Eiropas Savienības
Padome

Briselē, 2022. gada 25. novembrī
(OR. en)

14959/22

Starpiestāžu lieta:
2021/0136(COD)

LIMITE

TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774

PIEZĪME

Sūtītājs:	Pastāvīgo pārstāvju komiteja (I)
Saņēmējs:	Padome
Iepr. dok. Nr.:	14344/22
K-jas dok. Nr.:	9471/21
Temats:	Priekšlikums – Eiropas Parlamenta un Padomes Regula, ar ko Regulu (ES) Nr. 910/2014 groza attiecībā uz Eiropas digitālās identitātes regulējuma izveidi – vispārēja pieeja

I. IEVADS

1. Komisija priekšlikumu Regulai par Eiropas digitālo identitāti **(Eiropas *eID*)** pieņēma 2021. gada 3. jūnijā [1]. Ar šo iniciatīvu groza 2014. gada *eIDAS* regulu [2], kas bija radījusi nepieciešamo pamatu drošai piekļuvei pakalpojumiem un darījumu veikšanai tiešsaistē un pāri robežām Eiropas Savienībā.

[1] Dok. 9471/21.
[2] Regula (ES) Nr. 910/2014.

2. Priekšlikums, kura pamatā ir LESD 114. pants, paredz, ka dalībvalstīm pēc obligāta atbilstības novērtējuma ir jāizdod Eiropas digitālās identitātes maks saskaņā ar paziņotu *eID* shēmu, kā pamatā ir kopīgi tehniski standarti. Lai izveidotu vajadzīgo tehnisko arhitektūru, paātrinātu pārskatītās regulas īstenošanu, sniegtu pamatnostādnes dalībvalstīm un nepieļautu sadrumstalotību, priekšlikumam bija pievienots ieteikums par Savienības rīkkopas izstrādi.

3. Ierosinātās regulas mērķis ir nodrošināt iedzīvotājiem un uzņēmumiem vispārēju piekļuvi drošai un uzticamai elektroniskai identifikācijai un autentifikācijai, izmantojot personīgu digitālo maku mobilajā tālrunī.

II. DARBS CITĀS IESTĀDĒS

1. Eiropas Parlamentā priekšlikums tika nodots Rūpniecības, pētniecības un enerģētikas komitejai (ITRE) un trim iesaistītajām komitejām atzinumu sniegšanai, proti, Iekšējā tirgus un patērētāju aizsardzības komitejai (IMCO), Juridiskajai komitejai (JURI) un Pilsoņu brīvību, tieslietu un iekšlietu komitejai (LIBE). Šā dosjē referente ir *Romana Jerković* (*S&D*, Horvātija). ITRE komiteja ziņojumu vēl nav pieņēmusi.

2. Eiropas Ekonomikas un sociālo lietu komitejai 2021. gada 15. jūlijā lūdza sniegt atzinumu par priekšlikumu; atzinums tika sniegts 2021. gada 20. oktobrī. 2021. gada 12. oktobrī ar atzinumu par priekšlikumu pēc savas iniciatīvas nāca klajā Eiropas Reģionu komiteja.

3. Eiropas Datu aizsardzības uzraudzītājs (EDAU) 2021. gada 28. jūlijā sniedza oficiālus komentārus par priekšlikumu.

III. PADOMĒ PAVEIKTAIS

1. Padomē priekšlikumu izskatīja Telesakaru un informācijas sabiedrības jautājumu darba grupā (turpmāk – *TELECOM* darba grupa), kas to sāka apspriest Portugāles prezidentūras laikā 2021. gada jūnijā. Analīze turpinājās *TELECOM* darba grupā Slovēnijas prezidentūras laikā, un pirmais lasījums veiksmīgi noslēdzās 2021. gada 15. novembrī.

2. Prezidentvalsts Francija ar **pirmo kompromisa priekšlikumu** iepazīstināja 15. februārī un 5. aprīlī, un **otrais** tika apspriests 23. maijā un 9. jūnijā. Saistībā ar politikas debatēm, kas 2022. gada 19. jūlijā notika *TELECOM* darba grupā, prezidentvalsts Čehija, balstoties uz prezidentvalsts Francijas darbu, izcēla galvenos neatrisinātos augsta līmeņa jautājumus un aicināja delegācijas paust vēlamos risinājumus nolūkā attiecīgi pārstrādāt attiecīgās otrā kompromisa priekšlikuma daļas. Pēc versijas pārskatīšanas tika izstrādāts **trešais kompromisa priekšlikums**, ar ko prezidentvalsts Čehija *TELECOM* darba grupu iepazīstināja 5. un 8. septembrī. Papildu formulējumi un saistītie pielāgojumi sekmīgi veicināja konverģences līmeņa padziļināšanos attiecībā uz lielāko daļu neatrisināto jautājumu.

3. Tomēr **ceturtais kompromisa priekšlikums**, ar ko *TELECOM* darba grupa tika iepazīstināta 28. septembrī, parādīja atšķirības, kas joprojām pastāv starp dalībvalstīm, jo īpaši attiecībā uz vienu augsta līmeņa jautājumu, proti, Eiropas digitālās identitātes makam izvēlēto uzticamības līmeni. Dažas dalībvalstis, kurās jau ir ieviesta valsts *eID* sistēma, sākotnēji pieņēma būtisku uzticamības līmeni un pēc tam ieguldīja tā nodrošināšanā, savukārt saskaņā ar pašreizējo *eID* priekšlikumu ir nepieciešams augsts uzticamības līmenis. Apzinoties, ka dažās dalībvalstīs ir izdots liels skaits elektroniskās identifikācijas līdzekļu ar būtisku uzticamības līmeni, prezidentvalsts Čehija ir arī ierosinājusi mehānismu atvieglotai lietotāju reģistrācijai, tādējādi veicinot Eiropas digitālās identitātes maku apgūšanu. Tas lietotājiem ļauj piereģistrēties Eiropas digitālās identitātes makam, izmantojot esošos valstu *eID* pakalpojumus ar būtisku uzticamības līmeni savienojumā ar papildu attālinātās reģistrācijas procedūrām, kas kopīgi atbilst prasībām par augstu uzticamības līmeni. Tehniskajām un darbības specifikācijām piemēro īstenošanas tiesību aktus, un atbilstību prasībām sertificē.

4. **Piektais kompromisa priekšlikums** tika apspriests *TELECOM* darba grupas 2022. gada 25. marta sanāksmē. *TELECOM* darba grupas 2022. gada 8. novembra sanāksmē prezidentvalsts Čehija iepazīstināja ar veiktajām nelielajām izmaiņām un, ņemot vērā papildu piezīmes un redakcionālos ierosinājumus, kas tika saņemti no delegācijām, sagatavoja **galīgo redakciju kompromisa priekšlikuma tekstam** nolūkā to iesniegt Pastāvīgo pārstāvju komitejā.

5. Pastāvīgo pārstāvju komiteja šo kompromisa priekšlikumu izskatīja 18. novembrī un **vienbalsīgi vienojās to iesniegt TTE (Telekomunikācijas) padomei bez jebkādām izmaiņām, lai panāktu vispārēju pieeju** tās 2022. gada 6. decembra sanāksmē.

IV. KOMPROMISA PRIEKŠLIKUMA GALVENIE ELEMENTI

1. Eiropas digitālās identitātes maks

Viens no galvenajiem politikas mērķiem Komisijas priekšlikumam par Eiropas digitālās identitātes maku ("maks") ir nodrošināt pilsoņiem un citiem iedzīvotājiem, kā noteikts valstu tiesību aktos, saskaņotus Eiropas digitālās identitātes līdzekļus, kas balstās uz Eiropas digitālās identitātes maka koncepciju. Kā elektronisks identifikācijas līdzeklis ("*eID līdzeklis*"), kas saskaņā ar valsts shēmām izdots ar augstu uzticamības līmeni, maks būtu atsevišķs *eID* līdzeklis, kas balstās uz personu identifikācijas datu un maka izdošanu, ko veic dalībvalstis.

2. Eiropas digitālās identitātes maku uzticamības līmenis

Uzticamības līmeņiem būtu jāraksturo elektroniskās identifikācijas līdzekļu ticamības pakāpe personas identitātes noskaidrošanā, tādējādi nodrošinot pārliecību, ka persona, kas uzdodas par personu ar kādu konkrētu identitāti, patiešām ir tā persona, kurai minētā identitāte ir piešķirta. Pamatojoties uz darba grupas sanāksmēs un Pastāvīgo pārstāvju komitejas 14. oktobra debatēs reģistrēto plašo atbalstu, maks ir jāizdod elektroniskās identifikācijas sistēmā ar augstu uzticamības līmeni. Turklāt **6.a pantā** ir pievienots īpašs noteikums par lietotāju reģistrāciju. Šo izmaiņu mērķis ir kliedēt to dalībvalstu bažas, kurās jau ir izdots ievērojams skaits valsts

eID līdzekļu ar augstu uzticamības līmeni. Šis nosacījums ļauj lietotājam izmantot savas valsts *eID* līdzekļus savienojumā ar papildu attālinātās reģistrācijas procedūrām, lai būtu iespējams veikt identitātes pārbaudi pie augsta uzticamības līmeņa un gala rezultātā saņemt maku. Tā kā *eID* regulas pamatā ir kiberdrošības sertifikācijas shēmas, kurām būtu jānodrošina saskaņots uzticamības līmenis saistībā ar Eiropas digitālās identitātes maku drošību, paredzams, ka kiberdrošības sertifikācija tiks piemērota arī kriptogrāfijas materiālu drošai glabāšanai. Tādēļ prezidentvalsts ir ierosinājusi jaunu **(10.b) apsvērumu**, ar ko tiek risināti tehniskie priekšnosacījumi augsta uzticamības līmeņa sasniegšanai un kas ļauj veikt turpmāku procesu saistībā ar Eiropas digitālās identitātes maku ieviešanu.

