai elektroniskās identifikācijas līdzekļi tiek saskaņoti vai sasaistīti ar esošu kontu, kas pieder tai pašai personai;

56) “datu ieraksts” ir elektroniski dati, kas reģistrēti ar saistītiem metadatiem, kuri atbalsta datu apstrādi;

57) “bezsaistes režīms” attiecībā uz Eiropas digitālās identitātes maku izmantošanu ir mijiedarbība starp lietotāju un trešo personu fiziskā atrašanās vietā, izmantojot tuva attāluma tehnoloģijas, kad Eiropas digitālās identitātes makam mijiedarbības nolūkā nav jāpiekļūst attālinātām sistēmām, izmantojot elektronisko sakaru tīklus.”;

4) regulas 5. pantu aizstāj ar šādu:

“*5. pants*

Pseidonīmi elektroniskā darījumā

Neskarot konkrētus Savienības vai valsts tiesību aktus, kas pieprasa lietotājiem identificēties, vai juridiskās sekas, kādas pseidonīmiem ir saskaņā ar valsts tiesību aktiem, lietotāja izvēlētu pseidonīmu izmantošana elektroniskos darījumos nav aizliegta.”;

5) regulas II nodaļā iekļauj šādu iedaļu:

“1. IEDAĻA

EIROPAS DIGITĀLĀS IDENTITĀTES MAKS

5.a pants

Eiropas digitālās identitātes maki

1. Lai nodrošinātu, ka visām fiziskām un juridiskām personām Savienībā ir droša, uzticama un netraucēta pārrobežu piekļuve publiskiem un privātiem pakalpojumiem, vienlaikus saglabājot pilnīgu kontroli pār saviem datiem, katra dalībvalsts 24 mēnešu laikā pēc šā panta 23. punktā un 5.c panta 6. punktā minēto īstenošanas aktu stāšanās spēkā dienas nodrošina vismaz vienu Eiropas digitālās identitātes maku.

2. Eiropas digitālās identitātes makus nodrošina vienā vai vairākos no šādiem veidiem:

a) tiešā veidā dalībvalsts;

b) atbilstīgi dalībvalsts pilnvarojumam;

c) neatkarīgi no dalībvalsts, bet minētā dalībvalsts tos atzīst.

3. Eiropas digitālās identitātes maku lietojumprogrammatūras sastāvdaļu pirmkods ir licencēts kā atvērtais pirmkods. Dalībvalstis var paredzēt, ka pienācīgi pamatotu iemeslu dēļ netiek izpausts tādu konkrētu sastāvdaļu pirmkods, kas nav instalētas lietotāja ierīcēs.

4. Eiropas digitālās identitātes maks lietotājam ļauj lietotājdraudzīgā, pārredzamā un izsekojamā veidā:

a) tikai lietotāja kontrolē droši pieprasīt, iegūt, atlasīt, apvienot, glabāt, dzēst, kopīgot un uzrādīt personas identifikācijas datus un attiecīgā gadījumā apvienojumā ar atribūtu elektroniskajiem apliecinājumiem, lai autentificētos atkarīgajām pusēm tiešsaistē un attiecīgā gadījumā bezsaistes režīmā nolūkā piekļūt publiskiem un privātiem pakalpojumiem, vienlaikus nodrošinot, ka ir iespējama selektīva datu izpaušana;

b) ģenerēt pseidonīmus un tos šifrētā veidā un lokāli glabāt Eiropas digitālās identitātes makā;

c) droši autentificēt citas personas Eiropas digitālās identitātes maku un drošā veidā saņemt un kopīgot personas identifikācijas datus un atribūtu elektroniskos apliecinājumus starp diviem Eiropas digitālās identitātes makiem;

d) piekļūt reģistram par visiem darījumiem, kas veikti ar Eiropas digitālās identitātes maka starpniecību, izmantojot kopīgu infopaneli, kas ļauj lietotājam:

   i) skatīt aktualizētu sarakstu, kurā norādītas atkarīgās personas, ar kurām lietotājs ir izveidojis savienojumu, un attiecīgā gadījumā visus datus, ar ko notikusi apmaiņa;

   ii) vienkāršā veidā pieprasīt atkarīgajai pusei dzēst personas datus, ievērojot Regulas (ES) 2016/679 17. pantu;

   iii) vienkāršā veidā ziņot valsts datu aizsardzības iestādei par atkarīgo pusi ja saņemts iespējami nelikumīgs vai aizdomīgs datu pieprasījums;

e) parakstīt ar kvalificētu elektronisko parakstu vai apzīmogot ar kvalificētu elektronisko zīmogu;

f) ciktāl tas tehniski iespējams, lejupielādēt lietotāja datus, atribūtu elektronisko apliecinājumu un konfigurācijas;

g) izmantot lietotāja tiesības uz datu pārnesamību.

5. Eiropas digitālās identitātes maki jo īpaši:

a) atbalsta kopīgus protokolus un saskarnes:

   i) lai izsniegtu personas identifikācijas datus, kvalificētus un nekvalificētus atribūtu elektroniskos apliecinājumus vai kvalificētus un nekvalificētus sertifikātus Eiropas digitālās identitātes makam;

   ii) lai atkarīgās puses varētu pieprasīt un validēt personas identifikācijas datus un atribūtu elektronisko apliecinājumu;

   iii) lai ar atkarīgajām pusēm kopīgotu un tām uzrādītu personas identifikācijas datus, atribūtu elektronisko apliecinājumu vai selektīvi izpaustus ar tiem saistītus datus tiešsaistē un attiecīgā gadījumā bezsaistes režīmā;

iv) lai lietotāji varētu mijiedarboties ar Eiropas digitālās identitātes maku un lai attēlotu ES digitālās identitātes maka uzticamības marķējumu;

v) lai nodrošinātu, ka lietotājs var droši pievienoties, izmantojot elektroniskās identifikācijas līdzekļus saskaņā ar 5.a panta 24. punktu;

vi) lai mijiedarbotos starp divu personu Eiropas digitālās identitātes makiem nolūkā drošā veidā saņemt, validēt un kopīgot personas identifikācijas datus un atribūtu elektroniskos apliecinājumus;

vii) lai autentificētu un identificētu atkarīgās puses, īstenojot autentifikācijas mehānismus saskaņā ar 5.b pantu;

viii) lai atkarīgās puses verificētu Eiropas digitālās identitātes maku autentiskumu un derīgumu;

ix) lai pieprasītu atkarīgajai pusei dzēst personas datus saskaņā ar Regulas (ES) 2016/679 17. pantu;

x) lai ziņotu par atkarīgo pusi kompetentajai valsts datu aizsardzības iestādei, ja ir saņemts iespējami nelikumīgs vai aizdomīgs datu pieprasījums;

xi) lai izveidotu kvalificētus elektroniskos parakstus vai elektroniskos zīmogus, izmantojot kvalificētu elektronisko parakstu vai elektronisko zīmogu radīšanas ierīces;

b) atribūtu elektronisko apliecinājumu uzticamības pakalpojumu sniedzējiem nesniedz nekādu informāciju par minēto elektronisko apliecinājumu izmantošanu;

c) nodrošina, ka atkarīgās puses var autentificēt un identificēt, īstenojot autentifikācijas mehānismus saskaņā ar 5. b pantu;

d) atbilst prasībām, kas 8. pantā noteiktas uzticamības līmenim "augsts", jo īpaši prasībām par identitātes pierādīšanu un verifikāciju, un elektroniskās identifikācijas līdzekļu pārvaldību un autentifikāciju;

e) tāda atribūtu elektroniskā apliecinājuma gadījumā, kurā integrētas informācijas izpaušanas procedūras, – īsteno piemēroto mehānismu, lai informētu lietotāju, ka atkarīgajai pusei vai Eiropas digitālās identitātes maka lietotajam, kas pieprasa atribūtu elektronisko apliecinājumu, ir atļauja piekļūt šādam apliecinājumam;

f) nodrošina, ka personas identifikācijas dati, kas pieejami no elektroniskās identifikācijas shēmas, atbilstoši kurai tiek nodrošināts Eiropas digitālās identitātes maks, unikāli pārstāv fizisko personu, juridisko personu vai fizisko personu, kas pārstāv fizisko vai juridisko personu, un ir saistīta ar minēto Eiropas digitālās identitātes maku;

g) visām fiziskajām personām piedāvā iespēju parakstīties, izmantojot kvalificētus elektroniskos parakstus pēc noklusējuma un bez maksas.

Neatkarīgi no pirmās daļas g) apakšpunkta dalībvalstis var paredzēt samērīgus pasākumus, lai nodrošinātu, ka fiziskas personas izmanto kvalificētus elektroniskos parakstus bez maksas tikai neprofesionālos nolūkos.

6. Dalībvalsts bez kavēšanās informē lietotājus par visiem drošības pārkāpumiem, kas varētu būt pilnībā vai daļēji kompromitējuši viņu Eiropas digitālās identitātes maku vai tā saturu, jo īpaši tad, ja viņu Eiropas digitālās identitātes maka darbība ir apturēta vai tas ir atsaukts, ievērojot 5.e pantu.

7. Neskarot 5.f pantu, dalībvalstis saskaņā ar valsts tiesību aktiem Eiropas digitālās identitātes makiem var paredzēt papildu funkcionalitātes, tostarp sadarbspēju ar esošajiem valsts elektroniskās identifikācijas līdzekļiem. Minētās papildu funkcionalitātes atbilst šim pantam.

8. Dalībvalstis nodrošina bezmaksas validācijas mehānismus nolūkā:

a) nodrošināt, ka var verificēt Eiropas digitālās identitātes maku autentiskumu un derīgumu;

b) ļaut Eiropas digitālās identitātes maku lietotājiem verificēt saskaņā ar 5.b pantu reģistrēto atkarīgo pušu identitātes autentiskumu un derīgumu.

9. Dalībvalstis nodrošina, ka Eiropas digitālās identitātes maka derīgumu var atsaukt šādos apstākļos:

a) pēc lietotāja nepārprotami izteikta pieprasījuma;

b) ja ir apdraudēta Eiropas digitālās identitātes maka drošība;

c) lietotāja nāves gadījumā vai juridiskās personas darbības izbeigšanas gadījumā.

10. Eiropas digitālās identitātes maku nodrošinātāji nodrošina, ka lietotāji var vienkāršā veidā lūgt tehnisko atbalstu un ziņot par tehniskām problēmām vai jebkuriem citiem incidentiem, kas negatīvi ietekmē Eiropas digitālās identitātes maka izmantošanu.

11. Eiropas digitālās identitātes makus nodrošina atbilstoši elektroniskās identifikācijas shēmai, kurai ir uzticamības līmenis "augsts".

12. Eiropas digitālās identitātes maki nodrošina integrētu drošību.

13. Eiropas digitālās identitātes makus visām fiziskām personām izdod, izmanto un atsauc bez maksas.

14. Lietotāji pilnībā kontrolē sava Eiropas digitālās identitātes maka izmantošanu un tajā ietvertos datus. Eiropas digitālās identitātes maka nodrošinātājs nevāc tādu informāciju par Eiropas digitālās identitātes maka izmantošanu, kas nav nepieciešama Eiropas digitālās identitātes maka pakalpojumu sniegšanai, un neapvieno personas identifikācijas datus vai citus personas datus, kas tiek glabāti vai attiecas uz Eiropas digitālās identitātes maka izmantošanu, ar personas datiem no citiem pakalpojumiem, kurus piedāvā minētais nodrošinātājs, vai no trešo personu pakalpojumiem, kas nav nepieciešami Eiropas digitālās identitātes maka pakalpojumu sniegšanai, ja vien lietotājs nav skaidri pieprasījis rīkoties citādi. Personas datus, kas attiecas uz Eiropas digitālās identitātes maku nodrošināšanu, glabā loģiski nošķirti no jebkuriem citiem datiem, kas ir Eiropas digitālās identitātes maka nodrošinātāja rīcībā. Ja Eiropas digitālās identitātes maku nodrošina privātas puses saskaņā ar šā panta 2. punkta b) un c) apakšpunktu, *mutatis mutandis* piemēro 45.h panta 3. punkta noteikumus.

15. Eiropas digitālās identitātes maku izmantošana ir brīvprātīga. Tādu fizisku vai juridisku personu piekļuve publiskiem un privātiem pakalpojumiem, piekļuve darba tirgum un darījumdarbības brīvība, kuras neizmanto Eiropas digitālās identitātes maku, netiek nekādi ierobežota vai padarīta neizdevīga. Publiskiem un privātajiem pakalpojumiem arī turpmāk var piekļūt, izmantojot citus esošus identifikācijas un autentifikācijas līdzekļus.

16. Eiropas digitālās identitātes maka tehniskā sistēma:

a) neļauj atribūtu elektronisko apliecinājumu sniedzējiem vai jebkurai citai pusei pēc atribūtu apliecinājuma izdošanas iegūt datus, kas ļauj izsekot darījumiem vai lietotāju uzvedībai, sasaistīt vai korelēt, vai citādi iegūt zināšanas par darījumiem vai lietotāju uzvedību, ja vien lietotājs to nav nepārprotami atļāvis;

b) iespējo privātuma saglabāšanas paņēmienus, kas nodrošina nesasaistāmību, ja atribūtu apliecināšanai nav nepieciešama lietotāja identifikācija.

17. Jebkādu personas datu apstrādi, ko veic dalībvalstis vai ko veic to vārdā struktūras vai puses, kuras ir atbildīgas par Eiropas digitālās identitātes maku kā elektroniskās identifikācijas līdzekļu nodrošināšanu, veic saskaņā ar piemērotiem un efektīviem datu aizsardzības pasākumiem. Pierāda šādas apstrādes atbilstību Regulai (ES) 2016/679. Dalībvalstis var ieviest valstu noteikumus, lai sīkāk precizētu šādu pasākumu piemērošanu.

18. Dalībvalstis bez nepamatotas kavēšanās paziņo Komisijai turpmāk minēto informāciju par:

a) struktūru, kas saskaņā ar 5.b panta 5. punktu atbild par to reģistrēto atkarīgo pušu saraksta izveidi un uzturēšanu, kuras izmanto Eiropas digitālās identitātes makus, un minētā saraksta atrašanās vietu;

b) struktūrām, kas atbild par Eiropas digitālās identitātes maku nodrošināšanu saskaņā ar 5.a panta 1. punktu;

c) struktūrām, kas atbild par to, lai personas identifikācijas dati būtu saistīti ar Eiropas digitālās identitātes maku saskaņā ar 5.a panta 5. punkta f) apakšpunktu;

d) mehānismu, kas ļauj validēt 5.a panta 5. punkta f) apakšpunktā minētos personas identifikācijas datus un atkarīgo pušu identitāti;

e) mehānismu, ar ko validē Eiropas digitālās identitātes maku autentiskumu un derīgumu.

Izmantojot drošu kanālu, Komisija publisko saskaņā ar pirmo daļu paziņoto informāciju, kura ir elektroniski parakstīta vai apzīmogota un sagatavota automatizētai apstrādei piemērotā formātā.

19. Neskarot šā panta 22. punktu, 11. pantu *mutatis mutandis* piemēro Eiropas digitālās identitātes makam.

20. Regulas 24. panta 2. punkta b) un d)–h) apakšpunktu *mutatis mutandis* piemēro Eiropas digitālās identitātes maku nodrošinātājiem.

21. Eiropas digitālās identitātes makus dara pieejamus lietošanai personām ar invaliditāti – ar tādiem pašiem nosacījumiem kā citiem lietotājiem – saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2019/882 (*).

22. Eiropas digitālās identitātes maku nodrošināšanas nolūkos Eiropas digitālās identitātes makiem un elektroniskās identifikācijas shēmām, saskaņā ar kurām tie tiek nodrošināti, nepiemēro 7., 9., 10., 12. un 12.a pantā noteiktās prasības.