3. Atkarīgo pušu paziņošana

3.1.**6.b pants** par atkarīgo pušu paziņošanu ir pārfrāzēts. Kopumā paziņošanas procesam, ar kuru atkarīgā puse informē par savu nodomu izmantot maku, vajadzētu būt rentablam, samērīgam ar risku un būtu jānodrošina, ka atkarīgās puses sniedz vismaz to informāciju, kas nepieciešama lai autentificētos makā. Pēc noklusējuma ir nepieciešama tikai minimāla informācija, un paziņojumam būtu jāļauj izmantot automatizētas vai vienkāršas pašpārskata procedūras.

3.2. Tomēr nozares prasību dēļ var būt nepieciešams īpašs režīms, piemēram, apstrādājot īpašu kategoriju personas datus. Tādēļ ir ieviests attiecīgs noteikums, kura mērķis ir aptvert gadījumus, kad ir nepieciešama stingrāka reģistrācijas vai autorizācijas procedūra. Savukārt gadījumos, kad Savienības vai valstu tiesību akti nenosaka īpašas prasības par piekļuvi informācijai, izmantojot maku, dalībvalstis tādas atkarīgās puses var atbrīvot no pienākuma paziņot par savu nodomu izmantot makus.

4. Sertifikācija

4.1. Regulai būtu jāsekmē, jāizmanto un jāļauj izmantot attiecīgās un spēkā esošās Kiberdrošības akta sertifikācijas shēmas vai to daļas, lai apliecinātu maku vai to daļu atbilstību piemērojamajām kiberdrošības prasībām. Tādēļ pilnībā jāpiemēro Kiberdrošības akta regulējums, tostarp salīdzinošās izvērtēšanas mehānisms starp Kiberdrošības aktā paredzētajām valsts kiberdrošības sertifikācijas iestādēm. Lai pēc iespējas saskaņotu *eID* regulu un

Kiberdrošības aktu, dalībvalstis izraudzīsies maka sertifikācijas nolūkam akreditētas publiskas un privātas struktūras, kā paredzēts Kiberdrošības aktā.

4.2. Turklāt Komisija tiek mudināta uzdot *ENISA* uzņemties maka kiberdrošības sertifikācijai paredzētas Kiberdrošības akta shēmas izstrādi un pieņemšanu. Kamēr šī shēma tiek izstrādāta, kā bāzes metodika maka sertifikācijā tiks izmantota *EUCC* (kopīgos kritērijos balstīta Eiropas kiberdrošības sertifikācijas shēma), kas publicēta saskaņā ar Kiberdrošības aktu. Attiecībā uz jautājumiem, kas nav saistīti ar kiberdrošību, jo īpaši tādiem, kas neaptver citus maka funkcionālos vai darbības aspektus, ir jāizveido specifikāciju, procedūru un atsauces standartu saraksts. Šīs prasības pakļauj sertifikācijai.

5. Īstenošanas termiņš maka nodrošināšanai

Pamatojoties uz dalībvalstu norādījumiem, tika ierosināts 24 mēnešu īstenošanas periodu skaitīt no **6.a panta 11. punktā** un **6.c panta 4. punktā** minēto īstenošanas aktu pieņemšanas dienas.

6. Maksas

6. a panta 6.a punktā un attiecīgajā apsvērumā ir skaidrots, ka fiziskām personām maku izsniegšanu, izmantošanu autentifikācijai un atsaukšanu vajadzētu nodrošināt bez maksas. Izņemot gadījumus, kad makus izmanto autentifikācijai, pakalpojumi, kuros tiek izmantots maks, varētu ietvert izmaksas, piemēram, maka atribūtu elektronisko apliecinājumu izdošana.

7. Piekļuve aparatūrai un programmatūras funkcijām, tostarp drošajam elementam

Prezidentvalsts ir ierosinājusi paredzēt skaidru formulējumu ar Regulu (ES) 2022/1925, ar ko nodrošina piekļuvi aparatūrai un programmatūras funkcijām kā daļai no vārtziņu sniegtajiem platformas pamatpakalpojumiem. Jaunajā **12.b pantā** skaidrots, ka maku nodrošinātāji un paziņoto elektroniskās identifikācijas līdzekļu izdevēji, kas rīkojas komerciālā vai profesionālā statusā, saskaņā ar attiecīgo Digitālo tirgu akta definīciju ir vārtziņu komerciālie lietotāji. Apsvērumam ir pievienots formulējums nolūkā izklāstīt ietekmi, ko rada saikne ar Digitālo tirgu tiesību aktu, proti, ka vārtziņiem būtu bez maksas jānodrošina efektīva sadarbspēja ar tām pašām operētājsistēmu, aparatūras vai programmatūras funkcijām, kas ir pieejamas vai tiek izmantotas, nodrošinot savus papildinošos un atbalsta pakalpojumus un aparatūru, un piekļuve tām sadarbspējas nolūkā.

8. Alternatīvas atribūtu elektroniskā apliecinājuma izdošanas iespējas valsts iestādēm

Ir saglabāta kvalificētu atribūtu elektronisko apliecinājumu izsniegšana, ko veic kvalificēti pakalpojuma sniedzēji, tostarp dalībvalstu pienākums nodrošināt, ka atribūtus var pārbaudīt, salīdzinot ar autentisku avotu publiskajā sektorā. Turklāt ir ieviesta iespēja, ka atribūtu elektronisko apliecinājumu, kam ir tāds pats juridiskais spēks kā kvalificētam atribūtu elektroniskajam apliecinājumam, makam var tieši izdot publiskā sektora iestāde, kura ir atbildīga par autentisko avotu, vai izraudzīta publiskā sektora iestāde tādas publiskā sektora iestādes vārdā, kura ir atbildīga par autentisko avotu, ar noteikumu, ka ir izpildītas nepieciešamās prasības. Šis priekšlikums ir atspoguļots jaunajā **45.a** un **45.da pantā** un **VII pielikumā**.

9. Ierakstu saskaņošana

Sākotnējais **11.a panta** nosaukums ir mainīts uz "Ierakstu saskaņošana", tādējādi labāk atspoguļojot šā noteikuma mērķi. Pamatojoties uz diskusiju, attiecībā uz makiem ir saglabāts unikāla un noturīga identifikatora jēdziens. Attiecīgajā definīcijā ir precizēts, ka identifikatoru var veidot vairāku valsts un nozares identifikatoru kombinācijas, ja vien tas kalpo savam mērķim. Ir skaidri noteikts, ka ierakstu saskaņošanu var sekmēt kvalificēts atribūtu elektroniskais apliecinājums. Turklāt **11.a pantā** ir iekļauts aizsardzības noteikums, saskaņā ar kuru dalībvalstis nodrošina personas datu aizsardzību un nepieļauj lietotāju profilēšanu. Visbeidzot, dalībvalstis, rīkojoties kā atkarīgās puses, nodrošina ierakstu saskaņošanu.

VI. NOBEIGUMS

1. Ņemot vērā minēto, Padome tiek aicināta:

   – izskatīt šīs piezīmes Pielikumā izklāstīto kompromisa tekstu;

   – TTE padomē (Telekomunikācijas) 2022. gada 6. decembrī apstiprināt vispārēju pieeju attiecībā uz Regulu par Eiropas digitālo identitāti (Eiropas *eID*).

_____

PIELIKUMS

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA,

ar ko Regulu (ES) Nr. 910/2014 groza attiecībā uz Eiropas digitālās identitātes regulējuma 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 [3],

saskaņā ar parasto likumdošanas procedūru,

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, paplašinātu tās priekšrocības privātajā sektorā un veicinātu uzticamas digitālās identitātes visiem eiropiešiem.

[3] OV C ..., ..., ... lpp.
[4] COM/2020/67 final.

(2) Savos 2020. gada 1.–2. oktobra secinājumos [5] Eiropadome aicināja Komisiju ierosināt izstrādāt drošas publiskas elektroniskas identifikācijas, tostarp sadarbspējīgu digitālo parakstu, Savienības mēroga regulējumu, lai cilvēkiem nodrošinātu kontroli pār viņu tiešsaistes identitāti un datiem, kā arī ļautu piekļūt sabiedriskiem, privātiem un pārrobežu digitāliem pakalpojumiem.

(3) Komisijas 2021. gada 9. marta paziņojumā "Digitālais kompass līdz 2030. gadam – Eiropas ceļam digitālajā gadu desmitā" [6] ir noteikts Savienības regulējuma mērķis, kas līdz 2030. gadam ļaus plaši izvērst uzticamu, lietotāju kontrolētu identitāti, ļaujot katram lietotājam pašam kontrolēt savu mijiedarbību un klātbūtni tiešsaistē.

(4) Saskaņotākai pieejai digitālajai identifikācijai būtu jāsamazina pašreizējās sadrumstalotības riski un izmaksas, ko rada atšķirīgu valstu risinājumu lietošana, un tā stiprinās vienoto tirgu, ļaujot pilsoņiem, citiem iedzīvotājiem, kā noteikts valsts tiesību aktos, un uzņēmumiem ērti, uzticami un vienoti identificēties visā Savienībā. Eiropas digitālās identitātes maks fiziskām un juridiskām personām visā Savienībā nodrošinās saskaņotus elektroniskās identifikācijas līdzekļus, kas tām ļaus veikt autentifikāciju un dalīties ar datiem, kas saistīti ar to identitāti. Ikvienam vajadzētu būt iespējai droši piekļūt sabiedriskiem un privātiem pakalpojumiem, paļaujoties uz uzlabotu uzticamības pakalpojumu ekosistēmu, kā arī uz verificētiem identitātes pierādījumiem un atribūtu apliecinājumiem, piemēram, akadēmisko kvalifikāciju, kas likumīgi atzīta un akceptēta visur Savienībā, profesionālo kvalifikāciju, grādu, licenci vai pilnvarām pārstāvēt uzņēmumu. Eiropas digitālās identitātes regulējuma mērķis ir panākt pāreju no paļaušanās vienīgi uz valsts digitālās identitātes risinājumiem uz tādu atribūtu elektronisko apliecinājumu sniegšanu, kas ir derīgi un juridiski atzīti visā Savienībā. Atribūtu elektronisko apliecinājumu sniedzējiem būtu jāgūst labums no skaidra un vienota noteikumu kopuma, un valsts iestādēm vajadzētu būt iespējai paļauties uz noteikta un ļoti droša formāta elektroniskiem dokumentiem.

---

[5] https://www.consilium.europa.eu/lv/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

[6] COM/2021/118 final/2.

(4.a) Vairākas dalībvalstis ir ieviesušas un plaši izmanto elektroniskās identifikācijas līdzekļus, kurus mūsdienās atzīst pakalpojumu sniedzēji Savienībā. Turklāt ieguldījumi gan valsts, gan pārrobežu risinājumos tika veikti, pamatojoties uz pašreizējo *eIDAS* regulu, tostarp *eIDAS* mezglu sadarbspējas tehnisko infrastruktūru. Lai nodrošinātu Eiropas digitālās identitātes maku papildināmību un pašreizējie paziņoto elektroniskās identifikācijas līdzekļu lietotāji tos ātri pieņemu, un lai līdz minimumam samazinātu ietekmi uz esošajiem pakalpojumu sniedzējiem, paredzams, ka Eiropas digitālās identitātes maki gūs labumu, balstoties uz pieredzi, kas gūta no esošajiem elektroniskās identifikācijas līdzekļiem, un izmantojot priekšrocības, ko sniedz Eiropas un valstu līmeņos izvērstā *eIDAS* infrastruktūra.

(5) Lai atbalstītu Eiropas uzņēmumu konkurētspēju, tiešsaistes pakalpojumu sniedzējiem vajadzētu būt iespējai paļauties uz digitālās identitātes risinājumiem, kas atzīti visā Savienībā, neatkarīgi no dalībvalsts, kurā tie izdoti, tādējādi gūstot labumu no saskaņotās Eiropas pieejas uzticamībai, drošībai un sadarbspējai. Gan lietotājiem, gan pakalpojumu sniedzējiem vajadzētu būt iespējai gūt labumu no vienādas juridiskās vērtības, ko visā Savienībā sniedz atribūtu elektroniskie apliecinājumi.

(6) Regula (ES) Nr. 2016/679 [7] attiecas uz personas datu apstrādi, īstenojot šo regulu. Tāpēc šajā regulā būtu jāparedz īpaši aizsardzības pasākumi, lai nepieļautu to, ka elektroniskās identifikācijas līdzekļu un atribūtu elektronisko apliecinājumu sniedzēji apvieno no citiem pakalpojumiem iegūtus personas datus ar personas datiem, kas saistīti ar pakalpojumiem, uz kuriem attiecas šī regula. Personas dati, kas attiecas uz Eiropas digitālās identitātes maku nodrošināšanu, būtu jāglabā loģiski nošķirti no citiem izsniedzēja glabātajiem datiem. Šī regula Eiropas digitālās identitātes maku izdevējiem neliedz piemērot papildu tehniskos pasākumus, kas veicina personas datu aizsardzību, piemēram, ar maku nodrošināšanu saistītu personas datu fizisku nošķiršanu no citiem izdevēja glabātajiem datiem.

[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.

(7) Jāparedz saskaņoti nosacījumi, lai izveidotu dalībvalstu nodrošinātu Eiropas digitālās identitātes maku regulējumu, kam būtu jādod iespēja visiem Savienības pilsoņiem un citiem iedzīvotājiem, kā noteikts valsts tiesību aktos, lietotājdraudzīgā un ērtā veidā droši koplietot ar viņu identitāti saistītu datus, ko kontrolē vienīgi lietotājs. Lai panāktu augstāko drošības līmeni, privātumu, lietotāju ērtību un plašu lietojamību, būtu jāattīsta šo mērķu sasniegšanai izmantotās tehnoloģijas. Dalībvalstīm būtu jānodrošina vienāda piekļuve digitālajai identifikācijai visiem to valstspiederīgajiem un iedzīvotājiem.

(8) Lai nodrošinātu, ka atkarīgās puses var paļauties uz Eiropas digitālās identitātes maku izmantošanu, un pasargātu lietotāju no sensitīvo datu nelikumīgas izmantošanas, atkarīgās puses būtu jāreģistrē kā daļa no paziņošanas procesa. Atkarīgajām pusēm piemērojamās paziņošanas prasības lielākajā daļā gadījumu būtu jābalsta uz ierobežota informācijas apjoma sniegšanu, kas nepieciešama atkarīgās puses autentifikācijai Eiropas digitālās identitātes makā. Saskaņā ar šīm prasībām būtu arī jāļauj izmantot automatizētas vai pašpārskata procedūras, tostarp ļaut dalībvalstīm paļauties uz esošajiem reģistriem un tos izmantot. Vienlaikus attiecībā uz sensitīvo datu kategorijām valstu un Savienības līmenī var pastāvēt īpaši režīmi, kas atkarīgajām pusēm varētu piemērot stingrākas reģistrācijas un autorizācijas prasības, lai šādos gadījumos novērstu identitātes datu nelikumīgu izmantošanu. Citos izmantošanas gadījumos atkarīgās puses var būt atbrīvotas no pienākuma paziņot par savu nodomu izmantot Eiropas digitālo maku, piemēram, ja attiecībā uz tiesībām pārbaudīt konkrētus atribūtus nav prasīts vai atļauts elektroniski autentificēt atkarīgo pusi. Parasti šādās klātienes situācijās lietotājs var identificēt atkarīgo pusi, ņemot vērā kontekstu, piemēram, nonākot saskarsmē ar automobiļu nomas darbinieku vai farmaceitu. Paredzēts, ka paziņošanas procesu pārvaldīs Savienības vai valstu nozaru tiesību akti, jo tas ļauj aptvert dažādus izmantošanas gadījumus, kas var būt atšķirīgi attiecībā uz reģistrācijas prasībām, darbības režīmu (tiešsaistē/bezsaistē) vai attiecībā uz prasību autentificēt ierīces, kas spēj nodrošināt saskarni ar Eiropas digitālās identitātes maku. Eiropas Digitālās identitātes maka līmenī nevajadzētu uzdot veikt pārbaudi par atkarīgo pušu izmantotu Eiropas digitālās identitātes maku.

(9) Visiem Eiropas digitālās identitātes makiem būtu jāļauj lietotājiem elektroniski identificēties un autentificēties tiešsaistē un bezsaistē pāri robežām, lai piekļūtu visdažādākajiem sabiedriskajiem un privātajiem pakalpojumiem. Neskarot dalībvalstu prerogatīvas attiecībā uz savu valstspiederīgo un iedzīvotāju identifikāciju, arī valsts iestādes, starptautiskās organizācijas un Savienības iestādes, struktūras, biroji un aģentūras var izmantot makus savām vajadzībām. Lietošana bezsaistē būtu svarīga daudzās nozarēs, tostarp veselības aprūpes nozarē, kur pakalpojumus bieži sniedz, mijiedarbojoties klātienē, un, lai varētu pārbaudīt autentiskumu, vajadzētu būt iespējai e-receptēm izmantot *QR* kodus vai līdzīgas tehnoloģijas. Atsaucoties uz "augstu" pārliecības līmeni, Eiropas digitālās identitātes makiem būtu jāizmanto potenciāls, ko piedāvā risinājumi, kas droši pret viltojumiem, piemēram, drošie elementi, lai izpildītu šajā regulā noteiktās drošības prasības. Eiropas digitālās identitātes makiem būtu arī jāļauj lietotājiem izveidot un izmantot kvalificētus elektroniskos parakstus un zīmogus, kas ir pieņemami visā ES. Lai personas un uzņēmumi visā ES varētu gūt labumu no vienkāršošanas un izmaksu samazināšanas, tostarp ļaujot izmantot pārstāvības pilnvaras un e-pilnvaras, dalībvalstīm būtu jāizdod Eiropas digitālās identitātes maki, pamatojoties uz kopīgiem standartiem, lai nodrošinātu nepārtrauktu sadarbspēju un augstu drošības līmeni. Tikai dalībvalstu kompetentās iestādes var nodrošināt augstu ticamības pakāpi, nosakot personas identitāti, un tādējādi sniegt pārliecību, ka persona, kas uzrāda vai apliecina konkrētu identitāti, patiešām ir persona, par kuru viņš vai viņa uzdodas. Tāpēc Eiropas digitālās identitātes makiem ir jāpaļaujas uz pilsoņu, citu iedzīvotāju vai juridisku personu juridisko identitāti. Uzticēšanās Eiropas digitālās identitātes makiem palielinātos, ja to izdevējiem būtu jāveic atbilstoši tehniski un organizatoriski pasākumi, kas garantē tādu drošības līmeni, kurš ir samērīgs ar riskiem, ko izraisa fizisku personu tiesības un brīvības saskaņā ar Regulu (ES) 2016/679. Fiziskām personām Eiropas digitālās identitātes maku izsniegšana, izmantošana autentifikācijai un atsaukšana ir bez maksas. Pakalpojumi, kuros izmanto maku, var ietvert izmaksas saistībā ar, piemēram, maka atribūtu elektronisko apliecinājumu izdošanu.