23. Līdz 2024. gada 21. novembrim Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šā panta 4., 5., 8. un 18. punktā noteiktajām prasībām attiecībā uz Eiropas digitālās identitātes maka īstenošanu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

24. Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka tehniskās specifikācijas un procedūras, lai atvieglotu lietotāju pievienošanu Eiropas digitālās identitātes makā, izmantojot vai nu elektroniskās identifikācijas līdzekļus, kas atbilst uzticamības līmenim "augsts", vai elektroniskās identifikācijas līdzekļus, kas atbilst uzticamības līmenim "būtisks", saistībā ar papildu attālinātās pievienošanas procedūrām, kas kopā atbilst uzticamības līmeņa "augsts" prasībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

5.b pants

Eiropas digitālās identitātes maku atkarīgās puses

1. Ja atkarīgā puse plāno izmantot Eiropas digitālās identitātes makus, lai sniegtu publiskus vai privātus pakalpojumus, izmantojot digitālu mijiedarbību, tā reģistrējas dalībvalstī, kurā tā veic uzņēmējdarbību.

2. Reģistrācijas process ir izmaksu ziņā lietderīgs un samērīgs ar riskiem. Atkarīgā puse iesniedz vismaz:

a) informāciju, kas vajadzīga, lai autentificētos Eiropas digitālās identitātes makiem, un kas ietver vismaz:

i) dalībvalsti, kurā atkarīgā puse veic uzņēmējdarbību; un

ii) atkarīgās puses nosaukumu un attiecīgā gadījumā tās reģistrācijas numuru, kas norādīts oficiālā reģistrā, kopā ar minētā oficiālā reģistra identifikācijas datiem;

b) atkarīgās puses kontaktinformāciju;

c) paredzēto Eiropas digitālās identitātes maku izmantojumu, tostarp norādi par datiem, ko atkarīgā puse pieprasīs no lietotājiem.

3. Atkarīgās puses nepieprasa lietotājiem sniegt citus datus kā vien tos, kas norādīti, ievērojot 2. punkta c) apakšpunktu.

4. Šā panta 1. un 2. punkts neskar Savienības vai valstu tiesību aktus, kas ir piemērojami konkrētu pakalpojumu sniegšanai.

5. Izmantojot drošu kanālu, dalībvalstis publisko 2. punktā minēto informāciju elektroniski parakstītā vai apzīmogotā veidā, automatizētai apstrādei piemērotā formātā.

6. Atkarīgās puses, kas reģistrētas saskaņā ar šo pantu, nekavējoties informē dalībvalstis par visām izmaiņām informācijā, kas reģistrācijā sniegta, ievērojot 2. punktu.

7. Dalībvalstis nodrošina kopīgu mehānismu, kas ļauj identificēt un autentificēt atkarīgās puses, kā minēts 5.a panta 5. punkta c) apakšpunktā.

8. Ja atkarīgās puses paredz paļauties uz Eiropas digitālās identitātes makiem, kas nodrošināti saskaņā ar šo regulu, tās sevi identificē Eiropas digitālās identitātes maka lietotājam.

9. Atkarīgās puses ir atbildīgas par procedūru veikšanu, ar ko autentificē un validē personas identifikācijas datus un atribūtu elektronisko apliecinājumu, kuri pieprasīti no Eiropas digitālās identitātes makiem. Atkarīgās puses neatsaka pseidonīmu izmantošanu, ja lietotāja identifikācija nav prasīta Savienības vai valstu tiesību aktos.

10. Starpnieki, kas rīkojas atkarīgo pušu vārdā, ir uzskatāmi par atkarīgām pusēm un neglabā datus par darījuma saturu.

11. Līdz 2024. gada 21. novembrim Komisija ar īstenošanas aktiem par Eiropas digitālās identitātes maku īstenošanu, kā minēts 5.a panta 23. punktā, nosaka tehniskās specifikācijas un procedūras, kas minētas šā panta 2., 5. un 6.–9. punktā minētajām prasībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

5.c pants

Eiropas digitālās identitātes maku sertifikācija

1. Eiropas digitālās identitātes maku un elektroniskās identifikācijas shēmas, saskaņā ar kuru tie tiek nodrošināti, atbilstību 5.a panta 4., 5. un 8. punktā noteiktajām prasībām, 5.a panta 14. punktā noteiktajai prasībai par loģisko nošķiršanu un attiecīgā gadījumā 5.a panta 24. punktā minētajiem standartiem un tehniskajām specifikācijām sertificē atbilstības novērtēšanas struktūras, ko izraudzījušās dalībvalstis.

2. Eiropas digitālās identitātes maku atbilstību prasībām, kas minētas šā panta 1. punktā un kas ir nozīmīgas kiberdrošībai, vai to daļām sertificē saskaņā ar Eiropas kiberdrošības sertifikācijas shēmām, kas pieņemtas, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2019/881 (**), un minētas šā panta 6. punktā minētajos īstenošanas aktos.

3. Attiecībā uz šā panta 1. punktā minētajām prasībām, kas nav nozīmīgas kiberdrošībai, un attiecībā uz šā panta 1. punktā minētajām prasībām, kas ir nozīmīgas kiberdrošībai, tiktāl, ciktāl šā panta 2. punktā minētās kiberdrošības sertifikācijas shēmas neaptver vai tikai daļēji aptver minētās kiberdrošības prasības, arī attiecībā uz minētajām prasībām dalībvalstis izveido valstu sertifikācijas shēmas, ievērojot prasības, kas noteiktas šā panta 6. punktā minētajos īstenošanas aktos. Dalībvalstis nosūta savus valsts sertifikācijas shēmu projektus Eiropas Digitālās identitātes sadarbības grupai, kas izveidota saskaņā ar 46.e panta 1. punktu ("sadarbības grupa"). Sadarbības grupa var izdot atzinumus un ieteikumus.

4. Sertifikācija saskaņā ar šā panta 1. punktu ir derīga ne ilgāk par pieciem gadiem, ja reizi divos gados tiek veikts ievainojamības novērtējums. Ja konstatēta ievainojamība un tā netiek laicīgi novērsta trīs mēnešu laikā pēc šādas konstatācijas, sertifikāciju anulē.

5. Atbilstību šīs regulas 5.a pantā noteiktajām prasībām, kas saistītas ar personas datu apstrādes darbībām, var sertificēt, ievērojot Regulu (ES) 2016/679.

6. Līdz 2024. gada 21. novembrim Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šā panta 1., 2. un 3. punktā minētajai Eiropas digitālās identitātes maku sertifikācijai. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

7. Dalībvalstis paziņo Komisijai 1. punktā minēto atbilstības novērtēšanas struktūru nosaukumu un adresi. Komisija minēto informāciju dara pieejamu visām dalībvalstīm.

8. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 47. pantu attiecībā uz tādu konkrētu kritēriju noteikšanu, kuri jāievēro šā panta 1. punktā minētajām atbilstības novērtēšanas struktūrām.

5.d pants

Sertificēto Eiropas digitālās identitātes maku saraksta publicēšana

1. Dalībvalstis bez nepamatotas kavēšanās informē Komisiju un saskaņā ar 46.e panta 1. punktu izveidoto sadarbības grupu par Eiropas digitālās identitātes makiem, kas nodrošināti, ievērojot 5.a pantu, un ko sertificējušas 5. c panta 1. punktā minētās atbilstības novērtēšanas struktūras. Tās bez nepamatotas kavēšanās informē Komisiju un saskaņā ar 46.e panta 1. punktu izveidoto sadarbības grupu, ja sertifikācija ir anulēta, un norāda anulēšanas iemeslus.

2. Neskarot 5.a panta 18. punktu, šā panta 1. punktā minētajā dalībvalstu sniegtajā informācijā iekļauj vismaz šādus elementus:

a) sertificētā Eiropas digitālās identitātes maka sertifikātu un sertifikācijas novērtējuma ziņojumu;

b) tās elektroniskās identifikācijas shēmas aprakstu, saskaņā ar kuru tiek nodrošināts Eiropas digitālās identitātes maks;

c) piemērojamo uzraudzības režīmu un informāciju par atbildības režīmu attiecībā uz pusi, kura nodrošina Eiropas digitālās identitātes maku;

d) iestādi vai iestādes, kas ir atbildīga(-as) par elektroniskās identifikācijas shēmu;

e) elektroniskās identifikācijas shēmas vai autentifikācijas, vai attiecīgo kompromitēto daļu apturēšanas vai atsaukšanas kārtību.

3. Pamatojoties informāciju, kas saņemta, ievērojot 1. punktu, Komisija izveido, publicē *Eiropas Savienības Oficiālajā Vēstnesī* un uztur mašīnlasāmā veidā sertificētu Eiropas digitālās identitātes maku sarakstu.

4. Dalībvalsts var iesniegt Komisijai pieprasījumu no 3. punktā minētā saraksta izņemt Eiropas digitālās identitātes maku un elektroniskās identifikācijas shēmu, saskaņā ar kuru tas tiek nodrošināts.

5. Ja ir izmaiņas informācijā, kas sniegta, ievērojot 1. punktu, dalībvalsts sniedz Komisijai atjauninātu informāciju.

6. Komisija atjaunina 3. punktā minēto sarakstu, attiecīgos saraksta grozījumus publicējot *Eiropas Savienības Oficiālajā Vēstnesī* viena mēneša laikā pēc tam, kad saņemts pieprasījums, ievērojot 4. punktu, vai atjaunināta informācija, ievērojot 5. punktu.

7. Līdz 2024. gada 21. novembrim Komisija, pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 5.a panta 23. punktā, nosaka šā panta 1., 4. un 5. punkta vajadzībām piemērojamos formātus un procedūras. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

5.e pants

Eiropas digitālās identitātes maku drošības prasību pārkāpums

1. Ja attiecībā uz Eiropas digitālās identitātes makiem, kas nodrošināti, ievērojot 5.a pantu, 5.a panta 8. punktā minētajiem validācijas mehānismiem vai elektroniskās identifikācijas shēmu, saskaņā ar kuru Eiropas digitālās identitātes maks tiek nodrošināts, ir noticis pārkāpums vai tie ir daļēji kompromitēti tādā veidā, kas ietekmē to uzticamību vai citu Eiropas digitālās identitātes maku uzticamību, dalībvalsts, kura nodrošinājusi attiecīgo Eiropas digitālās identitātes maku, bez nepamatotas kavēšanās aptur Eiropas digitālās identitātes maku nodrošināšanu un izmantošanu.

Gadījumā, kad to pamato pirmajā daļā minētā drošības pārkāpuma vai kompromitējuma nopietnība, dalībvalsts bez liekas kavēšanās atsauc Eiropas digitālās identitātes makus.

Dalībvalsts attiecīgi informē skartos lietotājus, vienotos kontaktpunktus, kas izraudzīti, ievērojot 46.c panta 1. punktu, atkarīgās puses un Komisiju.

2. Ja šā panta 1. punkta pirmajā daļā minētais drošības pārkāpums vai kompromitējums nav novērsts trīs mēnešu laikā pēc apturēšanas, dalībvalsts, kas nodrošinājusi Eiropas digitālās identitātes makus, atsauc minētos Eiropas digitālās identitātes makus un atsauc to derīgumu. Dalībvalsts attiecīgi informē par atsaukšanu skartos lietotājus, vienotos kontaktpunktus, kas izraudzīti, ievērojot 46.c panta 1. punktu, atkarīgās puses un Komisiju.

3. Ja šā panta 1. punkta pirmajā daļā minētais drošības pārkāpums vai kompromitējums ir novērsts, nodrošinātāja dalībvalsts bez nepamatotas kavēšanās atjauno Eiropas digitālās identitātes maku nodrošināšanu un izmantošanu un informē skartos lietotājus un atkarīgās puses, vienotos kontaktpunktus, kas izraudzīti, ievērojot 46.c panta 1. punktu, un Komisiju.

4. Komisija bez nepamatotas kavēšanās publicē *Eiropas Savienības Oficiālajā Vēstnesī* 5.d pantā minētā saraksta attiecīgos grozījumus.

5. Līdz 2024. gada 21. novembrim Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šā panta 1., 2. un 3. punktā minētajiem pasākumiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

5.f pants

Eiropas digitālās identitātes maku izmantošana pāri robežām

1. Ja dalībvalstis prasa elektronisko identifikāciju un autentifikāciju piekļuvei publiskas iestādes sniegtam tiešsaistes pakalpojumam, tās pieņem arī Eiropas digitālās identitātes makus, kas nodrošināti saskaņā ar šo regulu.

2. Ja privātām atkarīgajām pusēm, kas sniedz pakalpojumus, izņemot mikrouzņēmumus un mazos uzņēmumus, kā definēts Komisijas Ieteikuma 2003/361/EK (***) pielikuma 2. pantā, saskaņā ar Savienības vai valstu tiesību aktiem tiešsaistes identifikācijai ir jāizmanto droša lietotāju autentifikācija vai ja droša lietotāju autentifikācija tiešsaistes identifikācijai ir nepieciešama saskaņā ar līgumsaistībām, tostarp tādās jomās kā transports, enerģētika, banku pakalpojumi, finanšu pakalpojumi, sociālais nodrošinājums, veselība, dzeramais ūdens, pasta pakalpojumi, digitālā infrastruktūra, izglītība vai telesakari, minētās privātās atkarīgās puses ne vēlāk kā 36 mēnešus no 5.a panta 23. punktā un 5.c panta 6. punktā minēto īstenošanas aktu spēkā stāšanās dienas un vienīgi pēc lietotāja brīvprātīgi izteikta pieprasījuma pieņem Eiropas digitālās identitātes makus, kas nodrošināti saskaņā ar šo regulu.

3. Ja ļoti lielu tiešsaistes platformu nodrošinātāji, kā minēts Eiropas Parlamenta un Padomes Regulas (ES) 2022/2065 33. pantā (****), prasa lietotājiem autentificēties, lai piekļūtu tiešsaistes pakalpojumiem, tās arī piekrīt tam un sekmē to, ka saskaņā ar šo regulu nodrošinātie Eiropas digitālās identitātes maki tiek izmantoti lietotāja autentifikācijai vienīgi pēc lietotāja izteikta brīvprātīga pieprasījuma un attiecībā uz minimālajiem datiem, kas nepieciešami konkrētajam tiešsaistes pakalpojumam, kura vajadzībām tiek pieprasīta lietotāja autentifikācija.

4. Lai veicinātu to, ka šīs regulas darbības jomā esošie Eiropas digitālās identitātes maki ir plaši pieejami un izmantojami un mudinātu pakalpojumu sniedzējus pabeigt rīcības kodeksu izstrādi, Komisija sadarbībā ar dalībvalstīm sekmē rīcības kodeksu izstrādi ciešā kopdarbā ar visām attiecīgajām ieinteresētajām personām, tostarp pilsonisko sabiedrību.

5. Komisija 24 mēnešu laikā pēc Eiropas digitālās identitātes maku ieviešanas novērtē pieprasījumu pēc Eiropas digitālās identitātes makiem, to pieejamību un izmantojamību, ņemot vērā tādus kritērijus kā to pieņemšana no lietotāju puses, pakalpojumu sniedzēju klātbūtne pāri robežām, tehnoloģiskā attīstība, lietošanas modeļu dinamika un patērētāju pieprasījums.

(*) Eiropas Parlamenta un Padomes Direktīva (ES) 2019/882 (2019. gada 17. aprīlis) par produktu un pakalpojumu piekļūstamības prasībām (OV L 151, 7.6.2019., 70. lpp.).