(9.a) Ir lietderīgi veicināt Eiropas digitālās identitātes maku apgūšanu un izmantošanu, tos vienmērīgi integrējot publiskā un privātā sektora digitālo pakalpojumu ekosistēmā, kas jau ir ieviesta valsts, vietējā vai reģionālajā līmenī. Lai sasniegtu šo mērķi, dalībvalstis var paredzēt juridiskus un organizatoriskus pasākumus, lai uzlabotu Eiropas digitālās identitātes maku izdevēju elastīgumu un Eiropas digitālās identitātes makiem atļautu papildu funkcionalitātes, kas pārsniedz šajā regulā noteiktās, tostarp labāku sadarbspēju ar esošajiem valsts *eID* līdzekļiem. Tam nekādā gadījumā nevajadzētu nelabvēlīgi ietekmēt Eiropas digitālās identitātes maku pamatfunkciju nodrošināšanu, kā izklāstīts šajā regulā, nedz arī sekmēt esošo valsts risinājumu izmantošanu Eiropas digitālās identitātes maku vietā. Tā kā tie pārsniedz šīs regulas tvērumu, minētās papildu funkcijas negūst labumu no noteikumiem par Eiropas digitālās identitātes maku izmantošanu pārrobežu mērogā, kā izklāstīts šajā regulā.

(10) Lai sasniegtu augstu datu aizsardzības, drošuma un uzticamības līmeni, ar šo regulu būtu jāizveido saskaņots regulējums, kurā sīki izklāstītas kopējās specifikācijas un prasības, kas piemērojamas Eiropas digitālās identitātes makiem. Eiropas digitālās identitātes maku atbilstība šīm prasībām būtu jāapstiprina akreditētām atbilstības novērtēšanas struktūrām, ko norīkojušas dalībvalstis. Veicot sertifikāciju, jo īpaši būtu jāpaļaujas uz attiecīgajām Eiropas kiberdrošības sertifikācijas shēmām vai to daļām, kas izveidotas saskaņā ar Regulu (ES) 2019/881 [8], ciktāl tās aptver Eiropas digitālās identitātes makiem piemērojamās kiberdrošības prasības. Eiropas kiberdrošības sertifikācijas shēmu izmantošanai vajadzētu radīt saskaņotu uzticamības līmeni attiecībā uz Eiropas digitālās identitātes maku drošību, neatkarīgi no tā, kur Savienībā tie izsniegti. Eiropas digitālās identitātes maku kiberdrošības sertifikācijā būtu jāizmanto valstu kiberdrošības sertifikācijas iestāžu loma tādu sertifikātu atbilstības pārraudzīšanā un uzraudzīšanā, kurus savā jurisdikcijā izsniegušas atbilstības novērtēšanas iestādes, izmantojot attiecīgās Eiropas kiberdrošības shēmas. Līdzīgi sertifikācijā būtu attiecīgi jāizmanto Regulā (ES) 2019/881 norādītie standarti un tehniskās specifikācijas. Šādas specifikācijas var izmantot kā mūsdienīgus dokumentus, kā norādīts saskaņā ar attiecīgajām kiberdrošības sertifikācijas shēmām, ievērojot Regulu (ES) 2019/881. Ja neviena no attiecīgajām Eiropas kiberdrošības sertifikācijas shēmām, kas izveidotas, ievērojot Regulu (ES) 2019/881, neaptver attiecīgo pakalpojumu vai procesu sertifikāciju, kas veicina maka drošību, saskaņā ar Regulas (ES) 2019/881 III sadaļu būtu jāizveido atbilstošas shēmas. Būtu jāizveido kopēja un saskaņota Eiropas digitālās identitātes maku sertifikācijas shēma, lai novērtētu to atbilstību tām šajā regulā paredzētajām kopējām specifikācijām un prasībām, kuras nav saistītas ar kiberdrošību un datu aizsardzību, jo īpaši tām, kas aptver funkcionālos un darbības aspektus. Attiecībā uz šādu sertifikāciju, lai nodrošinātu augstu uzticamības un pārredzamības līmeni, būtu jāizveido mehānismi un procedūras nolūkā veicināt mācīšanos no līdzbiedriem un sadarbību starp dalībvalstīm attiecībā uz sertifikācijas struktūru un to izsniegto sertifikātu un sertifikācijas ziņojumu pārraudzību un pārskatīšanu. Šādam mācīšanās no līdzbiedriem mehānismam nevajadzētu skart Regulu (ES) 2016/679 un Regulu (ES) 2019/881. Maka sertifikācija saskaņā ar Regulu (EK) 2016/679 cita starpā ir brīvprātīgs instruments, ko var izmantot, lai apliecinātu atbilstību Regulā (EK) 2016/679 izklāstītajām prasībām, jo tās attiecas uz Eiropas digitālās identitātes makiem un to nodrošināšanu Eiropas pilsoņiem.

---

8 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.).

(10.a) Pilsoņu un iedzīvotāju reģistrācija Eiropas digitālās identitātes makiem būtu jāveicina, paļaujoties uz elektriskās identifikācijas līdzekļiem, kas izsniegti ar augstu uzticamības līmeni. Elektroniskās identifikācijas līdzekļi, kas izsniegti ar augstu uzticamības līmeni, būtu jāizmanto vienīgi gadījumos, kad saskaņotas tehniskās un darbības specifikācijas par elektroniskās identifikācijas līdzekļu izmantošanu, kas izsniegti ar augstu uzticamības līmeni, kopā ar citiem papildu identitātes verificēšanas līdzekļiem ļauj izpildīt šajā regulā izklāstītās prasības attiecībā uz augstu uzticamības līmeni. Tādiem papildu līdzekļiem vai pasākumiem vajadzētu būt uzticamiem un tādiem, lai lietotāji tos var ērti izmantot, un to pamatā vajadzētu būt iespējai izmantot attālinātās reģistrēšanās iespējas, kvalificētus sertifikātus, kas apliecināti ar kvalificētiem parakstiem, kvalificētus atribūtu elektroniskos apliecinājumus vai to kombināciju. Lai nodrošinātu Eiropas digitālās identitātes maku pietiekamu apgūšanu, īstenošanas aktos būtu jāizklāsta harmonizētas tehniskās un darbības specifikācijas attiecībā uz lietotāju reģistrēšanu, izmantojot elektroniskās identifikācijas līdzekļus, tostarp tos, kas izsniegti ar būtisku uzticamības līmeni.

(10.b) 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, drošības elementi lietotāju ierīcēs, Eiropas digitālās identitātes maki var izmantot sertificētus ārējos drošības elementus, lai aizsargātu kriptogrāfijas materiālus un citus sensitīvus datus, vai gadījumā, kad ir paziņoti augsta uzticamības līmeņa valsts risinājumi, apliecinātu atbilstību attiecīgajām regulas prasībām, ko piemēro maka uzticamības līmenim. Minētā pārejas pasākuma izmantošana būtu jāierobežo gadījumos, kad nepieciešams augsts uzticamības līmenis, piemēram, reģistrējot maka lietotāju un autentificējoties pakalpojumiem, kam nepieciešams augsts uzticamības līmenis. Autentificējoties pakalpojumiem, kam nepieciešams augsts uzticamības līmenis, nevajadzētu būt prasībai Eiropas digitālās identitātes makiem izmantot minēto pārejas pasākumu. Šai regulai nevajadzētu skart valstu noteikumus, piemēram, par sertificēta ārēja drošā elementa izsniegšanu un izmantošanu gadījumā, ja uz to atsaucas šis pārejas pasākums.

(11) Eiropas digitālās identitātes makiem būtu jāgarantē augstākais aizsardzības un drošības līmenis personas datiem, kurus izmanto autentifikācijai, neatkarīgi no tā, vai šie dati tiek glabāti lokāli, mākoņdatošanas risinājumos vai abu minēto kombinācijā atkarībā no dažādiem riska līmeņiem. Biometrisko datu kā autentifikācijas faktora apstrāde drošai lietotāju autentifikācijai ir viena no identifikācijas metodēm, kas nodrošina augstu ticamības līmeni, jo īpaši, ja to lieto kopā ar citiem autentifikācijas elementiem. Tā kā biometriskie dati ir unikāls personas raksturlielums, biometrisko datu apstrāde ir atļauta tikai saskaņā ar Regulas (ES) 2016/679 9. panta 2. punktā paredzētajiem izņēmumiem, un saistībā ar to ir jāveic pienācīgi aizsardzības pasākumi, kas ir samērīgi ar riskiem, ko šāda apstrāde var radīt fizisku personu tiesībām un brīvībām.