(**) Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

(***) Komisijas Ieteikums 2003/361/EK (2003. gada 6. maijs) par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

(****) Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (OV L 277, 27.10.2022., 1. lpp.).";

6) pirms regulas 6. panta iekļauj šādu virsrakstu:

"2. IEDAĻA

ELEKTRONISKĀS IDENTIFIKĀCIJAS SHĒMAS";

7) Regulas 7. panta g) punktu aizstāj ar šādu:

"g) vismaz sešus mēnešus pirms paziņošanas saskaņā ar 9. panta 1. punktu paziņotāja dalībvalsts 12. panta 5. punkta nolūkā pārējām dalībvalstīm sniedz minētās shēmas aprakstu saskaņā ar 12. panta 6. punktu pieņemtajos īstenošanas aktos noteikto procesuālo kārtību;";

8) regulas 8. panta 3. punkta pirmo daļu aizstāj ar šādu:

"3. Līdz 2015. gada 18. septembrim, ņemot vērā attiecīgos starptautiskos standartus un ievērojot 2. punktu, Komisija ar īstenošanas aktiem nosaka minimālās tehniskās specifikācijas, standartus un procedūras, uz kuriem atsaucoties, ir noteikts elektroniskās identifikācijas līdzekļu uzticamības līmenis "zems", "būtisks" un "augsts".";

9) regulas 9. panta 2. un 3. punktu aizstāj ar šādiem:

"2. Komisija bez nepamatotas kavēšanās *Eiropas Savienības Oficiālajā Vēstnesī* publicē to elektroniskās identifikācijas shēmu sarakstu, par kurām iesniegts paziņojums, ievērojot 1. punktu, kopā ar pamatinformāciju par minētajām shēmām.

3. Viena mēneša laikā pēc minētā paziņojuma saņemšanas dienas Komisija *Eiropas Savienības Oficiālajā Vēstnesī* publicē 2. punktā minētā saraksta grozījumus.";

10) 10. panta virsrakstu aizstāj ar šādu:

"Elektroniskās identifikācijas shēmu drošības prasību pārkāpums";

11) regulā iekļauj šādu pantu:

"*11.a pants*

Pārrobežu identitātes saskaņošana

1. Rīkojoties kā atkarīgās puses pārrobežu pakalpojumu jomā, dalībvalstis nodrošina nepārprotamu identitātes saskaņošanu fiziskām personām, kuras izmanto paziņotos elektroniskās identifikācijas līdzekļus vai Eiropas digitālās identitātes makus.

2. Dalībvalstis paredz tehniskus un organizatoriskus pasākumus, lai nodrošinātu augsta līmeņa aizsardzību personas datiem, ko izmanto identitātes saskaņošanai, un lai novērstu lietotāju profilēšanu.

3. Līdz 2024. gada 21. novembrim Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šā panta 1. punktā minētajām prasībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

12) regulas 12. pantu groza šādi:

a) virsrakstu aizstāj ar šādu:

"Sadarbspēja";

b) panta 3. punktu groza šādi:

i) punkta c) apakšpunktu aizstāj ar šādu:

"c) tā sekmē integrētu privātuma un drošības īstenošanu;";

ii) d) apakšpunktu svītro;

c) panta 4. punkta d) apakšpunktu aizstāj ar šādu:

"d) atsauci uz personas identifikācijas datu minimālo kopumu, kas vajadzīgi, lai unikāli apliecinātu fizisku vai juridisku personu vai fizisku personu, kura pārstāv citu fizisku personu vai juridisku personu, un kas ir pieejams no elektroniskās identifikācijas shēmām;";

d) panta 5. un 6. punktu aizstāj ar šādiem:

"5. Dalībvalstis veic to elektroniskās identifikācijas shēmu salīdzinošo izvērtēšanu, kuras ietilpst šīs regulas darbības jomā un par kurām jāpaziņo, ievērojot 9. panta 1. punkta a) apakšpunktu.

6. Līdz 2025. gada 18. martam Komisija ar īstenošanas aktiem nosaka vajadzīgo procesuālo kārtību šā panta 5. punktā minētajai salīdzinošajai izvērtēšanai, lai sekmētu riska pakāpei atbilstošu augsta līmeņa uzticamību un drošību. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

e) panta 7. punktu svītro;

f) panta 8. punktu aizstāj ar šādu:

"8. Līdz 2025. gada 18. septembrim, lai noteiktu vienādus nosacījumus šā panta 1. punktā minētās prasības īstenošanai, Komisija, ievērojot šā panta 3. punktā noteiktos kritērijus un ņemot vērā dalībvalstu sadarbības rezultātus, pieņem īstenošanas aktus attiecībā uz šā panta 4. punktā izklāstīto sadarbspējas sistēmu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

13) regulas II nodaļā iekļauj šādus pantus:

"*12.a pants*

Elektroniskās identifikācijas shēmu sertifikācija

1. Paziņojamo elektroniskās identifikācijas shēmu atbilstību šajā regulā noteiktajām kiberdrošības prasībām, tostarp atbilstību attiecīgajām kiberdrošības prasībām, kas noteiktas 8. panta 2. punktā attiecībā uz elektroniskās identifikācijas shēmu uzticamības līmeņiem, sertificē dalībvalstu izraudzītas atbilstības novērtēšanas struktūras.

2. Sertifikāciju saskaņā ar šā panta 1. punktu veic atbilstīgi attiecīgai kiberdrošības sertifikācijas shēmai, ievērojot Regulu (ES) 2019/881, vai tās daļām, ciktāl kiberdrošības sertifikāts attiecas uz minētajām kiberdrošības prasībām.

3. Sertifikācija saskaņā ar 1. punktu ir derīga ne ilgāk par pieciem gadiem ar noteikumu, ka ievainojamības novērtējums tiek veikts reizi divos gados. Ja konstatēta ievainojamība un tā netiek novērsta trīs mēnešu laikā pēc konstatācijas, sertifikāciju anulē.

4. Neatkarīgi no 2. punkta, dalībvalstis no paziņotājas dalībvalsts saskaņā ar minēto punktu var pieprasīt papildu informāciju par elektroniskās identifikācijas shēmām vai to daļu.

5. Elektroniskās identifikācijas shēmu salīdzinošo izvērtēšanu, kas minēta 12. panta 5. punktā, nepiemēro elektroniskās identifikācijas shēmām vai šādu shēmu daļām, kas sertificētas saskaņā ar šā panta 1. punktu. Dalībvalstis var izmantot sertifikātu vai atbilstības apliecinājumu, kas izdots saskaņā ar attiecīgu kiberdrošības sertifikācijas shēmu vai šādu shēmu daļām, par atbilstību ar kiberdrošību nesaistītajām 8. panta 2. punktā noteiktajām prasībām attiecībā uz elektroniskās identifikācijas shēmu uzticamības līmeņiem.

6. Dalībvalstis paziņo Komisijai 1. punktā minēto atbilstības novērtēšanas struktūru nosaukumu un adresi. Komisija minēto informāciju dara pieejamu visām dalībvalstīm.

12.b pants

Piekļuve aparatūrai un programmatūras funkcijām

Ja Eiropas digitālās identitātes maku nodrošinātāji un paziņotu elektroniskās identifikācijas līdzekļu izdevēji, kas rīkojas komerciālā vai profesionālā statusā un izmanto platformas pamatpakalpojumus, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2022/1925 (*) 2. panta 2. punktā, nolūkā nodrošināt Eiropas digitālās identitātes maku pakalpojumus un elektroniskās identifikācijas līdzekļus tiešajiem lietotājiem vai tos izmanto šādas nodrošināšanas laikā, ir komerciālie lietotāji, kā definēts minētās regulas 2. panta 21. punktā, vārtziņi jo īpaši nodrošina tiem efektīvu sadarbspēju ar tām pašām operētājsistēmas, aparatūras vai programmatūras funkcijām un dod tiem iespēju sadarbspējas nolūkā tām piekļūt. Šāda efektīva sadarbspēja un piekļuve tiek nodrošināta bez maksas un neatkarīgi no tā, vai aparatūras vai programmatūras funkcijas ir daļa no operētājsistēmas, kas ir pieejamas minētajam vārtzinim vai ko tas izmanto, sniedzot šādus pakalpojumus Regulas (ES) 2022/1925 6. panta 7. punkta nozīmē. Šis pants neskar šīs regulas 5.a panta 14. punktu.

(*) Eiropas Parlamenta un Padomes Regula (ES) 2022/1925 (2022. gada 14. septembris) par sāncensīgiem un godīgiem tirgiem digitālajā nozarē un ar ko groza Direktīvas (ES) 2019/1937 un (ES) 2020/1828 (Digitālo tirgu akts) (OV L 265, 12.10.2022., 1. lpp.).";

14) regulas 13. panta 1. punktu aizstāj ar šādu:

"1. Neatkarīgi no šā panta 2. punkta un neskarot Regulu (ES) 2016/679, uzticamības pakalpojumu sniedzēji ir atbildīgi par zaudējumiem, kas apzināti vai nolaidības dēļ radīti jebkurai fiziskai vai juridiskai personai tādēļ, ka nav ievēroti šajā regulā noteiktie pienākumi. Jebkurai fiziskai vai juridiskai personai, kurai nodarīti materiāli vai nemateriāli zaudējumi tādēļ, ka uzticamības pakalpojumu sniedzējs ir pārkāpis šo regulu, ir tiesības pieprasīt kompensāciju saskaņā ar Savienības un valstu tiesību aktiem.

Pienākums pierādīt nekvalificēta uzticamības pakalpojumu sniedzēja nodomu vai nolaidību ir fiziskai vai juridiskai personai, kas iesniedz prasību par šā punkta pirmajā daļā minētajiem zaudējumiem.

Tiek prezumēts kvalificēta uzticamības pakalpojumu sniedzēja nodoms vai neuzmanība, ja vien minētais kvalificētais uzticamības pakalpojumu sniedzējs nepierāda, ka šā punkta pirmajā daļā minētais zaudējums ir noticis bez kvalificētā uzticamības pakalpojumu sniedzēja nodoma vai nolaidības.";

15) regulas 14., 15. un 16. pantu aizstāj ar šādu:

"*14. pants*

Starptautiskie aspekti

1. Uzticamības pakalpojumus, ko sniedz uzticamības pakalpojumu sniedzēji, kuri ir iedibināti trešā valstī, vai starptautiska organizācija, atzīst par juridiski līdzvērtīgiem kvalificētiem uzticamības pakalpojumiem, ko sniedz kvalificēti uzticamības pakalpojumu sniedzēji, kuri ir iedibināti Savienībā, ja uzticamības pakalpojumi, kuru izcelsme ir trešā valstī vai starptautiskā organizācijā, ir atzīti ar īstenošanas aktiem vai nolīgumu, kas noslēgts starp Savienību un trešo valsti vai starptautisko organizāciju, ievērojot LESD 218. pantu.

Pirmajā daļā minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

2. Ar 1. punktā minētajiem īstenošanas aktiem un nolīgumu nodrošina, ka prasības, kuras piemērojamas kvalificētiem uzticamības pakalpojumu sniedzējiem, kas iedibināti Savienībā, un to sniegtajiem kvalificētiem uzticamības pakalpojumiem, ievēro uzticamības pakalpojumu sniedzēji attiecīgajā trešā valstī vai starptautiskās organizācijas un ka šīs prasības ievēro arī attiecībā uz to sniegtajiem uzticamības pakalpojumiem. Trešās valstis un starptautiskās organizācijas jo īpaši izveido, uztur un publicē uzticamības sarakstu ar atzītiem uzticamības pakalpojumu sniedzējiem.

3. Ar 1. punktā minētajiem nolīgumiem nodrošina, ka kvalificētos uzticamības pakalpojumus, ko sniedz kvalificēti uzticamības pakalpojumu sniedzēji, kuri iedibināti Savienībā, atzīst kā juridiski līdzvērtīgus tiem uzticamības pakalpojumiem, ko sniedz uzticamības pakalpojumu sniedzēji trešā valstī vai starptautiskā organizācija, ar kuru ir noslēgts nolīgums.

15. pants

Piekļūstamība personām ar invaliditāti un ar īpašām vajadzībām

Elektroniskās identifikācijas līdzekļu, uzticamības pakalpojumu sniegšana un minēto pakalpojumu sniegšanā izmantoto tiešā lietotāja produktu nodrošināšana tiek darīta pieejama vienkāršā un saprotamā valodā saskaņā ar Apvienoto Nāciju Organizācijas Konvenciju par personu ar invaliditāti tiesībām un saskaņā ar Direktīvas (ES) 2019/882 piekļūstamības prasībām, tādējādi sniedzot labumu arī personām ar funkcionāliem ierobežojumiem, piemēram, veciem cilvēkiem, un personām ar ierobežotu piekļuvi digitālajām tehnoloģijām.

16. pants

Sankcijas

1. Neskarot Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2555 (*) 31. pantu, dalībvalstis paredz noteikumus par sankcijām, kas piemērojamas par šīs regulas pārkāpumiem. Minētās sankcijas ir iedarbīgas, samērīgas un atturošas.

2. Dalībvalstis nodrošina, ka par šīs regulas pārkāpumiem, ko izdarījuši kvalificēti un nekvalificēti uzticamības pakalpojumu sniedzēji, piemēro administratīvus naudas sodus, kuru maksimālais apmērs ir vismaz:

a) 5 000 000 EUR, ja uzticamības pakalpojumu sniedzējs ir fiziska persona; vai

b) ja uzticamības pakalpojumu sniedzējs ir juridiska persona, 5 000 000 EUR jeb 1 % no tā uzņēmuma kopējā gada apgrozījuma pasaulē, pie kura uzticamības pakalpojumu sniedzējs piederēja finanšu gadā pirms gada, kurā noticis pārkāpums, atkarībā no tā, kura summa ir lielāka.

3. Atkarībā no dalībvalstu tiesību sistēmas noteikumus par administratīvajiem naudas sodiem var piemērot tādā veidā, ka naudas sodu ierosina kompetentā uzraudzības iestāde un uzliek kompetentās valstu tiesas. Šādu noteikumu piemērošana minētajās dalībvalstīs nodrošina, ka minētie tiesiskās aizsardzības līdzekļi ir efektīvi un ka tiem ir līdzvērtīga ietekme kā administratīvajiem naudas sodiem, ko tieši piemēro uzraudzības iestādes.

(*) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).";

16) regulas III nodaļas 2 iedaļas nosaukumu aizstāj ar šādu:

"Nekvalificēti uzticamības pakalpojumi";

17) regulas 17. un 18. pantu svītro;

18) regulas III nodaļas 2. iedaļā iekļauj šādu pantu:

"*19.a pants*

Prasības nekvalificētiem uzticamības pakalpojumu sniedzējiem

1. Nekvalificēts uzticamības pakalpojumu sniedzējs, nodrošinot nekvalificētus uzticamības pakalpojumus:

a) ir ieviesis attiecīgu politiku un veic atbilstošus pasākumus, lai pārvaldītu juridiskos, uzņēmējdarbības, operacionālos un citus tiešos vai netiešos riskus nekvalificētā uzticamības pakalpojuma sniegšanā, kuri, neatkarīgi no Direktīvas (ES) 2022/2555 21. panta, ietver pasākumus vismaz saistībā ar:

i) uzticamības pakalpojuma reģistrācijas un pievienošanas procedūrām;

ii) procesuālajām vai administratīvajām pārbaudēm, kas vajadzīgas uzticamības pakalpojumu sniegšanai;

iii) uzticamības pakalpojumu pārvaldību un īstenošanu;

b) paziņošanu uzraudzības iestādei, identificējamām skartajām personām, sabiedrībai, ja tas ir sabiedrības interesēs, un attiecīgā gadījumā citām attiecīgajām kompetentajām iestādēm par visiem tiem drošības pārkāpumiem vai traucējumiem pakalpojuma sniegšanā vai a) apakšpunkta i), ii) un iii) punktā minēto pasākumu īstenošanā, kuri būtiski ietekmē sniegto uzticamības pakalpojumu vai tajā glabātos personas datus, un to dara bez nepamatotas kavēšanās un jebkurā gadījumā ne vēlāk kā 24 stundu laikā no brīža, kad jebkādi drošības pārkāpumi vai traucējumi kļuvuši zināmi.

2. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras attiecībā uz šā panta 1. punkta a) apakšpunktu. Uzskata, ka atbilstība šajā pantā noteiktajām prasībām ir panākta tad, ja ir izpildīti minētie standarti, specifikācijas un procedūras. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

19) regulas 20. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Kvalificētu uzticamības pakalpojumu sniedzēju revīziju par minēto pakalpojumu sniedzēju līdzekļiem vismaz ik pēc 24 mēnešiem veic atbilstības novērtēšanas struktūra. Revīzijas nolūks ir apstiprināt, ka kvalificētie uzticamības pakalpojumu sniedzēji un to sniegtie kvalificētie uzticamības pakalpojumi atbilst prasībām, kas noteiktas šajā regulā un Direktīvas (ES) 2022/2555 21. pantā. Kvalificētie uzticamības pakalpojumu sniedzēji trīs darba dienu laikā pēc iegūtā atbilstības novērtēšanas ziņojuma saņemšanas to iesniedz uzraudzības iestādei.";

b) pantā iekļauj šādus punktus:

"1.a Kvalificēti uzticamības pakalpojumu sniedzēji ne vēlāk kā vienu mēnesi pirms jebkādām plānotajām revīzijām informē uzraudzības iestādi un ļauj uzraudzības iestādei pēc pieprasījuma piedalīties novērotāja statusā.

1.b Dalībvalstis bez nepamatotas kavēšanās paziņo Komisijai 1. punktā minēto atbilstības novērtēšanas struktūru nosaukumus, adreses un akreditācijas informāciju, kā arī visas turpmākās izmaiņas šajā informācijā. Komisija minēto informāciju dara pieejamu visām dalībvalstīm.";

c) panta 2., 3. un 4. punktu aizstāj ar šādu:

"2. Neskarot 1. punktu, uzraudzības iestāde var jebkurā laikā veikt revīziju vai lūgt atbilstības novērtēšanas struktūrai veikt kvalificēto uzticamības pakalpojumu sniedzēju atbilstības novērtēšanu par minēto uzticamības pakalpojumu sniedzēju līdzekļiem, lai apstiprinātu, ka tie un to sniegtie kvalificētie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām. Ja personas datu aizsardzības noteikumi, iespējams, ir pārkāpti, uzraudzības iestāde bez nepamatotas kavēšanās informē kompetentās uzraudzības iestādes, kas izveidotas, ievērojot Regulas (ES) 2016/679 51. pantu.

3. Ja kvalificētais uzticamības pakalpojumu sniedzējs neizpilda kādu no šajā regulā noteiktajām prasībām, uzraudzības iestāde pieprasa, lai tas attiecīgā gadījumā noteiktajā termiņā labotu prasību neizpildi.

Ja minētais pakalpojumu sniedzējs nav labojis prasību neizpildi un attiecīgā gadījumā uzraudzības iestādes noteiktajā termiņā, uzraudzības iestāde, ja tas ir pamatoti jo īpaši minētās neizpildes apmēra, ilguma un seku dēļ, anulē minētā pakalpojumu sniedzēja vai tā skartā pakalpojuma kvalifikācijas statusu, kuru tas sniedz.

3.a Ja kompetentās iestādes, kas izraudzītas vai izveidotas, ievērojot Direktīvas (ES) 2022/2555 8. panta 1. punktu, informē uzraudzības iestādi par to, ka kvalificētais uzticamības pakalpojumu sniedzējs nepilda kādu no minētās direktīvas 21. pantā noteiktajām prasībām, uzraudzības iestāde, ja tas ir pamatoti jo īpaši minētās neizpildes apmēra, ilguma un seku dēļ, anulē minētā pakalpojumu sniedzēja vai tā skartā pakalpojuma kvalifikācijas statusu, kuru tas sniedz.

3.b Ja uzraudzības iestādes, kas izveidotas, ievērojot Regulas (ES) 2016/679 51. pantu, informē uzraudzības iestādi par to, ka kvalificētais uzticamības pakalpojumu sniedzējs nepilda kādu no minētajā Regulā noteiktajām prasībām, uzraudzības iestāde, ja tas ir pamatoti jo īpaši minētās neizpildes apmēra, ilguma un seku dēļ, anulē minētā pakalpojumu sniedzēja vai tā skartā pakalpojuma kvalifikācijas statusu, kuru tas sniedz.

3.c Uzraudzības iestāde informē kvalificēto uzticamības pakalpojumu sniedzēju par to, ka viņa kvalifikācijas statuss vai attiecīgā pakalpojuma kvalifikācijas statuss ir anulēts. Uzraudzības iestāde informē saskaņā ar šīs regulas 22. panta 3. punktu paziņoto struktūru, lai atjauninātu minētā panta 1. punktā minētos uzticamības sarakstus, kā arī kompetento iestādi, kas izraudzīta vai izveidota, ievērojot Direktīvas (ES) 2022/2555 8. panta 1. punktu.

4. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šādos nolūkos:

a) atbilstības novērtēšanas struktūru akreditācijai un 1. punktā minētajam atbilstības novērtēšanas ziņojumam;

b) revīzijas prasībām, saskaņā ar kurām atbilstības novērtēšanas struktūras veic kvalificēto uzticamības pakalpojumu sniedzēju atbilstības novērtēšanu, tostarp salikto novērtēšanu, kā minēts 1. punktā;

c) atbilstības novērtēšanas shēmām, saskaņā ar kurām atbilstības novērtēšanas struktūras veic kvalificēto uzticamības pakalpojumu sniedzēju atbilstības novērtēšanu, un 1. punktā minētā ziņojuma sniegšanai.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

20) regulas 21. pantu groza šādi:

a) panta 1. un 2. punktu aizstāj ar šādu:

"1. Ja uzticamības pakalpojumu sniedzēji plāno sākt sniegt kādu kvalificētu uzticamības pakalpojumu, tie paziņo uzraudzības iestādei par savu nodomu kopā ar atbilstības novērtēšanas struktūras izdotu atbilstības novērtēšanas ziņojumu, kurā apstiprināta šajā regulā un Direktīvas (ES) 2022/2555 21. pantā noteikto prasību izpilde.

2. Uzraudzības iestāde verificē, vai uzticamības pakalpojumu sniedzējs un tā sniegtie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām un jo īpaši prasībām, kas noteiktas kvalificētiem uzticamības pakalpojumu sniedzējiem un to sniegtajiem kvalificētiem uzticamības pakalpojumiem.

Lai verificētu uzticamības pakalpojumu sniedzēja atbilstību Direktīvas (ES) 2022/2555 21. pantā noteiktajām prasībām, uzraudzības iestāde kompetentajām iestādēm, kas izraudzītas vai izveidotas, ievērojot minētās direktīvas 8. panta 1. punktu, pieprasa veikt uzraudzības darbības minētajā sakarā un sniegt informāciju par rezultātiem bez nepamatotas kavēšanās un jebkurā gadījumā divu mēnešu laikā pēc minētā pieprasījuma saņemšanas. Ja divu mēnešu laikā pēc paziņojuma saņemšanas verificēšana nav pabeigta, minētās kompetentās iestādes informē uzraudzības iestādi, norādot kavēšanās iemeslus un termiņu, līdz kuram verifikācija tiks pabeigta.

Ja uzraudzības iestāde secina, ka uzticamības pakalpojumu sniedzējs un tā sniegtie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām, uzraudzības iestāde vēlākais trīs mēnešus pēc paziņojuma saņemšanas saskaņā ar šā panta 1. punktu piešķir kvalifikācijas statusu uzticamības pakalpojumu sniedzējam un tā sniegtajiem uzticamības pakalpojumiem un informē 22. panta 3. punktā minēto struktūru, lai atjauninātu 22. panta 1. punktā minētos uzticamības sarakstus.

Ja trīs mēnešu laikā pēc paziņojuma saņemšanas verificēšana nav pabeigta, uzraudzības iestāde informē uzticamības pakalpojumu sniedzēju, norādot kavēšanās iemeslus un termiņu, līdz kuram verifikācija jāpabeidz.";

b) panta 4. punktu aizstāj ar šādu:

"4. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka paziņošanas un verifikācijas formātus un procedūras šā panta 1. un 2. punkta nolūkā. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

21) regulas 24. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Izdodot kvalificētu sertifikātu vai kvalificētu elektronisko atribūtu apliecinājumu, kvalificēts uzticamības pakalpojumu sniedzējs verificē tās fiziskās vai juridiskās personas identitāti, kurai paredzēts izdot kvalificēto sertifikātu vai kvalificēto elektronisko atribūtu apliecinājumu, un vajadzības gadījumā jebkādus īpašus šīs fiziskās vai juridiskās personas atribūtus.

1.a Šā panta 1. punktā minēto identitātes verifikāciju kvalificētais uzticamības pakalpojumu sniedzējs tieši vai ar trešās personas starpniecību veic ar piemērotiem līdzekļiem, pamatojoties uz vienu no turpmāk minētajām metodēm vai vajadzības gadījumā uz to kombināciju un saskaņā ar 1.c punktā minētajiem īstenošanas aktiem:

a) izmantojot Eiropas digitālās identitātes maku vai paziņotus elektroniskās identifikācijas līdzekļus, kas atbilst 8. pantā noteiktajām prasībām attiecībā uz uzticamības līmeni "augsts";

b) izmantojot kvalificēta elektroniskā paraksta sertifikātu vai kvalificētu elektronisko zīmogu, kas izdots atbilstīgi a), c) vai d) apakšpunktam;

c) izmantojot citas identifikācijas metodes, kuras nodrošina personas identifikāciju ar augstu ticamības līmeni un kuru atbilstību apstiprina atbilstības novērtēšanas struktūra;

d) fiziskās personas vai juridiskās personas pilnvarotā pārstāvja fiziskā klātbūtnē, izmantojot atbilstīgus pierādījumus un procedūras, saskaņā ar valstu tiesību aktiem.

1.b Panta 1. punktā daļā minēto atribūtu verifikāciju kvalificētais uzticamības pakalpojumu sniedzējs, tieši vai ar trešās personas starpniecību, veic ar piemērotiem līdzekļiem, pamatojoties uz vienu no turpmāk minētajām metodēm vai vajadzības gadījumā uz to kombināciju un saskaņā ar 1.c punktā minētajiem īstenošanas aktiem:

a) izmantojot Eiropas digitālās identitātes maku vai paziņotu elektroniskās identifikācijas līdzekli, kas atbilst 8. pantā noteiktajām prasībām attiecībā uz uzticamības līmeni "augsts";

b) izmantojot kvalificēta elektroniskā paraksta sertifikātu vai kvalificētu elektronisko zīmogu, kas izdoti saskaņā ar 1.a punkta a), c) vai d) apakšpunktu;

c) izmantojot kvalificētu atribūtu elektronisko apliecinājumu;

d) izmantojot citas metodes, kuras nodrošina atribūtu verifikāciju ar augstu ticamības līmeni un kuru atbilstību apstiprina atbilstības novērtēšanas struktūra;

e) fiziskās personas vai juridiskās personas pilnvarota pārstāvja fiziskā klātbūtnē, izmantojot atbilstīgus pierādījumus un procedūras, saskaņā ar valstu tiesību aktiem.

1.c Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras identitātes un atribūtu verifikācijai saskaņā ar šā panta 1., 1.a un 1. b punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

b) panta 2. punktu groza šādi:

i) panta a) apakšpunktu aizstāj ar šādu:

"a) informē uzraudzības iestādi vismaz vienu mēnesi pirms jebkādu izmaiņu ieviešanas savu kvalificēto uzticamības pakalpojumu sniegšanā vai vismaz trīs mēnešus pirms tam par nodomu pārtraukt minētās darbības;";

ii) punkta d) un e) apakšpunktu aizstāj ar šādiem:

"d) pirms iesaistīšanās līgumattiecībās skaidri, visaptveroši un viegli pieejamā veidā publiski pieejamā vietā un individuāli informē jebkuru personu, kura vēlas izmantot kādu kvalificētu uzticamības pakalpojumu, par precīziem minētā pakalpojuma izmantošanas noteikumiem, tostarp visiem tā izmantošanas ierobežojumiem;

e) izmanto uzticamas sistēmas un produktus, kas ir aizsargāti pret izmaiņām un nodrošina to atbalstīto procesu tehnisko drošību un uzticamību, tostarp izmantojot piemērotus kriptogrāfijas paņēmienus;";

iii) punktam pievieno šādus apakšpunktus:

"fa) neatkarīgi no Direktīvas (ES) 2022/2555 21. panta ir ieviesis attiecīgu politiku un veic atbilstošus pasākumus, ar ko pārvalda juridiskos, uzņēmējdarbības, operacionālos un citus tiešos vai netiešos riskus, kuri apdraud kvalificētā uzticamības pakalpojuma sniegšanu, tostarp vismaz pasākumus, kas saistīti ar:

i) pakalpojuma reģistrācijas un pievienošanas procedūrām;

ii) procesuālajām vai administratīvajām pārbaudēm;

iii) pakalpojumu pārvaldību un īstenošanu;

fb) paziņo uzraudzības iestādei, identificējamām skartajām personām, attiecīgā gadījumā citām attiecīgajām kompetentajām iestādēm un pēc uzraudzības iestādes pieprasījuma sabiedrībai, ja tas ir sabiedrības interesēs, par visiem tiem drošības pārkāpumiem vai traucējumiem pakalpojuma sniegšanā vai fa), i), ii) vai iii) punktā minēto pasākumu īstenošanā, kuri būtiski ietekmē sniegto uzticamības pakalpojumu vai tajā glabātos personas datus, un to dara bez nepamatotas kavēšanās un jebkurā gadījumā ne vēlāk kā 24 stundas pēc incidenta;";

iv) punkta g), h) un i) apakšpunktu aizstāj ar šādiem:

"g) veic piemērotus pasākumus pret datu viltošanu, zādzību vai piesavināšanos vai pret to, ka dati tiek dzēsti, mainīti vai darīti nepieejami bez attiecīgām tiesībām;

h) tik ilgi, cik nepieciešams pēc tam, kad kvalificētais uzticamības pakalpojumu sniedzējs ir izbeidzis darbību, reģistrē un nodrošina pieejamu visu attiecīgo informāciju par kvalificētā uzticamības pakalpojumu sniedzēja izdotajiem un saņemtajiem datiem, jo īpaši tādēļ, lai sniegtu pierādījumus tiesvedībā un lai nodrošinātu pakalpojuma nepārtrauktību. Šādu reģistrāciju var veikt elektroniski;

i) ir sagatavojuši aktuālu darbības pārtraukšanas plānu, lai nodrošinātu pakalpojumu nepārtrauktību atbilstoši noteikumiem, kurus verificējusi uzraudzības iestāde, ievērojot 46.b panta 4. punkta i) apakšpunktu;";

v) punkta j) apakšpunktu svītro;

vi) punktam pievieno šādu daļu:

"Uzraudzības iestāde var pieprasīt informāciju papildus informācijai, kas paziņota, ievērojot pirmās daļas a) apakšpunktu, vai atbilstības novērtējuma rezultātus un var izvirzīt nosacījumus atļaujas piešķiršanai, lai īstenotu paredzētās izmaiņas kvalificētajos uzticamības pakalpojumos. Ja trīs mēnešos no paziņojuma saņemšanas verificēšana nav pabeigta, uzraudzības iestāde informē uzticamības pakalpojumu sniedzēju, norādot kavēšanās iemeslus un termiņu, līdz kuram verifikācija tiks pabeigta.";

c) panta 5. punktu aizstāj ar šādu:

"4.a Šā panta 3. un 4. punktu attiecīgi piemēro kvalificētu atribūtu elektronisko apliecinājumu atsaukšanai.

4.b Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 47. pantu, ar kuriem nosaka šā panta 2. punkta fa) apakšpunktā minētos papildu pasākumus.

5. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šā panta 2. punktā noteiktajām prasībām. Uzskata, ka atbilstība šajā punktā noteiktajām prasībām ir panākta tad, ja ir izpildīti minētie standarti, specifikācijas un procedūras. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

22) regulas III nodaļas 3. iedaļā iekļauj šādu pantu:

"24.a pants

Kvalificētu uzticamības pakalpojumu atzīšana

1. Kvalificētus elektroniskos parakstus, kuru pamatā ir kvalificēts sertifikāts, kas izdots vienā dalībvalstī, un kvalificētus elektroniskos zīmogus, kuru pamatā ir kvalificēts sertifikāts, kas izdots vienā dalībvalstī, atzīst attiecīgi par kvalificētiem elektroniskajiem parakstiem un kvalificētiem elektroniskajiem zīmogiem visās pārējās dalībvalstīs.