(11.a) Eiropas digitālās identitātes maka darbībai jābūt pārredzamai un jāļauj apstrādāt personas datus pārbaudāmā veidā. Lai to panāktu, dalībvalstis tiek mudinātas atklāt pirmkodu tām Eiropas digitālās identitātes maku programmatūras sastāvdaļām, kas ir saistītas ar personas datu un juridisku personu datu apstrādi. Šāda pirmkoda atklāšana ļautu sabiedrībai, tostarp lietotājiem un izstrādātājiem, saprast tā darbību. Tas arī varētu palielināt lietotāju uzticību maka ekosistēmai un uzlabot maku drošību, ikvienam ļaujot ziņot par kodam konstatētajām ievainojamībām un kļūdām. Tas mudina piegādātājus izstrādāt un nodrošināt ļoti drošu produktu. Papildus un attiecīgā gadījumā dalībvalstis arī tiek mudinātas sniegt pieeju piekļuves kodam saskaņā ar atvērtā pirmkoda licenci. Atvērtā pirmkoda licence ļauj sabiedrībai, tostarp lietotājiem un izstrādātājiem, pirmkodu mainīt vai izmantot atkārtoti.

(12) Lai nodrošinātu, ka Eiropas digitālās identitātes regulējums ir atvērts inovācijām, tehnoloģiju attīstībai un ir nākotnes prasībām atbilstošs, dalībvalstis būtu jāmudina kopīgi izveidot piemērotu vidi, kurā kontrolētā un drošā veidā pārbaudīt novatoriskus risinājumus, jo īpaši, lai uzlabotu risinājumu funkcionalitāti, personas datu aizsardzību, drošību un sadarbspēju, un informētu par tehnisko atsauču un juridisko prasību turpmākajiem atjauninājumiem. Šai videi būtu jāveicina Eiropas mazo un vidējo uzņēmumu, jaunuzņēmumu un individuālu novatoru un pētnieku iekļaušana.

(13) Regula (ES) Nr. 2019/1157 [9] līdz 2021. gada augustam pastiprina identitātes karšu drošību ar uzlabotiem drošības elementiem. Dalībvalstīm būtu jāapsver iespēja tās paziņot saskaņā ar elektroniskās identifikācijas shēmām, lai paplašinātu elektroniskās identifikācijas līdzekļu pārrobežu pieejamību.

(14) 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 saskaņā ar Regulu 910/2014.

(15) Pašreizējo paziņošanas un mācīšanās no līdzbiedriem procedūru racionalizēšana novērsīs dažādas pieejas dažādu paziņoto elektroniskās identifikācijas shēmu novērtēšanai un veicinās dalībvalstu savstarpējo uzticēšanos. Jauniem, vienkāršotiem mehānismiem būtu jāveicina dalībvalstu sadarbība to paziņoto elektroniskās identifikācijas shēmu drošības un sadarbspējas jomā.

(16) Dalībvalstīm būtu jāgūst labums no jauniem, elastīgiem rīkiem, ar kuriem nodrošina atbilstību šīs regulas un attiecīgo īstenošanas aktu prasībām. Šai regulai būtu jāļauj dalībvalstīm izmantot ziņojumus un novērtējumus, ko veikušas akreditētas atbilstības novērtēšanas struktūras, kā paredzēts sertifikācijas shēmās, kas saskaņā ar Regulu (ES) 2019/881 jāizveido Savienības līmenī, lai atbalstītu savas prasības par shēmu vai to daļu saskaņošanu ar regulas prasībām par paziņoto elektroniskās identifikācijas shēmu sadarbspēju un drošību.

---

[9] 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.).

(17.a) Dalībvalstu izdotu vai Eiropas digitālā identitātes maka ģenerētu unikālu un noturīgu identifikatoru izmantošana kopā ar personas identifikācijas datiem ir būtiska, lai nodrošinātu, ka lietotāja identitāte ir verificējama, jo īpaši publiskajā sektorā un tajos gadījumos, kad to nosaka Savienības tiesību akti vai valsts tiesību akti. Šai regulai būtu jānodrošina, ka Eiropas digitālās identitātes maks var nodrošināt mehānismu, kas ļauj saskaņot ierakstus, tostarp izmantojot kvalificētu atribūtu elektronisko apliecinājumu, un ļauj ietvert unikālus un noturīgus identifikatorus personas identifikācijas datu kopā. Unikālu un noturīgu identifikatoru var veidot viens vai vairāki identifikācijas dati, kas var būt specifiski nozarei, ar nosacījumu, ka tie unikāli identificē lietotāju visā Savienībā. Eiropas digitālās identitātes makam būtu arī jānodrošina mehānisms, kas atkarīgajai pusei ļauj izmantot specifiskus identifikatorus gadījumos, kad unikālā un noturīgā identifikatora izmantošanu paredz valsts vai Savienības tiesību akti. Visos gadījumos mehānismam, ar ko tiek veicināta ierakstu saskaņošana un unikālo un noturīgo identifikatoru izmantošana, būtu jānodrošina, ka lietotājs ir aizsargāts pret personas datu ļaunprātīgu izmantošanu saskaņā ar šo regulu un piemērojamajiem Savienības tiesību aktiem, jo īpaši Regulu (ES) 2016/679, tostarp pret profilēšanas un izsekošanas risku, kas saistīts ar Eiropas digitālās identitātes maka izmantošanu.

(17.aa) Ir būtiski ņemt vērā lietotāju vajadzības, tādējādi palielinot pieprasījumu pēc Eiropas digitālās identitātes makiem. Vajadzētu būt pieejamiem jēgpilnas izmantošanas gadījumiem un tiešsaistes pakalpojumiem, kuros tiek izmantoti pieejamie Eiropas digitālās identitātes maki. Lietotāju ērtībai un nolūkā nodrošināt šādu pakalpojumu pārrobežu pieejamību, ir svarīgi veikt darbības, ar ko tiek sekmēta visās dalībvalstīs līdzīga pieeja tiešsaistes pakalpojumu izstrādē, projektēšanā un ieviešanā. Lai sasniegtu šo mērķi, par lietderīgu instrumentu potenciāli varētu kļūt nesaistošās pamatnostādnes par to, kā izstrādāt, projektēt un ieviest tiešsaistes pakalpojumus, kuros tiek izmantoti Eiropas digitālās identitātes maki. Šīs pamatnostādnes būtu jāsagatavo, pienācīgi ņemot vērā Savienības sadarbspējas regulējumu. Dalībvalstīm vajadzētu būt vadošajai lomai to pieņemšanā.

(18) Saskaņā ar Direktīvu (ES) 2019/882 [10] personām ar invaliditāti būtu jāspēj vienlīdzīgi ar citiem lietotājiem lietot Eiropas digitālās identitātes makus, uzticamības pakalpojumus un galalietotāju produktus, ko izmanto šo pakalpojumu sniegšanā.

(19) 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 valsts vai Savienības tiesību aktos. Turklāt tai nebūtu jāietekmē valstu formātam izvirzītās prasības, kas attiecas uz publiskiem reģistriem, jo īpaši komercreģistriem un zemes reģistriem.

(20) Uzticamības pakalpojumu sniegšana un lietošana kļūst arvien nozīmīgāka starptautiskajā tirdzniecībā un sadarbībā. ES starptautiskie partneri veido uzticamības regulējumus, iedvesmojoties no Regulas (ES) Nr. 910/2014. Tādēļ, lai atvieglotu šādu pakalpojumu un to sniedzēju atzīšanu, īstenošanas tiesību aktos var paredzēt nosacījumus, saskaņā ar kuriem trešo valstu uzticamības regulējumus varētu uzskatīt par līdzvērtīgiem šajā regulā paredzētajam kvalificētu uzticamības pakalpojumu un šādu pakalpojumu sniedzēju regulējumam, kas papildina Savienībā un trešās valstīs reģistrētu uzticamības pakalpojumu un šādu pakalpojumu sniedzēju savstarpējas atzīšanas iespēju saskaņā ar Līguma 218. pantu. Paredzot nosacījumus, saskaņā ar kuriem trešo valstu uzticamības regulējumus varētu uzskatīt par līdzvērtīgiem šajā regulā paredzētajam kvalificētu uzticamības pakalpojumu un šādu pakalpojumu sniedzēju regulējumam, būtu jānodrošina, ka tiek ievēroti attiecīgie Direktīvas XXXX/XXX (NIS2 direktīva) un Regulas (ES) 2016/679 noteikumi, kā arī uzticamības saraksti tiek izmantoti kā būtiski elementi, lai panāktu uzticēšanos.

[10] 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.).

(21) Šīs regulas pamatā vajadzētu būt Savienības aktiem, kas nodrošina sāncensīgus un godīgus tirgus digitālajā nozarē. Jo īpaši tās pamatā vajadzētu būt Regulai (ES) 022/1925, ar ko ievieš noteikumus galveno platformas pakalpojumu sniedzējiem, kas norīkoti par vārtziņiem, un cita starpā aizliedz vārtziņiem pieprasīt komerciālajiem lietotājiem izmantot, piedāvāt vai sadarboties ar vārtziņa identifikācijas pakalpojumu saistībā ar pakalpojumiem, ko komerciālie lietotāji piedāvā, izmantojot attiecīgā vārtziņa galvenos platformas pakalpojumus. Regulas (ES) 2022/1925 6. panta 7. punkta f) apakšpunktā ir noteikts, ka vārtziņi ļauj komerciālajiem lietotājiem un papildpakalpojumu sniedzējiem piekļūt tai pašai operētājsistēmai, aparatūras vai programmatūras funkcijām, kas ir pieejamas vai tiek izmantotas vārtziņa papildpakalpojumu sniegšanā, un sadarboties ar tām. Saskaņā ar Regulas (ES) 2022/1925 2. panta 15. punktu identifikācijas pakalpojumi ir papildpakalpojumu veids. Tāpēc komerciālajiem lietotājiem un papildpakalpojumu sniedzējiem vajadzētu būt iespējai piekļūt šādām aparatūras vai programmatūras funkcijām, piemēram, viedtālruņu drošajiem elementiem, un sadarboties ar tām, izmantojot Eiropas digitālās identitātes makus vai dalībvalstu paziņotos elektroniskās identifikācijas līdzekļus.

(22) Lai racionalizētu uzticamības pakalpojumu sniedzējiem uzliktos kiberdrošības pienākumus, kā arī ļautu šiem pakalpojumu sniedzējiem un to attiecīgajām kompetentajām iestādēm gūt labumu no tiesiskā regulējuma, kas izveidots ar Direktīvu XXXX/XXXX (NIS2 direktīva), uzticamības pakalpojumiem ir jāveic atbilstoši tehniski un organizatoriski pasākumi saskaņā ar Direktīvu XXXX/XXXX (NIS2 direktīva), 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 Direktīvu XXXX/XXXX (NIS2 direktīva) sniegtu savus pakalpojumus un ziņotu par nozīmīgiem incidentiem un kiberdraudiem. Attiecībā uz ziņošanu par incidentiem uzticamības pakalpojumu sniedzējiem būtu jāpaziņo par visiem 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 XXXXXX [NIS2] būtu uzskatāmi par tādiem, kuri papildina prasības, kas uzticamības pakalpojumu sniedzējiem noteiktas saskaņā ar šo regulu. Attiecīgā gadījumā saskaņā ar Direktīvu XXXX/XXXX (NIS2 direktīva) norīkotajām kompetentajām iestādēm arī turpmāk būtu jāpiemēro iedibinātā valsts prakse vai norādījumi par drošības un ziņošanas prasību īstenošanu un šādu prasību ievērošanas pārraudzību saskaņā ar Regulu (ES) Nr. 910/2014. Šīs regulas prasības neietekmē pienākumu ziņot par personas datu pārkāpumiem saskaņā ar Regulu (ES) 2016/679.

(23) Pienācīgi jāapsver iespēja nodrošināt efektīvu sadarbību starp TIS un eIDA iestādēm. Gadījumos, kad uzraudzības iestāde saskaņā ar šo regulu atšķiras no kompetentajām iestādēm, kas norīkotas saskaņā ar Direktīvu XXXX/XXXX [NIS2], šīm iestādēm būtu cieši un savlaicīgi jāsadarbojas, apmainoties ar attiecīgo informāciju, lai nodrošinātu efektīvu uzraudzību un uzticamības pakalpojumu sniedzēju atbilstību šajā regulā un Direktīvā XXXX/XXXX [NIS2] noteiktajām prasībām. Jo īpaši saskaņā ar šo regulu uzraudzības iestādēm vajadzētu būt tiesīgām saskaņā ar Direktīvu XXXXX/XXXX [NIS2] lūgt kompetento iestādi sniegt attiecīgu informāciju, kas vajadzīga kvalificēta statusa piešķiršanai, un veikt pārraudzības darbības, lai pārbaudītu uzticamības pakalpojumu sniedzēju atbilstību attiecīgajām NIS2 prasībām, vai pieprasīt uzticamības pakalpojumu sniedzējiem novērst neatbilstību.

(24) Ir būtiski izveidot tiesisko regulējumu, kas atvieglo pārrobežu atzīšanu starp esošajām valstu tiesību sistēmām attiecībā uz elektroniski reģistrētiem piegādes pakalpojumiem. Minētais regulējums varētu arī radīt jaunas tirgus iespējas Savienības uzticamības pakalpojumu sniedzējiem piedāvāt jaunus elektroniski reģistrētus piegādes pakalpojumus visā Eiropā. Lai nodrošinātu, ka dati, izmantojot kvalificētu elektroniski reģistrētu piegādes pakalpojumu, tiek piegādāti pareizajam adresātam, kvalificētiem elektroniski reģistrētiem piegādes pakalpojumiem ar pilnīgu noteiktību būtu jānodrošina adresāta identifikācija, savukārt attiecībā uz sūtītāja identifikāciju būtu pietiekama identifikācija ar augstu ticamības līmeni. Dalībvalstīm būtu jāmudina kvalificētu elektroniski reģistrētu piegādes pakalpojumu sniedzējus nodrošināt savu pakalpojumu sadarbspēju ar kvalificētiem elektroniski reģistrētajiem 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.

(25) Vairumā gadījumu pilsoņi un citi iedzīvotāji nevar droši un ar augstu datu aizsardzības līmeni digitāli pāri robežām apmainīties ar informāciju, kas saistīta ar viņu identitāti, piemēram, adresi, vecumu un profesionālo kvalifikāciju, vadītāja apliecībām un citām atļaujām un maksājumu datiem.

(26) Vajadzētu būt iespējai izdot un apstrādāt uzticamus digitālos atribūtus un palīdzēt samazināt administratīvo slogu, dodot pilsoņiem un citiem iedzīvotājiem iespēju tos izmantot savos privātajos un publiskajos darījumos. Pilsoņiem un citiem iedzīvotājiem, piemēram, vajadzētu būt iespējai pierādīt, ka viņiem ir derīga vienas dalībvalsts iestādes izsniegta vadītāja apliecība, ko var pārbaudīt un uz kuru var paļauties citu dalībvalstu attiecīgās iestādes, paļauties uz sava sociālā nodrošinājuma akreditācijas datiem vai uz nākotnes digitālajiem ceļošanas dokumentiem pārrobežu kontekstā.

(27) Ikvienam subjektam, kas vāc, veido un izsniedz apstiprinātus atribūtus, piemēram, diplomus, licences, dzimšanas apliecības, vajadzētu būt iespējai kļūt par atribūtu elektroniskās apliecināšanas pakalpojumu sniedzēju. Atkarīgajām personām būtu jāizmanto atribūtu elektroniskie apliecinājumi kā līdzvērtīgi papīra formāta apliecinājumiem. Tādēļ atribūtu elektroniskam apliecinājumam nevajadzētu liegt juridisko spēku, pamatojoties uz to, ka tas ir elektroniskā formātā vai neatbilst kvalificēta elektroniska atribūtu apliecinājuma prasībām. Šajā nolūkā būtu jānosaka vispārīgas prasības, lai nodrošinātu, ka kvalificētam atribūtu elektroniskam apliecinājumam ir līdzvērtīgs juridisks spēks kā likumīgi izsniegtiem papīra formāta apliecinājumiem. Tomēr šīs prasības būtu jāpiemēro, neskarot Savienības vai valsts tiesību aktus, kas nosaka papildu īpašas nozares prasības attiecībā uz formātu ar attiecīgu juridisku spēku, un jo īpaši attiecīgā gadījumā attiecībā uz atribūtu kvalificēta elektroniska apliecinājuma pārrobežu atzīšanu.

(28) Lai Eiropas digitālās identitātes maki būtu plaši pieejami un lietojami, tos jāpieņem privātiem pakalpojumu sniedzējiem. Privātām atkarīgām personām, kuras sniedz pakalpojumus transporta, enerģētikas, banku, finanšu pakalpojumu, sociālā nodrošinājuma, veselības aprūpes, dzeramā ūdens, pasta pakalpojumu, digitālās infrastruktūras, izglītības vai telekomunikāciju jomā, būtu jāpieņem Eiropas digitālās identitātes maku lietošana pakalpojumu sniegšanas vajadzībām, ja valsts vai Savienības tiesību aktos vai līgumsaistībās ir paredzēta stingra lietotāja autentifikācija. Lai sekmētu Eiropas digitālās identitātes maka izmantošanu un pieņemšanu, būtu jāņem vērā plaši pieņemti nozares standarti un specifikācijas. Ja ļoti lielas tiešsaistes platformas, kā noteikts Regulas [atsauce uz DSA regulu] 25. panta 1. punktā, pieprasa lietotājiem autentificēties, lai tie varētu piekļūt tiešsaistes pakalpojumiem, šīm platformām vajadzētu būt pilnvarotām pieņemt Eiropas digitālās identitātes maku lietošanu pēc lietotāja brīvprātīga pieprasījuma. Lietotājiem nevajadzētu būt pienākumam izmantot maku, lai piekļūtu privātiem pakalpojumiem, taču, ja viņi to vēlas, lielām tiešsaistes platformām šim nolūkam būtu jāpieņem Eiropas digitālās identitātes maks, vienlaikus ievērojot datu minimizēšanas principu. Ņemot vērā ļoti lielu tiešsaistes platformu nozīmi to pieejamības dēļ, jo īpaši, ja tā izteikta pakalpojuma saņēmēju un ekonomisko darījumu skaitā, ir jāuzlabo lietotāju aizsardzība pret krāpšanu un jānodrošina augsts datu aizsardzības līmenis. Savienības līmenī būtu jāizstrādā pašregulācijas rīcības kodeksi ("rīcības kodeksi"), ar kuriem veicina elektroniskās identifikācijas līdzekļu, tostarp Eiropas digitālās identitātes maku, plašu pieejamību un lietojamību 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. Tie būtu jāizstrādā 12 mēnešos pēc šīs regulas pieņemšanas. Komisijai 24 mēnešos pēc to ieviešanas būtu jānovērtē šo noteikumu efektivitāte attiecībā uz Eiropas digitālās identitātes maku pieejamību lietotājiem un lietojamību.