2. Kvalificētas elektroniskā paraksta radīšanas ierīces un kvalificētas elektroniskā zīmoga radīšanas ierīces, kas sertificētas vienā dalībvalstī, atzīst attiecīgi par kvalificētām elektroniskā paraksta radīšanas ierīcēm un kvalificētām elektroniskā zīmoga radīšanas ierīcēm visās pārējās dalībvalstīs.

3. Kvalificētu elektronisko parakstu sertifikātu, kvalificētu elektronisko zīmogu sertifikātu, kvalificētu uzticamības pakalpojumu, kas paredzēts attālinātu kvalificētu elektroniskā paraksta radīšanas ierīču pārvaldībai, un kvalificētu uzticamības pakalpojumu, kas paredzēts attālinātu kvalificētu elektroniskā zīmoga radīšanas ierīču pārvaldībai, kurus nodrošina vienā dalībvalstī, atzīst attiecīgi par kvalificētu elektronisko parakstu sertifikātu, kvalificētu elektronisko zīmogu sertifikātu, kvalificētu uzticamības pakalpojumu, kas paredzēts attālinātu kvalificētu elektroniskā paraksta radīšanas ierīču pārvaldībai, un kvalificētu uzticamības pakalpojumu, kas paredzēts attālinātu kvalificētu elektroniskā zīmoga radīšanas ierīču pārvaldībai, visās pārējās dalībvalstīs.

4. Kvalificētu validācijas pakalpojumu, kas paredzēts kvalificētam elektroniskajam parakstam, un kvalificētu validācijas pakalpojumu, kas paredzēts kvalificētam elektroniskajam zīmogam, kurus sniedz vienā dalībvalstī, atzīst attiecīgi par kvalificētu validācijas pakalpojumu, kas paredzēts kvalificētam elektroniskajam parakstam, un par kvalificētu validācijas pakalpojumu kvalificētam elektroniskajam zīmogam, visās pārējās dalībvalstīs.

5. Kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumu un kvalificētu elektronisko zīmogu kvalificētas saglabāšanas pakalpojumu, ko sniedz vienā dalībvalstī, atzīst attiecīgi par kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumu un kvalificētu elektronisko zīmogu kvalificētas saglabāšanas pakalpojumu visās pārējās dalībvalstīs.

6. Kvalificētu elektronisko laika zīmogu, kas izsniegts vienā dalībvalstī, atzīst par kvalificētu elektronisko laika zīmogu visās pārējās dalībvalstīs.

7. Kvalificētu tīmekļa vietņu autentifikācijas sertifikātu, kas izdots vienā dalībvalstī, atzīst par kvalificētu tīmekļa vietņu autentifikācijas sertifikātu visās pārējās dalībvalstīs.

8. Kvalificētu elektroniski reģistrētu piegādes pakalpojumu, kas sniegts vienā dalībvalstī, atzīst par kvalificētu elektroniski reģistrētu piegādes pakalpojumu visās pārējās dalībvalstīs.

9. Kvalificētu atribūtu elektronisko apliecinājumu, kas izdots vienā dalībvalstī, atzīst par kvalificētu atribūtu elektronisko apliecinājumu visās pārējās dalībvalstīs.

10. Kvalificētu elektroniskās arhivēšanas pakalpojumu, kas sniegts vienā dalībvalstī, atzīst par kvalificētu elektroniskās arhivēšanas pakalpojumu visās pārējās dalībvalstīs.

11. Kvalificētu elektronisko virsgrāmatu, ko nodrošina vienā dalībvalstī, atzīst par kvalificētu elektronisko virsgrāmatu visās pārējās dalībvalstīs.";

23) regulas 25. panta 3. punktu svītro;

24) regulas 26. pantu groza šādi:

a) panta daļa kļūst par 1. punktu;

b) pantam pievieno šādu punktu:

"2. Līdz 2026. gada 21. maijam Komisija izvērtē vajadzību pieņemt īstenošanas aktus nolūkā noteikt atsauces standartu sarakstu un vajadzības gadījumā noteikt specifikācijas un procedūras uzlabotiem elektroniskajiem parakstiem. Pamatojoties uz minēto izvērtējumu, Komisija var pieņemt šādus īstenošanas aktus. Uzskata, ka atbilstība prasībām attiecībā uz uzlabotiem elektroniskajiem parakstiem ir panākta tad, ja uzlabotais elektroniskais paraksts atbilst minētajiem standartiem, specifikācijām un procedūrām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

25) regulas 27. panta 4. punktu svītro;

26) regulas 28. panta 6. punktu aizstāj ar šādu:

"6. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras kvalificētiem elektronisko parakstu sertifikātiem. Uzskata, ka atbilstība I pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā paraksta sertifikāts atbilst minētajiem standartiem, specifikācijām un procedūrām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

27) regulas 29. pantā iekļauj šādu punktu:

"1.a Elektroniskā paraksta radīšanas datu ģenerēšanu vai pārvaldību vai šādu paraksta radīšanas datu dublēšanu rezerves kopijas nolūkā veic tikai parakstītāja vārdā, pēc parakstītāja pieprasījuma un tikai kvalificēts uzticamības pakalpojumu sniedzējs, kas sniedz kvalificētu uzticamības pakalpojumu attālinātas kvalificētas elektroniskā paraksta radīšanas ierīces pārvaldībai.";

28) regulā iekļauj šādu pantu:

"29.a pants

Prasības kvalificētam pakalpojumam, ar ko pārvalda attālinātas kvalificētās elektroniskā paraksta radīšanas ierīces

1. Attālinātu kvalificēto elektroniskā paraksta radīšanas ierīču pārvaldību kā kvalificētu pakalpojumu sniedz tikai kvalificēts uzticamības pakalpojumu sniedzējs, kas:

a) parakstītāja vārdā ģenerē vai pārvalda elektroniskā paraksta radīšanas datus;

b) neatkarīgi no II pielikuma 1. punkta d) apakšpunkta elektroniskā paraksta radīšanas datus nokopē tikai rezerves kopijas vajadzībām ar noteikumu, ka ir izpildītas šādas prasības:

i) nokopēto datu kopu drošībai ir tāds pats līmenis, kādā ir oriģinālās datu kopas;

ii) nokopēto datu kopu skaits nedrīkst pārsniegt minimālo skaitu, kāds nepieciešams, lai nodrošinātu pakalpojumu nepārtrauktību;

c) atbilst visām prasībām, kuras noteiktas sertifikācijas ziņojumā par konkrēto attālināto kvalificēto elektroniskā paraksta radīšanas ierīci un kas izdots, ievērojot 30. pantu.

2. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā specifikācijas un procedūras šā panta 1. punkta vajadzībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

29) regulas 30. pantā iekļauj šādu punktu:

"3.a Šā panta 1. punktā minētās sertifikācijas derīgums nepārsniedz piecus gadus ar noteikumu, ka ievainojamības novērtējums tiek veikts reizi divos gados. Ja ievainojamības tiek konstatētas un netiek novērstas, sertifikāciju anulē.";

30) regulas 31. panta 3. punktu aizstāj ar šādu:

"3. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka formātus un procedūras šā panta 1. punkta vajadzībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

31) Regulas 32. pantu groza šādi:

a) panta 1. punktam pievieno šādu daļu:

"Uzskata, ka atbilstība šā punkta pirmajā daļā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu validācija atbilst 3. punktā minētajiem standartiem, specifikācijām un procedūrām.";

b) panta 3. punktu aizstāj ar šādu:

"3. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras kvalificētu elektronisko parakstu validācijai. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

32) regulā iekļauj šādu pantu:

"*32.a pants*

Prasības tādu uzlabotu elektronisko parakstu validēšanai, kuru pamatā ir kvalificēti sertifikāti

"1. Ar uzlabota elektroniskā paraksta validācijas procesu, kura pamatā ir kvalificēts sertifikāts, apstiprina uzlabota elektroniskā paraksta derīgumu ar noteikumu, ka:

a) sertifikāts, kas apliecina parakstu, parakstīšanas brīdī bija kvalificēts elektroniskā paraksta sertifikāts atbilstīgi I pielikumam;

b) kvalificēto sertifikātu izdevis kvalificēts uzticamības pakalpojumu sniedzējs, un tas parakstīšanas brīdī bija derīgs;

c) paraksta validācijas dati atbilst datiem, kurus sniedz atkarīgajai pusei;

d) unikālu datu kopums, kas apliecina sertifikātā minētā parakstītāja identitāti, ir pareizi nosūtīts atkarīgajai pusei;

e) ja parakstīšanas brīdī tika izmantots pseidonīms, tas ir skaidri norādīts atkarīgajai pusei;

f) parakstīto datu integritāte nav kompromitēta;

g) parakstīšanas brīdī bija izpildītas 26. pantā noteiktās prasības.

2. Ar sistēmu, ko izmanto tāda uzlabota elektroniskā paraksta validēšanai, kura pamatā ir kvalificēts sertifikāts, atkarīgajai pusei tiek sniegti precīzi validēšanas procesa rezultāti, ļaujot atkarīgajai pusei atklāt jebkādas ar drošību saistītas problēmas.

3. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras tādu uzlabotu elektronisko parakstu validācijai, kuru pamatā ir kvalificēti sertifikāti. Uzskata, ka atbilstība šā panta 1. punktā noteiktajām prasībām ir panākta tad, ja tādu uzlabotu elektronisko parakstu validācija, kuru pamatā ir kvalificēti sertifikāti, atbilst minētajiem standartiem, specifikācijām un procedūrām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

33) regulas 33. panta 2. punktu aizstāj ar šādu:"

"2. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šā panta 1. punktā minētajiem kvalificētajiem validēšanas pakalpojumiem. Uzskata, ka atbilstība šā panta 1. punktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu kvalificētie validēšanas pakalpojumi atbilst minētajiem standartiem, specifikācijām un procedūrām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

34) regulas 34. pantu groza šādi:

a) iekļauj šādu punktu:

"1.a Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumi atbilst 2. punktā minētajiem standartiem, specifikācijām un procedūrām.";

b) panta 2. punktu aizstāj ar šādu:

"2. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

35) regulas 35. panta 3. punktu svītro;

36) regulas 36. pantu groza šādi:

a) panta vienīgā daļa kļūst par 1. punktu;

b) pantam pievieno šādu punktu:

"2. Līdz 2026. gada 21. maijam Komisija izvērtē vajadzību pieņemt īstenošanas aktus nolūkā noteikt atsauces standartu sarakstu un vajadzības gadījumā noteikt specifikācijas un procedūras uzlabotiem elektroniskiem zīmogiem. Pamatojoties uz minēto izvērtējumu, Komisija var pieņemt šādus īstenošanas aktus. Uzskata, ka atbilstība prasībām attiecībā uz uzlabotiem elektroniskiem zīmogiem ir panākta tad, ja uzlabots elektroniskais zīmogs atbilst minētajiem standartiem, specifikācijām un procedūrām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

37) regulas 37. panta 4. punktu svītro;

38) regulas 38. panta 6. punktu aizstāj ar šādu:

"6. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras kvalificētiem elektronisko zīmogu sertifikātiem. Uzskata, ka atbilstība III pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā zīmoga sertifikāts atbilst minētajiem standartiem, specifikācijām un procedūrām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

39) regulā iekļauj šādu pantu:

"39.a pants

Prasības kvalificētam pakalpojumam, ar ko pārvalda attālinātas kvalificēta elektroniskā zīmoga radīšanas ierīces

Regulas 29.a pantu *mutatis mutandis* piemēro kvalificētam pakalpojumam, ko sniedz attālinātu kvalificēta elektroniskā zīmoga radīšanas ierīču pārvaldībai.";

40) regulas III nodaļas 5. iedaļā iekļauj šādu pantu:

"40.a pants

Prasības tādu uzlabotu elektronisko zīmogu validēšanai, kuru pamatā ir kvalificēti sertifikāti

Regulas 32.a pantu *mutatis mutandis* piemēro tādu uzlabotu elektronisko zīmogu validēšanai, kuru pamatā ir kvalificēti sertifikāti.";

41) regulas 41. panta 3. punktu svītro;

42) regulas 42. pantu groza šādi:

a) iekļauj šādu punktu:

"1.a Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja datuma un laika sasaiste ar datiem un laika avota precizitāte atbilst 2. punktā minētajiem standartiem, specifikācijām un procedūrām.";

b) panta 2. punktu aizstāj ar šādu:

"2. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras datuma un laika sasaistei ar datiem un laika avota precizitātes noteikšanai. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

43) regulas 44. pantu groza šādi:

a) iekļauj šādu punktu:

"1.a Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja datu nosūtīšanas un saņemšanas process atbilst 2. punktā minētajiem standartiem, specifikācijām un procedūrām.";

b) panta 2. punktu aizstāj ar šādu:

"2. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras datu nosūtīšanas un saņemšanas procesiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

c) pantā iekļauj šādus punktus:

"2.a Kvalificētu elektroniski reģistrētu piegādes pakalpojumu sniedzēji var vienoties par to kvalificēto elektroniski reģistrēto piegādes pakalpojumu sadarbspēju, kurus viņi sniedz. Šāda sadarbspējas sistēma atbilst 1. punktā noteiktajām prasībām, un šādu atbilstību apstiprina atbilstības novērtēšanas struktūra.

2.b Komisija var ar īstenošanas aktiem noteikt atsauces standartu sarakstu un vajadzības gadījumā noteikt specifikācijas un procedūras šā panta 2.a punktā minētajai sadarbspējas sistēmai. Tehniskās specifikācijas un standartu saturs ir izmaksu ziņā lietderīgi un samērīgi. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

44) regulas 45. pantu aizstāj ar šādu:

"45. pants

Prasības kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem

1. Kvalificēti tīmekļa vietņu autentifikācijas sertifikāti atbilst IV pielikumā noteiktajām prasībām. Atbilstību minētajām prasībām izvērtē saskaņā ar šā panta 2. punktā minētajiem standartiem, specifikācijām un procedūrām.

1.a Saskaņā ar šā panta 1. punktu izdotos kvalificētos tīmekļa vietņu autentifikācijas sertifikātus atpazīst tīmekļa pārlūkprogrammu nodrošinātāji. Tīmekļa pārlūkprogrammu nodrošinātāji nodrošina, ka sertifikātā apliecinātie identitātes dati un papildu apliecinātie atribūti tiek attēloti lietotājdraudzīgā veidā. Tīmekļa pārlūkprogrammu nodrošinātāji nodrošina atbalstu un sadarbspēju ar šā panta 1. punktā minētajiem kvalificētajiem tīmekļa vietņu autentifikācijas sertifikātiem, izņemot attiecībā uz Ieteikuma 2003/361/EK pielikuma 2. pantā definētajiem mikrouzņēmumiem un mazajiem uzņēmumiem pirmo piecu gadu laikā, kad tie darbojas kā tīmekļa pārlūkošanas pakalpojumu sniedzēji.

1.b Uz kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem neattiecas neviena cita obligātā prasība, kas nav noteikta 1. punktā.

2. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šā panta 1. punktā minētajiem kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

45) regulā iekļauj šādu pantu:

"45.a pants

Kiberdrošības piesardzības pasākumi

1. Tīmekļa pārlūkprogrammu nodrošinātāji neveic nekādus pasākumus, kas ir pretrunā pienākumiem, kas tām noteikti 45. pantā, jo īpaši prasībām atzīt kvalificētus tīmekļa vietņu autentifikācijas sertifikātus un lietotājdraudzīgā veidā attēlot sniegtos identitātes datus.

2. Atkāpjoties no 1. punkta un tikai tad, ja pastāv pamatotas bažas saistībā ar kāda identificēta sertifikāta vai sertifikātu kopuma drošības pārkāpumiem vai integritātes zudumu, tīmekļa pārlūkprogrammu nodrošinātāji var attiecībā uz minēto sertifikātu vai sertifikātu kopumu veikt piesardzības pasākumus.

3. Ja tīmekļa pārlūkprogrammas nodrošinātājs veic pasākumus, ievērojot 2. punktu, tīmekļa pārlūkprogrammas nodrošinātājs par savām bažām, pievienojot arī aprakstu par pasākumiem, kas veikti minēto bažu kliedēšanai, bez nepamatotas kavēšanās rakstiski paziņo Komisijai, kompetentajai uzraudzības iestādei, vienībai, kurai sertifikāts izdots, un kvalificētajam uzticamības pakalpojumu sniedzējam, kas izdevis minēto sertifikātu vai sertifikātu kopumu. Saņemot šādu paziņojumu, kompetentā uzraudzības iestāde attiecīgajam tīmekļa pārlūkprogrammas nodrošinātājam izdod apstiprinājumu par saņemšanu.

4. Kompetentā uzraudzības iestāde pārbauda paziņojumā izvirzītos jautājumus saskaņā ar 46.b panta 4. punkta k) apakšpunktu. Ja šīs izmeklēšanas rezultātā netiek anulēts sertifikāta kvalificētais statuss, uzraudzības iestāde attiecīgi informē tīmekļa pārlūkprogrammas nodrošinātāju un pieprasa minētajam nodrošinātājam izbeigt šā panta 2. punktā minētos piesardzības pasākumus.";

46) Direktīvas III nodaļā iekļauj šādas iedaļas:

"9. IEDAĻA

ATRIBŪTU ELEKTRONISKAIS APLIECINĀJUMS

45.b pants

Atribūtu elektroniskā apliecinājuma juridiskais spēks

1. Atribūtu elektroniskajam apliecinājumam neliedz juridisku spēku vai pieņemamību kā pierādījumam tiesvedībā tikai elektroniskā formāta dēļ vai tādēļ, ka tas neatbilst kvalificēta elektroniskā atribūtu apliecinājuma prasībām.

2. Kvalificētam elektroniskajam atribūtu apliecinājumam un atribūtu apliecinājumiem, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdoti tās vārdā, ir tāds pats juridiskais spēks kā likumīgi izdotiem apliecinājumiem papīra formātā.

3. Atribūtu apliecinājumu, ko izdevusi par autentisku avotu atbildīga publiska iestāde vienā dalībvalstī vai kas izdots tās vārdā, visās dalībvalstīs atzīst par atribūtu apliecinājumu, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā.

45.c pants

Atribūtu elektroniskais apliecinājums sabiedrisko pakalpojumu jomā

Ja saskaņā ar valstu tiesību aktiem ir vajadzīga elektroniska identifikācija, izmantojot elektroniskās identifikācijas līdzekļus un autentifikāciju, lai piekļūtu publiskas iestādes sniegtam tiešsaistes pakalpojumam, personas identifikācijas dati elektroniskajā atribūtu apliecinājumā neaizstāj elektronisko identifikāciju, izmantojot elektroniskās identifikācijas līdzekļus, un elektroniskās identifikācijas autentifikāciju, ja vien dalībvalsts to nav īpaši atļāvusi. Šādā gadījumā akceptē arī kvalificētus elektroniskos atribūtu apliecinājumus no citām dalībvalstīm.

45.d pants

Prasības kvalificētam elektroniskajam atribūtu apliecinājumam

1. Kvalificēts elektroniskais atribūtu apliecinājums atbilst V pielikumā noteiktajām prasībām.

2. Atbilstību V pielikumā noteiktajām prasībām izvērtē saskaņā ar šā panta 5. punktā minētajiem standartiem, specifikācijām un procedūrām.

3. Uz kvalificētiem elektroniskajiem atribūtu apliecinājumiem neattiecas nekādas obligātas prasības papildus V pielikumā noteiktajām prasībām.

4. Ja kvalificēts elektroniskais atribūtu apliecinājums pēc sākotnējās izdošanas ir atsaukts, tas vairs nav derīgs no tā atsaukšanas brīža un tā statusu nekādā gadījumā nevar atgriezt.

5. Līdz 2024. gada 21. novembrim Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras kvalificētiem elektroniskajiem atribūtu apliecinājumiem. Minētie īstenošanas akti ir saskanīgi ar 5.a panta 23. punktā minētajiem īstenošanas aktiem par Eiropas digitālās identitātes maka īstenošanu. Tos pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

45.e pants

Atribūtu verifikācija attiecībā pret autentiskiem avotiem

1. Dalībvalstis 24 mēnešu laikā pēc 5.a panta 23. punktā un 5.c panta 6. punktā minēto īstenošanas aktu stāšanās spēkā dienas nodrošina, ka vismaz attiecībā uz VI pielikumā norādītajiem atribūtiem – ja šie atribūti atkarīgi no autentiskiem avotiem publiskajā sektorā – tiek veikti pasākumi, kas ļauj kvalificētiem elektronisko atribūtu apliecinājumu uzticamības pakalpojumu sniedzējiem pēc lietotāja pieprasījuma ar elektroniskiem līdzekļiem verificēt minētos atribūtus, saskaņā ar Savienības vai valstu tiesību aktiem.

2. Līdz 2024. gada 21. novembrim Komisija, ņemot vērā attiecīgos starptautiskos standartus, ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras atribūtu katalogam, kā arī atribūtu apliecināšanas shēmas un kvalificētu atribūtu elektronisko apliecinājumu verifikācijas procedūras šā panta 1. punkta nolūkā. Minētie īstenošanas akti ir saskanīgi ar 5.a panta 23. punktā minēto īstenošanas aktu par Eiropas digitālās identitātes maka īstenošanu. Tos pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

45.f pants

Prasības elektroniskajam atribūtu apliecinājumam, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā

1. Elektroniskais atribūtu apliecinājums, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā, atbilst šādām prasībām:

a) VII pielikumā izklāstītajām prasībām;

b) kvalificētajam sertifikātam, kas apliecina tādas 3. panta 46. punktā minētās publiskās iestādes kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu, kura identificēta kā VII pielikuma b) punktā minētais izdevējs, ietverot konkrētu sertificētu atribūtu kopumu automatizētai apstrādei piemērotā veidā, un:

i) norādot, ka izdevējiestāde saskaņā ar Savienības vai valstu tiesību aktiem ir izveidota kā iestāde, kas ir atbildīga par autentisko avotu, uz kura pamata tiek izdots elektroniskais atribūtu apliecinājums, vai kā iestāde, kas izraudzīta rīkoties tās vārdā;

ii) sniedzot virkni datu, kas nepārprotami apliecina i) punktā minēto autentisko avotu; un

iii) norādot i) punktā minētos Savienības vai valsts tiesību aktus.

2. Dalībvalsts, kurā ir izveidotas 3. panta 46. punktā minētās publiskās iestādes, nodrošina, ka publiskās iestādes, kas izdod elektroniskos atribūtu apliecinājumus, atbilst uzticamības līmenim, kas ir līdzvērtīgs kvalificētu uzticamības pakalpojumu sniedzēju uzticamības līmenim saskaņā ar 24. pantu.

3. Dalībvalstis informē Komisiju par 3. panta 46. punktā minētajām publiskajām iestādēm. Minētajā paziņojumā iekļauj atbilstības novērtēšanas ziņojumu, ko izdevusi atbilstības novērtēšanas struktūra un kas apstiprina, ka ir izpildītas šā panta 1., 2. un 6. punktā noteiktās prasības. Izmantojot drošu kanālu, Komisija publisko 3. panta 46. punktā minēto publisko iestāžu sarakstu, kas ir elektroniski parakstīts vai apzīmogots un sagatavots automatizētai apstrādei piemērotā formātā.

4. Ja elektroniskais atribūtu apliecinājums, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā, ir atsaukts pēc sākotnējās izdošanas, tas zaudē derīgumu no tā atsaukšanas brīža un tā statusu neatjauno.

5. Elektronisko atribūtu apliecinājumu, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā, uzskata par atbilstīgu 1. punktā noteiktajām prasībām, ja tas atbilst 6. punktā minētajiem standartiem, specifikācijām un procedūrām.

6. Līdz 2024. gada 21. novembrim Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras elektroniskam atribūtu apliecinājumam, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā. Minētie īstenošanas akti ir saskanīgi ar 5.a panta 23. punktā minēto īstenošanas aktu par Eiropas digitālās identitātes maka īstenošanu. Tos pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

7. Līdz 2024. gada 21. novembrim Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas, formātus un procedūras šā panta 3. punkta vajadzībām. Minētie īstenošanas akti ir saskanīgi ar 5.a panta 23. punktā minētajiem īstenošanas aktiem par Eiropas digitālās identitātes maka īstenošanu. Tos pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

8. Regulas 3. panta 46. punktā minētās publiskās iestādes, kas izdod elektronisko atribūtu apliecinājumu, nodrošina saskarni ar Eiropas digitālās identitātes makiem, kas izdoti saskaņā ar 5.a pantu.

45.g pants

Atribūtu elektroniskā apliecinājuma izdošana Eiropas digitālās identitātes makiem

1. Atribūtu elektronisko apliecinājumu sniedzēji nodrošina Eiropas digitālās identitātes maka lietotājiem iespēju pieprasīt, iegūt, glabāt un pārvaldīt atribūtu elektronisko apliecinājumu neatkarīgi no tā, kurā dalībvalstī tiek nodrošināts Eiropas digitālās identitātes maks.

2. Atribūtu kvalificētu elektronisko apliecinājumu sniedzēji nodrošina saskarni ar Eiropas digitālās identitātes makiem, kas izdoti saskaņā ar 5.a pantu.

45.h pants

Papildu noteikumi atribūtu elektronisko apliecinājumu pakalpojumu sniegšanai

1. Atribūtu kvalificētu un nekvalificētu elektronisko apliecinājumu pakalpojumu sniedzēji personas datus, kas saistīti ar minēto pakalpojumu sniegšanu, neapvieno ar personas datiem no citiem to vai to komercpartneru piedāvātiem pakalpojumiem.

2. Personas datus, kas attiecas uz atribūtu elektroniskā apliecinājuma pakalpojumu sniegšanu, glabā loģiski nošķirti no citiem elektroniskā atribūtu apliecinājuma pakalpojumu sniedzēja glabātajiem datiem.

3. Kvalificētu elektronisko atribūtu apliecinājumu pakalpojumu sniedzēji šādu kvalificētu uzticamības pakalpojumu sniegšanu īsteno tā, lai tie būtu funkcionāli nodalīti no citiem to sniegtajiem pakalpojumiem.

10. IEDAĻA

ELEKTRONISKĀS ARHIVĒŠANAS PAKALPOJUMI

45.i pants

Elektroniskās arhivēšanas pakalpojumu juridiskais spēks

1. Elektroniskajiem datiem un elektroniskajiem dokumentiem, kas tiek saglabāti, izmantojot elektroniskās arhivēšanas pakalpojumu, nedrīkst liegt juridisku spēku vai pieņemamību kā pierādījumam tiesvedībā, un tos nevar noraidīt tikai elektroniskā formāta dēļ vai tādēļ, ka tie netiek saglabāti, izmantojot kvalificētu elektroniskās arhivēšanas pakalpojumu.

2. Uz elektroniskajiem datiem un elektroniskiem dokumentiem, kas tiek saglabāti, izmantojot elektroniskās arhivēšanas pakalpojumu, attiecas prezumpcija par to integritāti un to izcelsmi saglabāšanas periodā, kuru garantē kvalificēts uzticamības pakalpojumu sniedzējs.

45.j pants

Prasības kvalificētiem elektroniskās arhivēšanas pakalpojumiem

1. Kvalificēti elektroniskās arhivēšanas pakalpojumi atbilst šādām prasībām:

a) tos sniedz kvalificēti uzticamības pakalpojumu sniedzēji;

b) tajos izmanto procedūras un tehnoloģijas, kas spēj nodrošināt elektronisko datu un elektronisko dokumentu ilglaicīgumu un salasāmību pēc tehnoloģiskā derīguma termiņa beigām un vismaz visā juridiski vai līgumiski noteiktajā saglabāšanas periodā, vienlaikus saglabājot to integritāti un to izcelsmes precizitāti;

c) tie nodrošina, ka minētie elektroniskie dati un minētie elektroniskie dokumenti tiek saglabāti tā, lai tos pasargātu no pazaudēšanas un pārveidošanas, izņemot izmaiņas, kas attiecas uz to nesēju vai elektronisko formātu;

d) tie ļauj pilnvarotām atkarīgajām pusēm automatizēti saņemt ziņojumu, kas apstiprina, ka uz elektroniskajiem datiem un elektroniskajiem dokumentiem, kas izgūti no kvalificēta elektroniskā arhīva, no saglabāšanas perioda sākuma līdz to izguves brīdim attiecas datu integritātes prezumpcija.

Pirmās daļas d) apakšpunktā minēto ziņojumu sniedz uzticamā un efektīvā veidā, un uz tā ir kvalificētā elektroniskās arhivēšanas pakalpojuma sniedzēja kvalificēts elektroniskais paraksts vai kvalificēts elektroniskais zīmogs.

2. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras kvalificētiem elektroniskās arhivēšanas pakalpojumiem. Uzskata, ka atbilstība prasībām, kas noteiktas kvalificētiem elektroniskās arhivēšanas pakalpojumiem, ir panākta tad, ja kvalificēts elektroniskās arhivēšanas pakalpojums atbilst minētajiem standartiem, specifikācijām un procedūrām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.;

11. IEDAĻA

ELEKTRONISKĀS VIRSGRĀMATAS

45.k pants

Elektronisko virsgrāmatu juridiskais spēks

1. Elektroniskajai virsgrāmatai ir neapšaubāms juridiskais spēks vai tā ir pieņemama kā pierādījums tiesvedībā, un to nedrīkst noraidīt tikai elektroniskā formāta dēļ vai tādēļ, ka tā neatbilst prasībām, kas piemērojamas kvalificētām elektroniskajām virsgrāmatām.

2. Uz datu ierakstiem, kas iekļauti kvalificētā elektroniskajā virsgrāmatā, attiecas prezumpcija par to unikālo un precīzo secīgo hronoloģisko secību un to integritāti.

45.l pants

Prasības kvalificētām elektroniskajām virsgrāmatām

1. Kvalificētas elektroniskās virsgrāmatas atbilst šādām prasībām:

a) tās rada un pārvalda viens vai vairāki kvalificēti uzticamības pakalpojumu sniedzēji;

b) tās nosaka datu ierakstu izcelsmi virsgrāmatā;

c) tās datu ierakstiem nodrošina unikālu hronoloģisko secību virsgrāmatā;

d) tajās datus reģistrē tā, lai visas turpmākās datu izmaiņas būtu uzreiz nosakāmas, nodrošinot to integritāti laika gaitā.

2. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja elektroniskā virsgrāmata atbilst 3. punktā minētajiem standartiem, specifikācijām un procedūrām.

3. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka atsauces standartu sarakstu un vajadzības gadījumā nosaka specifikācijas un procedūras šā panta 1. punktā noteiktajām prasībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

47) regulā iekļauj šādu nodaļu:

"IVa NODAĻA

PĀRVALDĪBAS SATVARS

46.a pants

Eiropas digitālās identitātes maka satvara uzraudzība

1. Dalībvalstis izraugās vienu vai vairākas uzraudzības iestādes, kas iedibinātas to teritorijā.

Saskaņā ar pirmo daļu izraudzītajām uzraudzības iestādēm piešķir vajadzīgās pilnvaras un pienācīgus resursus, lai tās varētu efektīvi, lietderīgi un neatkarīgi pildīt savus uzdevumus.

2. Dalībvalstis paziņo Komisijai saskaņā ar 1. punktu izraudzīto uzraudzības iestāžu nosaukumus un adreses, kā arī visas turpmākās izmaiņas šajā informācijā. Komisija publicē paziņoto uzraudzības iestāžu sarakstu.