(29) Selektīva atklāšana ir jēdziens, kas datu īpašniekam dod iespēju atklāt tikai atsevišķas daļas no plašākas datu kopas, lai saņēmēja struktūra saņemtu vienīgi nepieciešamo informāciju, piemēram, lai datu īpašnieks atkarīgajai personai atklātu vienīgi tos datus, kuri ir nepieciešami, lai sniegtu lietotāja pieprasīto pakalpojumu. Eiropas digitālās identitātes makam tehniski būtu jādod iespēja selektīvi atklāt atribūtus atkarīgām personām. Tādus selektīvi atklātus atribūtus, tostarp, ja tie sākotnēji veido daļu no vairākiem atšķirīgiem elektroniskiem apliecinājumiem, vēlāk var apvienot un izsniegt atkarīgajām personām. Šī funkcija ir kļuvusi par galveno struktūras elementu, tādējādi uzlabojot ērtību un personas datu aizsardzību, tostarp datu minimizēšanu.

(30) Atribūti, ko kvalificētu uzticamības pakalpojumu sniedzēji nodrošina kā kvalificētas atribūtu apliecināšanas daļu, būtu jāpārbauda, salīdzinot ar autentiskiem avotiem, vai nu tieši kvalificētam uzticamības pakalpojumu sniedzējam, vai ar valsts līmenī norīkotu starpnieku starpniecību saskaņā ar valsts vai Savienības tiesību aktiem, nolūkā veikt drošu apliecinātu atribūtu apmaiņu starp identitātes vai atribūtu apliecināšanas pakalpojumu sniedzējiem un atkarīgajām personām. Dalībvalstīm valsts līmenī būtu jāizveido pienācīgi mehānismi, lai nodrošinātu, ka kvalificētu uzticamības pakalpojumu sniedzēji, kuri izsniedz kvalificētus atribūtu elektroniskos apliecinājumus, var ar tās personas piekrišanu, kurai apliecinājums izsniegts, pārbaudīt atribūtu autentiskumu, izmantojot autentiskus avotus. Pienācīgi mehānismi var ietvert īpašu starpnieku vai tehnisku risinājumu izmantošanu saskaņā ar valsts tiesību aktiem, kas ļauj piekļūt autentiskiem avotiem. Mehānisma pieejamības nodrošināšanai, kas ļaus veikt atribūtu pārbaudi pret autentiskiem avotiem, vajadzētu sekmēt, ka kvalificētu uzticamības pakalpojumu sniedzēji, kuri izsniedz kvalificētu atribūtu elektronisko apliecinājumu, ievēro savus pienākumus, kas izklāstīti šajā regulā.
VI pielikumā ir ietverts 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 pret attiecīgo autentisko avotu. Dalībvalstīm būtu jāvienojas par konkrētiem atribūtiem, kas ietilpst šajās kategorijās.

(31) Drošai elektroniskai identifikācijai un atribūtu apliecināšanas nodrošināšanai būtu jāsniedz papildu elastība un risinājumi finanšu pakalpojumu nozarē, lai varētu identificēt klientus un apmainīties ar īpašiem 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 stingru klientu autentifikācijas prasību izpildi attiecībā uz tiešsaistes identifikāciju, lai pieteiktos kontā, un darījumu uzsākšanu maksājumu pakalpojumu jomā.

(31.a) Lai nodrošinātu konsekventu sertifikācijas praksi visā ES, Komisijai vajadzētu izdot pamatnostādnes par kvalificēta elektroniskā paraksta radīšanas ierīču un kvalificēta elektroniskā zīmoga radīšanas ierīču sertifikāciju un atkārtotu sertifikāciju, tostarp par to derīgumu un termiņiem. Šī regula neliedz dalībvalstīm atļaut publiskām vai privātām struktūrām, kurām ir sertificētas kvalificēta elektroniskā paraksta radīšanas ierīces, uz laiku pagarināt sertifikāta derīguma termiņu, ja likumīgi noteiktajā termiņā nebija iespējams veikt šīs ierīces atkārtotu sertifikāciju, kam par pamatu ir cits iemesls, kas nav pārkāpums vai ar drošību saistīts incidents, un neskarot piemērojamo sertifikācijas praksi.

(32) Tīmekļa vietņu autentifikācijas pakalpojumi sniedz lietotājiem augsta līmeņa pārliecību, ka par šo tīmekļa vietni atbild īsta un likumīga vienība, neatkarīgi no platformas, kas tiek izmantota tā attēlošanai. Minētie pakalpojumi palīdz veidot uzticēšanos un ticamību, veicot darījumdarbību tiešsaistē un samazinot krāpšanas gadījumu skaitu tiešsaistē. Tīmekļa vietņu autentifikācijas pakalpojumu lietošanai tīmekļa vietnēs vajadzētu būt brīvprātīgai. Tomēr, lai tīmekļa vietņu autentifikācija kļūtu par veidu, kā palielināt uzticēšanos, sniedzot labāku pieredzi lietotājam un turpmāku izaugsmi iekšējā tirgū, ar šo regulu tīmekļa vietņu autentifikācijas pakalpojumu sniedzējiem un to sniegtajiem pakalpojumiem vajadzētu noteikt minimālos drošības un atbildības pienākumus. Šajā nolūkā tīmekļa pārlūkprogrammu nodrošinātājiem būtu jānodrošina atbalsts un sadarbspēja ar kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem saskaņā ar Regulu (ES) Nr. 910/2014. Tiem būtu jāatzīst kvalificēti tīmekļa vietņu autentifikācijas sertifikāti un jāļauj pārlūkprogrammas vidē uzrādīt galalietotājam sertificētus identitātes datus, pamatojoties uz specifikācijām, kas izklāstītas saskaņā ar šo regulu. Kvalificēta tīmekļa vietņu autentifikācijas sertifikāta atzīšanai par kvalificēta uzticamības pakalpojuma sniedzēja izsniegtu kvalificētu sertifikātu vajadzētu nodrošināt, ka šajā sertifikātā ietvertos identitātes datus var autentificēt un pārbaudīt saskaņā ar šo regulu. Tam nevajadzētu ietekmēt tīmekļa pārlūkprogrammu nodrošinātāju iespējas risināt būtiskas ar drošības pārkāpumu un atsevišķu sertifikātu integritātes zudumu saistītas neatbilstības, tādējādi uzlabojot galalietotāju drošību tiešsaistē. Lai vēl vairāk aizsargātu pilsoņus un veicinātu kvalificētu tīmekļa vietņu autentifikācijas sertifikātu lietošanu, dalībvalstu iestādēm būtu jāapsver to iekļaušana savās tīmekļa vietnēs.

(33) Daudzas dalībvalstis ir ieviesušas valsts prasības drošas un uzticamas digitālās arhivēšanas pakalpojumiem, lai ilgtermiņā saglabātu elektroniskos dokumentus un saistītos uzticamības pakalpojumus. Lai nodrošinātu juridisko noteiktību, uzticēšanos un saskaņošanu visās dalībvalstīs, būtu jāizveido tiesisks regulējums kvalificētiem elektroniskās arhivēšanas pakalpojumiem, iedvesmojoties no citu šajā regulā izklāstīto uzticamības pakalpojumu regulējuma. Šim regulējumam būtu jāpiedāvā uzticamības pakalpojumu sniedzējiem un lietotājiem efektīvs instrumentu kopums, kas ietver funkcionālas prasības elektroniskās arhivēšanas pakalpojumam, kā arī skaidras juridiskās sekas, ja tiek izmantots kvalificēts elektroniskās arhivēšanas pakalpojums. Šie noteikumi būtu jāpiemēro elektroniski iegūtiem dokumentiem, kā arī papīra dokumentiem, kas ir skenēti un digitalizēti. Vajadzības gadījumā šiem noteikumiem būtu jāļauj saglabātos elektroniskos datus pārnest uz dažādiem datu nesējiem vai formātiem, lai pagarinātu to ilgizturību un salasāmību pēc tehnoloģiskā derīguma termiņa beigām, vienlaikus pēc iespējas samazinot zudumus un izmaiņas. Ja elektroniskie dati, kas iesniegti digitālās 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, kas izveidoti ar šo regulu. Lai izveidotu saglabāšanas pierādījumus, kuros izmanto elektroniskos parakstus, elektroniskos zīmogus vai elektroniskos laika zīmogus, būtu jāizmanto kvalificēti elektroniskie uzticamības pakalpojumi. Ciktāl elektroniskās arhivēšanas pakalpojumi nav saskaņoti ar šo regulu, dalībvalstis saskaņā ar Savienības tiesību aktiem var saglabāt vai ieviest valsts noteikumus attiecībā uz minētajiem pakalpojumiem, piemēram, īpašus noteikumus, kas pieļauj dažas atkāpes attiecībā uz pakalpojumiem, kuri integrēti organizācijā un kurus stingri izmanto šīs organizācijas "iekšējiem arhīviem". Šajā regulā nevajadzētu nošķirt elektroniski iegūtus dokumentus no fiziskiem dokumentiem, kas ir digitalizēti.

(33.a) Valstu arhīvu un atmiņas iestādes kā organizācijas, kas nodarbojas ar dokumentārā mantojuma saglabāšanu sabiedrības interesēs, parasti ir pilnvarotas veikt savu darbību saskaņā ar valsts tiesību aktiem, un tās ne vienmēr sniedz uzticamības pakalpojumus šīs regulas nozīmē. Ciktāl šīs iestādes nesniedz šādus pakalpojumus, šī regula neskar to darbību.