3. Saskaņā ar 1. punktu izraudzīto uzraudzības iestāžu loma ir šāda:

a) uzraudzīt Eiropas digitālās identitātes maku nodrošinātājus, kas veic uzņēmējdarbību izraudzīšanas dalībvalsts teritorijā, un, veicot *ex ante* un *ex post* uzraudzības darbības, nodrošināt, ka minētie nodrošinātāji un to izdotie Eiropas digitālās identitātes maki atbilst šajā regulā noteiktajām prasībām;

b) izmantojot *ex post* uzraudzības darbības, vajadzības gadījumā rīkoties attiecībā uz Eiropas digitālās identitātes maku nodrošinātājiem, kas iedibināti izraudzīšanas dalībvalsts teritorijā, kad tiek saņemta informācija, ka nodrošinātāji vai to izdotie Eiropas digitālās identitātes maki pārkāpj šo regulu.

4. Saskaņā ar 1. punktu izraudzīto uzraudzības iestāžu uzdevumi cita starpā jo īpaši ir šādi:

a) sadarboties ar citām uzraudzības iestādēm un sniegt tām palīdzību saskaņā ar 46.c un 46.e pantu;

b) pieprasīt informāciju, kas vajadzīga, lai pārraudzītu atbilstību šai regulai;

c) informēt attiecīgo dalībvalstu attiecīgās kompetentās iestādes, kas izraudzītas vai izveidotas saskaņā ar Direktīvas (ES) 2022/2555 8. panta 1. punktu, par jebkādiem būtiskiem drošības pārkāpumiem vai integritātes zudumu, kas tām kļuvuši zināmi, pildot savus uzdevumus, un tāda būtiska drošības pārkāpuma vai integritātes zuduma gadījumā, kas skar citas dalībvalstis, – informēt attiecīgās dalībvalsts vienoto kontaktpunktu, kas izraudzīts vai izveidots saskaņā ar Direktīvas (ES) 2022/2555 8. panta 3. punktu, un saskaņā ar šīs regulas 46.c panta 1. punktu izraudzītos vienotos kontaktpunktus citās attiecīgajās dalībvalstīs, un informēt sabiedrību vai pieprasīt to darīt Eiropas digitālās identitātes maka nodrošinātājam, ja uzraudzības iestāde konstatē, ka drošības pārkāpuma vai integritātes zuduma publiskošana būtu sabiedrības interesēs;

d) veikt pārbaudes uz vietas un uzraudzību neklātienē;

e) prasīt, lai Eiropas digitālās identitātes maku nodrošinātāji labotu jebkuru šajā regulā noteikto prasību neizpildi;

f) ja Eiropas digitālās identitātes maks tiek nelikumīgi vai krāpnieciski izmantots, – apturēt vai atcelt atkarīgo pušu reģistrāciju un iekļaušanu 5.b panta 7. punktā minētajā mehānismā;

g) sadarboties ar kompetentajām uzraudzības iestādēm, kas izveidotas, ievērojot Regulas (ES) 2016/679 51. pantu, jo īpaši, bez nepamatotas kavēšanās tās informējot, ja šķiet, ka ir notikuši personas datu aizsardzības noteikumu pārkāpumi, un par drošības pārkāpumiem, kas varētu būt personas datu aizsardzības pārkāpumi.

5. Ja saskaņā ar 1. punktu izraudzītā uzraudzības iestāde pieprasa Eiropas digitālās identitātes maka nodrošinātājam labot jebkuru šajā regulā noteikto prasību neizpildi, ievērojot 4. punkta e) apakšpunktu, un minētais nodrošinātājs attiecīgā gadījumā minētās uzraudzības iestādes noteiktā termiņā attiecīgi nerīkojas, saskaņā ar 1. punktu izraudzītā uzraudzības iestāde, ņemot vērā jo īpaši attiecīgās neizpildes apjomu, ilgumu un sekas, var uzdot nodrošinātājam apturēt vai pārtraukt Eiropas digitālās identitātes maka nodrošināšanu. Uzraudzības iestāde bez nepamatotas kavēšanās informē citu dalībvalstu uzraudzības iestādes, Komisiju, atkarīgās puses un Eiropas digitālās identitātes maka lietotājus par lēmumu pieprasīt apturēt vai pārtraukt Eiropas digitālās identitātes maka nodrošināšanu.

6. Katru gadu līdz 31. martam katra saskaņā ar 1. punktu izraudzītā uzraudzības iestāde iesniedz Komisijai pārskatu par galvenajām iepriekšējā kalendārajā gadā veiktajām darbībām. Komisija minētos gada ziņojumus dara pieejamus Eiropas Parlamentam un Padomei.

7. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka šā panta 6. punktā minētā ziņojuma formātus un procedūras. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

46.b pants

Uzticamības pakalpojumu uzraudzība

1. Dalībvalstis izraugās uzraudzības iestādi, kas iedibināta tās teritorijā, vai, pēc savstarpējas vienošanās ar citu dalībvalsti, izraugās uzraudzības iestādi, kas iedibināta minētajā citā dalībvalstī. Minētā uzraudzības iestāde ir atbildīga par uzraudzības uzdevumiem dalībvalstī, kas veic izraudzīšanu.

Saskaņā ar pirmo daļu izraudzītajām uzraudzības iestādēm piešķir vajadzīgās pilnvaras un pienācīgus resursus, lai tās varētu pildīt savus uzdevumus.

2. Dalībvalstis paziņo Komisijai savu attiecīgo saskaņā ar 1. punktu izraudzīto uzraudzības iestāžu nosaukumus un adreses, kā arī visas turpmākās izmaiņas šajā informācijā. Komisija publicē paziņoto uzraudzības iestāžu sarakstu.

3. Saskaņā ar 1. punktu izraudzīto uzraudzības iestāžu loma ir šāda:

a) uzraudzīt kvalificētus uzticamības pakalpojumu sniedzējus, kuri iedibināti izraudzīšanas dalībvalsts teritorijā, un nodrošināt, veicot *ex ante* un *ex post* uzraudzības darbības, ka minētie kvalificētie uzticamības pakalpojumu sniedzēji un to sniegtie kvalificētie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām;

b) izmantojot *ex post* uzraudzības darbības, vajadzības gadījumā rīkoties attiecībā uz nekvalificētiem uzticamības pakalpojumu sniedzējiem, kuri iedibināti izraudzīšanas dalībvalsts teritorijā, kad tiek saņemta informācija, ka minētie nekvalificētie uzticamības pakalpojumu sniedzēji vai to sniegtie uzticamības pakalpojumi, iespējams, neatbilst šajā regulā noteiktajām prasībām.

4. Saskaņā ar 1. punktu izraudzītās uzraudzības iestādes uzdevumi cita starpā jo īpaši ir šādi:

a) informēt attiecīgo dalībvalstu attiecīgās kompetentās iestādes, kas izraudzītas vai izveidotas saskaņā ar Direktīvas (ES) 2022/2555 8. panta 1. punktu, par jebkādiem būtiskiem drošības pārkāpumiem vai integritātes zudumu, kas tai kļuvuši zināmi, pildot savus uzdevumus, un būtiska drošības pārkāpuma vai integritātes zuduma gadījumā, kas skar citas dalībvalstis, informēt attiecīgās dalībvalsts vienoto kontaktpunktu, kas izraudzīts vai izveidots saskaņā ar Direktīvas (ES) 2022/2555 8. panta 3. punktu, un saskaņā ar šīs regulas 46.c panta 1. punktu izraudzītos vienotos kontaktpunktus citās attiecīgajās dalībvalstīs, un informēt sabiedrību vai pieprasīt to darīt uzticamības pakalpojumu sniedzējam, ja uzraudzības iestāde konstatē, ka drošības pārkāpuma vai integritātes zuduma publiskošana būtu sabiedrības interesēs;

b) sadarboties ar citām uzraudzības iestādēm un sniegt tām palīdzību saskaņā ar 46.c un 46.e pantu;

c) analizēt 20. panta 1. punktā un 21. panta 1. punktā minētos atbilstības novērtēšanas ziņojumus;

d) ziņot Komisijai par savām galvenajām darbībām saskaņā ar šā panta 6. punktu;

e) veikt revīzijas vai lūgt atbilstības novērtēšanas struktūrai veikt kvalificēto uzticamības pakalpojumu sniedzēju atbilstības novērtēšanu saskaņā ar 20. panta 2. punktu;

f) sadarboties ar kompetentajām uzraudzības iestādēm, kas izveidotas saskaņā ar Regulas (ES) 2016/679 51. pantu, jo īpaši, bez nepamatotas kavēšanās tās informējot, ja šķietami ir notikuši personas datu aizsardzības noteikumu pārkāpumi, un par drošības pārkāpumiem, kas varētu būt personas datu aizsardzības pārkāpumi;

g) piešķirt kvalifikācijas statusu uzticamības pakalpojumu sniedzējiem un to sniegtajiem pakalpojumiem un anulēt šo statusu saskaņā ar 20. un 21. pantu;

h) informēt struktūru, kas ir atbildīga par 22. panta 3. punktā minēto valstu uzticamības sarakstu, par lēmumiem piešķirt vai anulēt kvalificētā statusu, ja vien minētā struktūra nav arī uzraudzības iestāde, kas izraudzīta saskaņā ar šā panta 1. punktu;

i) verificēt darbības pārtraukšanas plānu esamību un pareizu piemērošanu, ja kvalificētais uzticamības pakalpojumu sniedzējs pārtrauc savas darbības, tostarp attiecībā uz to, kā tiek saglabāta informācijas pieejamība saskaņā ar 24. panta 2. punkta h) apakšpunktu;

j) prasīt, lai uzticamības pakalpojumu sniedzēji labotu jebkuru šajā regulā noteikto prasību neizpildi;

k) izmeklēt tīmekļa pārlūkprogrammu nodrošinātāju prasījumus, ievērojot 45.a pantu, un vajadzības gadījumā rīkoties.

5. Dalībvalstis var prasīt saskaņā ar 1. punktu izraudzītajai uzraudzības iestādei izveidot, uzturēt un atjaunināt uzticamības infrastruktūru saskaņā ar valstu tiesību aktiem.

6. Katru gadu līdz 31. martam katra saskaņā ar 1. punktu izraudzītā uzraudzības iestāde iesniedz Komisijai pārskatu par galvenajām iepriekšējā kalendārajā gadā veiktajām darbībām. Komisija minētos gada ziņojumus dara pieejamus Eiropas Parlamentam un Padomei.

7. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem pieņem pamatnostādnes par to, kā saskaņā ar šā panta 1. punktu izraudzītās uzraudzības iestādes veic šā panta 4. punktā minētos uzdevumus, un ar īstenošanas aktiem nosaka šā panta 6. punktā minētā ziņojuma formātus un procedūras. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

46.c pants

Vienotie kontaktpunkti

1. Katra dalībvalsts izraugās vienotu kontaktpunktu uzticamības pakalpojumiem, Eiropas digitālās identitātes makiem un paziņotajām elektroniskās identifikācijas shēmām.

2. Katrs vienotais kontaktpunkts pilda koordinācijas funkciju, lai veicinātu pārrobežu sadarbību starp uzticamības pakalpojumu sniedzēju uzraudzības iestādēm un starp Eiropas digitālās identitātes maku nodrošinātāju uzraudzības iestādēm un attiecīgā gadījumā ar Komisiju un Eiropas Savienības Kiberdrošības aģentūru (*ENISA*) un citām kompetentajām iestādēm savā dalībvalstī.

3. Katra dalībvalsts publisko un bez nepamatotas kavēšanās paziņo Komisijai saskaņā ar 1. punktu izraudzīto vienoto kontaktpunktu nosaukumus un adreses, kā arī visas turpmākās izmaiņas šajā informācijā.

4. Komisija publicē saskaņā ar 3. punktu paziņoto vienoto kontaktpunktu sarakstu.

46.d pants

Savstarpēja palīdzība

1. Lai atvieglotu šajā regulā noteikto pienākumu uzraudzību un izpildi, saskaņā ar 46.a panta 1. punktu un 46. b panta 1. punktu izraudzītās uzraudzības iestādes, tostarp ar Sadarbības grupas starpniecību, kas izveidota saskaņā ar 46.e panta 1. punktu, var lūgt savstarpēju palīdzību no tās citas dalībvalsts uzraudzības iestādēm, kurā Eiropas digitālās identitātes maka nodrošinātājs vai uzticamības pakalpojumu sniedzējs ir iedibināts vai kurā atrodas tā tīkls un informācijas sistēmas vai tiek sniegti tā pakalpojumi.

2. Savstarpējā palīdzība nozīmē, ka vismaz notiek šādas darbības:

a) uzraudzības iestāde, kas piemēro uzraudzības un izpildes pasākumus vienā dalībvalstī, informē citas attiecīgās dalībvalsts uzraudzības iestādi un apspriežas ar to;

b) uzraudzības iestāde var pieprasīt citas attiecīgās dalībvalsts uzraudzības iestādei veikt uzraudzības vai izpildes pasākumus, tostarp, piemēram, pieprasījumus veikt ar 20. un 21. pantā minētajiem atbilstības novērtēšanas ziņojumiem saistītas pārbaudes attiecībā uz uzticamības pakalpojumu sniegšanu;

c) attiecīgā gadījumā uzraudzības iestādes var kopā ar citu dalībvalstu uzraudzības iestādēm veikt kopīgu izmeklēšanu.

Attiecīgās dalībvalstis saskaņā ar saviem valstu tiesību aktiem vienojas par saskaņā ar šā panta pirmo daļu veikto kopīgo rīcību kārtību un procedūrām un izstrādā tās.

3. Uzraudzības iestāde, kurai ir lūgta palīdzība, var noraidīt minēto pieprasījumu, pamatojoties uz jebkuru no šādiem iemesliem:

a) lūgtā palīdzība nav samērīga ar uzraudzības iestādes uzraudzības darbībām, kas veiktas saskaņā ar 46.a un 46. b pantu;

b) uzraudzības iestāde nav kompetenta sniegt minēto palīdzību;

c) lūgtās palīdzības sniegšana būtu pretrunā šīs regulas noteikumiem.

4. Līdz 2025. gada 21. maijam un pēc tam reizi divos gados Sadarbības grupa, kas izveidota saskaņā ar 46.e panta 1. punktu, izdod norādījumus par šā panta 1. un 2. punktā minētās savstarpējās palīdzības organizatoriskajiem aspektiem un procedūrām.

46.e pants

Eiropas Digitālās identitātes sadarbības grupa

1. Lai atbalstītu un atvieglotu dalībvalstu pārrobežu sadarbību un informācijas apmaiņu par uzticamības pakalpojumiem, Eiropas digitālās identitātes makiem un paziņotajām elektroniskās identifikācijas shēmām, Komisija izveido Eiropas Digitālās identitātes sadarbības grupu ("Sadarbības grupa").

2. Sadarbības grupas sastāvā ir dalībvalstu iecelti pārstāvji un Komisijas pārstāvji. Sadarbības grupu vada Komisija. Komisija nodrošina Sadarbības grupas sekretariātu.

3. Attiecīgo ieinteresēto personu pārstāvjus uz *ad hoc* pamata var uzaicināt apmeklēt sadarbības grupas sanāksmes un piedalīties tās darbā kā novērotājus.

4. Ja Sadarbības grupā apmainās ar viedokļiem, paraugpraksi un informāciju par attiecīgiem kiberdrošības aspektiem, piemēram, pievēršas paziņojumiem par drošības pārkāpumiem un ja risina jautājumus saistībā ar kiberdrošības sertifikātu vai standartu izmantošanu, Sadarbības grupas darbā novērotājas statusā uzaicina piedalīties *ENISA*.

5. Sadarbības grupai ir šādi uzdevumi:

a) apmainīties ar padomiem un sadarboties ar Komisiju attiecībā uz jaunām politikas iniciatīvām digitālās identitātes maku, elektroniskās identifikācijas līdzekļu un uzticamības pakalpojumu jomā;

b) attiecīgā gadījumā konsultēt Komisiju sākotnējā tādu īstenošanas un deleģēto aktu projektu sagatavošanas stadijā, kurus paredzēts pieņemt, ievērojot šo regulu;

c) lai atbalstītu uzraudzības iestādes šīs regulas noteikumu īstenošanā:

   i) apmainīties ar paraugpraksi un informāciju attiecībā uz šīs regulas noteikumu īstenošanu;

   ii) novērtēt attiecīgās norises digitālās identitātes maka, elektroniskās identifikācijas un uzticamības pakalpojumu jomās;

   iii) organizēt kopīgas sanāksmes ar attiecīgajām ieinteresētajām personām no visas Savienības, lai apspriestu Sadarbības grupas veiktās darbības un apkopotu sniegto informāciju par jaunām politikas problēmām;

   iv) ar *ENISA* atbalstu apmainīties ar viedokļiem, paraugpraksi un informāciju par attiecīgiem kiberdrošības aspektiem, kas attiecas uz Eiropas digitālās identitātes makiem, elektroniskās identifikācijas shēmām un uzticamības pakalpojumiem;

   v) apmainīties ar paraugpraksi attiecībā uz drošības pārkāpumu paziņošanas politikas izstrādi un īstenošanu un kopīgiem pasākumiem, kā minēts 5.e un 10. pantā;

   vi) organizēt kopīgas sanāksmes ar TID sadarbības grupu, kas izveidota, ievērojot Direktīvas (ES) 2022/2555 14. panta 1. punktu, lai apmainītos ar attiecīgu informāciju par uzticamības pakalpojumiem un elektronisko identifikāciju saistībā ar kiberdraudiem, incidentiem, ievainojamībām, izpratnes veicināšanas iniciatīvām, apmācību, vingrinājumiem un prasmēm, spēju veidošanu, spējām standartu un tehnisko specifikāciju jomā, kā arī standartiem un tehniskajām specifikācijām;

   vii) pēc uzraudzības iestādes pieprasījuma apspriest konkrētus savstarpējas palīdzības lūgumus, kā minēts 46. d pantā;

   viii) veicināt informācijas apmaiņu starp uzraudzības iestādēm, sniedzot norādījumus par 46.d pantā minētās savstarpējās palīdzības organizatoriskajiem aspektiem un procedūrām;

d) organizēt to elektroniskās identifikācijas shēmu salīdzinošo izvērtēšanu, kuras jāpaziņo saskaņā ar šo regulu.

6. Dalībvalstis nodrošina efektīvu un lietderīgu savu izraudzīto pārstāvju sadarbību Sadarbības grupā.

7. Līdz 2025. gada 21. maijam Komisija ar īstenošanas aktiem nosaka vajadzīgo procesuālo kārtību, lai veicinātu šā panta 5. punkta d) apakšpunktā minēto dalībvalstu sadarbību. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.";

48) regulas 47. pantu groza šādi:

a) panta 2. un 3. punktu aizstāj ar šādiem:

"2. Pilnvaras pieņemt 5.c panta 7. punktā, 24. panta 4.b punktā un 30. panta 4. punktā minētos deleģētos aktus Komisijai piešķir uz nenoteiktu laiku no 2014. gada 17. septembra.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 5.c panta 7. punktā, 24. panta 4.b punktā un 30. panta 4. 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 esošos deleģētos aktus.";

b) panta 5. punktu aizstāj ar šādu:

"5. Saskaņā ar 5.c panta 7. punktu, 24. panta 4.b punktu vai 30. panta 4. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešu laikposmā 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 minēto laikposmu pagarina par diviem mēnešiem.";

49) regulas VI nodaļā iekļauj šādu pantu:

"48.a pants

Ziņojumu sniegšanas prasības

1. Dalībvalstis nodrošina statistikas datu vākšanu saistībā ar to teritorijā nodrošināto Eiropas digitālās identitātes maku darbību un kvalificēto uzticamības pakalpojumu sniegšanu.

2. Statistikas datos, kas tiek vākti saskaņā ar 1. punktu, ir ietverti šādi elementi:

a) to fizisko un juridisko personu skaits, kurām ir derīgs Eiropas digitālās identitātes maks;

b) to pakalpojumu veids un skaits, kuros tiek akceptēta Eiropas digitālās identitātes maka izmantošana;

c) ar atkarīgajām pusēm un kvalificētiem uzticamības pakalpojumiem saistīto lietotāju sūdzību un patērētāju aizsardzības vai datu aizsardzības incidentu skaits;

d) kopsavilkuma ziņojums, kurā iekļauti dati par incidentiem, kas kavē Eiropas digitālās identitātes maka izmantošanu;

e) kopsavilkums par būtiskiem drošības incidentiem, datu aizsardzības pārkāpumiem un skartajiem Eiropas digitālās identitātes maku vai kvalificētu uzticamības pakalpojumu lietotājiem.

3. Šā panta 2. punktā minētos statistikas datus dara publiski pieejamus atklātā un plaši izmantotā mašīnlasāmā formātā.

4. Katru gadu līdz 31. martam dalībvalstis iesniedz Komisijai ziņojumu par statistikas datiem, kas savākti saskaņā ar 2. punktu.";

50) regulas 49. pantu aizstāj ar šādu:

"49. pants

Pārskatīšana

1. Komisija pārskata šīs regulas piemērošanu un sniedz ziņojumu Eiropas Parlamentam un Padomei līdz 2026. gada 21. maijam. Minētajā ziņojumā Komisija jo īpaši izvērtē, vai ir lietderīgi grozīt šīs regulas darbības jomu vai konkrētus tās noteikumus, tostarp jo īpaši 5.c panta 5. punktā iekļautos noteikumus, ņemot vērā šīs regulas piemērošanā gūto pieredzi, kā arī norises tehnoloģiju, tirgus un tiesiskajā jomā. Vajadzības gadījumā minētajam ziņojumam pievieno priekšlikumu grozīt šo regulu.

2. Šā panta 1. punktā minētajā ziņojumā iekļauj novērtējumu par šīs regulas darbības jomas aptverto paziņoto elektroniskās identifikācijas līdzekļu un Eiropas digitālās identitātes maku, pieejamību, drošību un izmantojamību un novērtē, vai visiem privātiem tiešsaistes pakalpojumu sniedzējiem, kas lietotāju autentifikācijai izmanto trešo personu elektroniskās identifikācijas pakalpojumus, prasa akceptēt paziņoto elektroniskās identifikācijas līdzekļu un Eiropas digitālās identitātes maka izmantošanu.

3. Komisija līdz 2030. gada 21. maijam un pēc tam reizi četros gados iesniedz ziņojumu Eiropas Parlamentam un Padomei par panākumiem šīs regulas mērķu īstenošanā.";

51) regulas 51. pantu aizstāj ar šādu:

"51. pants

Pārejas pasākumi

1. Drošas paraksta radīšanas ierīces, kuru atbilstība ir noteikta saskaņā ar Direktīvas 1999/93/EK 3. panta 4. punktu, līdz 2027. gada 21. maijam turpina uzskatīt par kvalificētām elektroniskā paraksta radīšanas ierīcēm saskaņā ar šo regulu.

2. Kvalificētus sertifikātus, kas fiziskām personām izdoti saskaņā ar Direktīvu 1999/93/EK, līdz 2026. gada 21. maijam, turpina uzskatīt par kvalificētiem elektroniskā paraksta sertifikātiem saskaņā ar šo regulu.

3. Attālinātu kvalificēta elektroniskā paraksta un zīmoga radīšanas ierīču pārvaldību, kuru veic kvalificēti uzticamības pakalpojumu sniedzēji, kas nav kvalificēti uzticamības pakalpojumu sniedzēji, kuri sniedz kvalificētus uzticamības pakalpojumus attālinātu kvalificēta elektroniskā paraksta un zīmoga radīšanas ierīču pārvaldībai saskaņā ar 29.a un 39.a pantu var veikt bez nepieciešamības iegūt kvalifikācijas statusu šo pārvaldības pakalpojumu sniegšanai, līdz 2026. gada 21. maijam.

4. Kvalificēti uzticamības pakalpojumu sniedzēji, kuriem saskaņā ar šo regulu pirms 2024. gada 20. maija ir piešķirts kvalifikācijas statuss, cik vien iespējams drīz, bet jebkurā gadījumā līdz 2026. gada 21. maijam iesniedz uzraudzības iestādei atbilstības novērtēšanas ziņojumu, kas apliecina atbilstību 24. panta 1. punktam, 1.a punktam un 1.b punktam.";

52) regulas I–IV pielikumu attiecīgi groza saskaņā ar šīs regulas I–IV pielikumu;

53) pievieno jaunu V, VI un VII pielikumu, kā noteikts šīs regulas V, VI un VII pielikumā.

2. 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, 2024. gada 11. aprīlī

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētāja	*priekšsēdētāja*
R. METSOLA	H. LAHBIB

I PIELIKUMS

Regulas (ES) Nr. 910/2014 I pielikuma i) punktu aizstāj ar šādu:

“i) informāciju par pakalpojumiem, kurus var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu, vai vietu, kur šie pakalpojumi pieejami;”.

II PIELIKUMS

Regulas (ES) Nr. 910/2014 II pielikuma 3. un 4. punktu svītro.

III PIELIKUMS

Regulas (ES) Nr. 910/2014 III pielikuma i) punktu aizstāj ar šādu:

"i) informāciju par pakalpojumiem, kurus var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu, vai vietu, kur šie pakalpojumi pieejami;".

IV PIELIKUMS

Regulas (ES) Nr. 910/2014 IV pielikumu groza šādi:

1) pielikuma c) apakšpunktu aizstāj ar šādu:

"c) fiziskām personām – vismaz tās personas vārdu, kurai sertifikāts ir izdots, vai pseidonīmu; ja tiek izmantots pseidonīms, to skaidri norāda;

ca) juridiskām personām – unikālu datu kopumu, kas nepārprotami apliecina juridisko personu, kurai sertifikāts ir izdots, norādot vismaz tās juridiskās personas nosaukumu, kurai sertifikāts ir izdots, un attiecīgā gadījumā – oficiālajos reģistros norādīto reģistrācijas numuru;";

2) pielikuma j) apakšpunktu aizstāj ar šādu tekstu:

"j) informāciju par sertifikāta derīguma statusa pakalpojumiem, kurus var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu, vai vietu, kur šie pakalpojumi pieejami;".

V PIELIKUMS

"V PIELIKUMS

PRASĪBAS KVALIFICĒTAM ELEKTRONISKAJAM ATRIBŪTU APLIECINĀJUMAM

Kvalificētā elektroniskajā atribūtu apliecinājumā ir šāda informācija:

a) norāde, kas ir vismaz automatizētai apstrādei piemērotā formā, par to, ka apliecinājums ir izdots kā kvalificēts elektroniskais atribūtu apliecinājums;

b) datu kopums, kas nepārprotami apliecina tā kvalificētā uzticamības pakalpojumu sniedzēja identitāti, kurš izdod kvalificēto elektronisko atribūtu apliecinājumu, tostarp vismaz informācija par dalībvalsti, kurā pakalpojumu sniedzējs veic uzņēmējdarbību, un:

   i) attiecībā uz juridisku personu – nosaukums un attiecīgā gadījumā reģistrācijas numurs, kas norādīts oficiālajos reģistros;

   ii) attiecībā uz fiziskai personu – personas vārds un uzvārds;

c) datu kopums, kas nepārprotami apliecina subjektu, uz kuru attiecas apliecinātie atribūti; ja tiek izmantots pseidonīms, to skaidri norāda;

d) apliecinātais atribūts vai apliecinātie atribūti, tostarp attiecīgā gadījumā informācija, kas vajadzīga minēto atribūtu tvēruma noteikšanai;

e) precīza informācija par apliecinājuma derīguma termiņa sākumu un beigām;

f) apliecinājuma identifikācijas kods, kam attiecībā uz kvalificētu uzticamības pakalpojumu sniedzēju ir jābūt unikālam, un attiecīgā gadījumā norāde par apliecinājumu shēmu, kuras daļa ir atribūtu apliecinājums;

g) apliecinājuma izdevēja, proti, kvalificētā uzticamības pakalpojumu sniedzēja kvalificētais elektroniskais paraksts vai kvalificētais elektroniskais zīmogs;

h) vieta, kur bez maksas ir pieejams sertifikāts, kas apliecina g) punktā minēto kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu;

i) informācija par pakalpojumiem, kurus var izmantot, lai noskaidrotu kvalificētā apliecinājuma derīguma statusu, vai vieta, kur šie pakalpojumi pieejami."

VI PIELIKUMS

"VI PIELIKUMS

OBLIGĀTO ATRIBŪTU SARAKSTS

Ievērojot 45.e pantu, dalībvalstis nodrošina, ka tiek veikti pasākumi, kas saskaņā ar Savienības vai valsts tiesību aktiem un gadījumos, kad atribūti ir atkarīgi no autentiskiem avotiem publiskajā sektorā, atribūtu elektronisko apliecinājumu kvalificētiem uzticamības pakalpojumu sniedzējiem dod iespēju pēc lietotāja pieprasījuma ar elektroniskiem līdzekļiem, atribūtus salīdzinot ar attiecīgo autentisko avotu valsts līmenī vai izmantojot tādu izraudzītu starpnieku palīdzību, kas atzīti valsts līmenī, verificēt turpmāk norādīto atribūtu autentiskumu:

1. Adrese.
2. Vecums.
3. Dzimums.
4. Ģimenes stāvoklis.
5. Ģimenes sastāvs.
6. Valstspiederība vai pilsonība.
7. Izglītības kvalifikācija, nosaukumi un apliecības.
8. Profesionālā kvalifikācija, nosaukumi un apliecības.
9. Pilnvaras un pilnvarojumi pārstāvēt fiziskas vai juridiskas personas.
10. Publiskās atļaujas un licences.
11. Juridiskām personām – finansiālie un uzņēmumu dati."

VII PIELIKUMS

"VII PIELIKUMS

PRASĪBAS ELEKTRONISKAJAM ATRIBŪTU APLIECINĀJUMAM, KO IZDEVUSI PAR AUTENTISKU AVOTU ATBILDĪGA PUBLISKA IESTĀDE VAI KAS IZDOTS TĀS VĀRDĀ

Elektroniskajā atribūtu apliecinājumā, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā, ir šāda informācija:

a) norāde, kas ir vismaz automatizētai apstrādei piemērotā formā, par to, ka apliecinājums ir izdots kā elektroniskais atribūtu apliecinājums, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā;

b) datu kopums, kas nepārprotami apliecina publisko iestādi, kura izdod atribūtu elektronisko apliecinājumu, tostarp vismaz dalībvalsts, kurā minētā publiskā iestāde ir izveidota, un tās nosaukums un attiecīgā gadījumā tās reģistrācijas numurs, kas norādīts oficiālajos reģistros;

c) datu kopums, kas nepārprotami apliecina subjektu, uz kuru attiecas apliecinātie atribūti; ja izmanto pseidonīmu, to skaidri norāda;

d) apliecinātais atribūts vai apliecinātie atribūti, tostarp attiecīgā gadījumā informācija, kas vajadzīga minēto atribūtu tvēruma noteikšanai;

e) precīza informācija par apliecinājuma derīguma termiņa sākumu un beigām;

f) apliecinājuma identifikācijas kods, kam attiecībā uz publisko izdevējiestādi ir jābūt unikālam, un attiecīgā gadījumā norāde par apliecinājumu shēmu, kuras daļa ir attiecīgais atribūtu apliecinājums;

g) izdevējiestādes kvalificētais elektroniskais parakstu vai kvalificētais elektroniskais zīmogs;

h) vieta, kur bez maksas ir pieejams sertifikāts, kas apliecina g) punktā minēto kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu;

i) informācija par pakalpojumiem, kurus var izmantot, lai noskaidrotu apliecinājuma derīguma statusu, vai vieta, kur šie pakalpojumi pieejami."