(34) Elektroniskās virsgrāmatas ir elektronisko datu ierakstu sekvence, kas nodrošina to integritāti un hronoloģiskās secības precizitāti. Elektronisko virsgrāmatu mērķis ir izveidot datu ierakstu hronoloģisko secību, lai nepieļautu, ka digitālie aktīvi tiek kopēti un pārdoti vairākiem saņēmējiem. Elektroniskās virsgrāmatas var izmantot, piemēram, digitālajiem īpašumtiesību ierakstiem globālajā tirdzniecībā, piegādes ķēdes finansēšanai, intelektuālā īpašuma tiesību vai preču, piemēram, elektroenerģijas, digitalizācijai. Kopā ar citām tehnoloģijām tās var palīdzēt rast risinājumus efektīvākiem un pārveidojošākiem sabiedriskajiem pakalpojumiem, piemēram, e-balsošana, muitas iestāžu pārrobežu sadarbība, akadēmisko iestāžu pārrobežu sadarbība vai nekustamā īpašuma īpašumtiesību reģistrēšana decentralizētos zemes reģistros. Kvalificētas elektroniskās virsgrāmatas rada juridisku prezumpciju par datu ierakstu unikālu un precīzu secīgu hronoloģisku secību un integritāti virsgrāmatā. Elektronisko virsgrāmatu īpašās iezīmes, proti, datu ierakstu secīgā hronoloģiskā secība, nošķir elektroniskās virsgrāmatas no citiem uzticamības pakalpojumiem, piemēram, elektroniskiem laika zīmogiem un elektroniski reģistrētiem piegādes pakalpojumiem. Proti, ne digitālo dokumentu zīmogošana laikā, ne to nosūtīšana, izmantojot elektroniski reģistrētus piegādes pakalpojumus, bez turpmākiem tehniskiem vai organizatoriskiem pasākumiem nevarētu pietiekami kavēt viena un tā paša digitālā aktīva kopēšanu un pārdošanu dažādām pusēm vairāk nekā vienu reizi. Elektroniskās virsgrāmatas izveides un atjaunināšanas process ir atkarīgs no izmantotās virsgrāmatas veida (centralizēta vai izkliedēta).

(35) Lai novērstu iekšējā tirgus sadrumstalotību, būtu jāizveido Eiropas mēroga tiesiskais regulējums, kas ļautu pārrobežu līmenī atzīt uzticamības pakalpojumus datu reģistrēšanai kvalificētās elektroniskās virsgrāmatās. Elektronisko virsgrāmatu uzticamības pakalpojumu sniedzēji būtu jāpilnvaro pārbaudīt datu secīgu reģistrēšanu virsgrāmatā. Šī regula neskar jebkādas juridiskās saistības, kas saskaņā ar Savienības un valsts tiesību aktiem var būt jāievēro, izmantojot elektroniskās virsgrāmatas. Piemēram izmantošanas gadījumiem, kas saistīti ar personas datu apstrādi, būtu jāatbilst Regulai (ES) 2016/679. Izmantošanas gadījumiem, kas saistīti ar kriptoaktīviem, vajadzētu būt saderīgiem ar visiem piemērojamiem finanšu noteikumiem, tostarp, piemēram, Finanšu instrumentu tirgu direktīvu [11], Maksājumu pakalpojumu direktīvu [12], E-naudas direktīvu [13], kā arī ar iespējamiem turpmākiem tiesību aktiem par kriptoaktīvu tirgiem un nelikumīgi iegūtu līdzekļu legalizācijas novēršanas noteikumiem, kurus varētu iekļaut līdzekļu pārvedumu regulā [14] un varētu pieprasīt kriptoaktīvu pakalpojumu sniedzējiem pārbaudīt elektronisko virsgrāmatu lietotāju identitāti, lai nodrošinātu atbilstību starptautiskajiem nelikumīgi iegūtu līdzekļu legalizācijas novēršanas standartiem.

---

11 Eiropas Parlamenta un Padomes Direktīva 2014/65/ES (2014. gada 15. maijs) par finanšu instrumentu tirgiem un ar kuru groza Direktīvu 2002/92/EK (OV L 173, 12.6.2014., 349.–496. lpp.).

12 Eiropas Parlamenta un Padomes Direktīva (ES) 2015/2366 (2015. gada 25. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (OV L 337, 23.12.2015., 35.–127. lpp.).

13 Eiropas Parlamenta un Padomes Direktīva 2009/110/EK (2009. gada 16. septembris) par elektroniskās naudas iestāžu darbības sākšanu, veikšanu un konsultatīvu uzraudzību, par grozījumiem Direktīvā 2005/60/EK un Direktīvā 2006/48/EK un par Direktīvas 2000/46/EK atcelšanu (OV L 267, 10.10.2009., 7.–17. lpp.).

14 Sk. Komisijas 2021. gada 20. jūlija priekšlikumu pārstrādāt Eiropas Parlamenta un Padomes Regulu (ES) 2015/847 (2015. gada 20. maijs) par līdzekļu pārvedumiem pievienoto informāciju, COM/2021/422 final.

(36) Lai izvairītos no sadrumstalotības un šķēršļiem atšķirīgo standartu un tehnisko ierobežojumu dēļ un lai nodrošinātu koordinētu procesu, lai neapdraudētu nākotnes Eiropas digitālās identitātes regulējuma īstenošanu, ir vajadzīgs Komisijas, dalībvalstu un privātā sektora ciešas un strukturētas sadarbības process. Lai sasniegtu šo mērķi, dalībvalstīm būtu jāsadarbojas atbilstīgi Komisijas ieteikumā XXX/XXXX [Rīkkopa saskaņotai pieejai Eiropas digitālās identitātes regulējumam] [15] paredzētajam regulējumam nolūkā noteikt rīkkopu Eiropas digitālās identitātes regulējumam. Rīkkopā būtu jāietver visaptveroša tehniskā arhitektūra un atsauču regulējums, kopīgu standartu un tehnisko atsauču kopums, kā arī pamatnostādņu un paraugprakses aprakstu kopums, kas aptver vismaz visus Eiropas digitālās identitātes maka, tostarp e-parakstu, kā arī kvalificēta atribūtu apliecināšanas uzticamības pakalpojuma funkciju un sadarbspējas aspektus, kā noteikts šajā regulā. Šajā saistībā dalībvalstīm būtu arī jāpanāk vienošanās par kopīgiem uzņēmējdarbības modeļa elementiem un Eiropas digitālās identitātes maka maksājumu struktūru, lai atvieglotu ieviešanu, jo īpaši maziem un vidējiem uzņēmumiem pārrobežu kontekstā. Rīkkopas saturam būtu jāattīstās vienlaikus ar Eiropas digitālās identitātes regulējuma apspriešanas un pieņemšanas procesa rezultātu un tas jāataino.

(36.a) Dalībvalstīm būtu jāparedz noteikumi par sankcijām par pārkāpumiem, piemēram, tiešu vai netiešu praksi, kas rada nekvalificētu un kvalificētu uzticamības pakalpojumu sajaukšanu vai ES uzticamības zīmes ļaunprātīgu izmantošanu, ko veic nekvalificēti uzticamības pakalpojumu sniedzēji. ES uzticamības zīmi nevajadzētu izmantot apstākļos, kas tieši vai netieši liek domāt, ka visi šā pakalpojumu sniedzēja piedāvātie nekvalificētie uzticamības pakalpojumi ir kvalificēti.

[15] [Pievienot atsauci, tiklīdz tā ir pieņemta.]

(36.b) Šai regulai būtu jānodrošina kvalificēto uzticamības pakalpojumu saskaņots kvalitātes, uzticamības un drošības līmenis neatkarīgi no darbības veikšanas vietas. Tādējādi kvalificētam uzticamības pakalpojumu sniedzējam būtu jāļauj izmantot ārpakalpojumus savām darbībām, kas saistītas ar kvalificēta uzticamības pakalpojuma sniegšanu ārpus Savienības, ja tas sniedz garantijas, nodrošinot, ka uzraudzības darbības un revīzijas var īstenot tā, it kā šīs darbības tiktu veiktas Savienībā. Ja nav iespējams pilnībā nodrošināt atbilstību regulai, uzraudzības iestādēm vajadzētu būt iespējai pieņemt samērīgus un pamatotus pasākumus, tostarp atcelt sniegtā uzticamības pakalpojuma kvalificēto statusu.

(36.c) Lai nodrošinātu juridisko noteiktību attiecībā uz tādu uzlabotu elektronisko parakstu derīgumu, kuru pamatā ir kvalificēti sertifikāti, ir svarīgi precizēt uz kvalificētiem sertifikātiem balstīta uzlabota elektroniskā paraksta komponentus, kas būtu jānovērtē pārbaudītājam, kurš veic minētā paraksta validēšanu.

(36.d) Uzticamības pakalpojumu sniedzējiem būtu jāizmanto kriptogrāfijas algoritmi, kas atspoguļo pašreizējo paraugpraksi un šo algoritmu uzticamu īstenošanu, lai nodrošinātu savu uzticamības pakalpojumu drošību un uzticamību.

(36.e) Šajā regulā būtu jānosaka kvalificētu uzticamības pakalpojumu sniedzēju pienākums pārbaudīt tās fiziskās vai juridiskās personas identitāti, kurai ir izdots kvalificētais sertifikāts, pamatojoties uz dažādām saskaņotām metodēm visā ES. Šāda metode var ietvert paļaušanos uz elektroniskās identifikācijas līdzekļiem, kas atbilst ticamības līmeņa "būtisks" prasībām apvienojumā ar saskaņotām papildu attālinātām procedūrām, kas nodrošina personas identifikāciju ar augstu ticamības līmeni.

(36.f) Eiropas digitālās identitātes maku emitenti un paziņoto elektroniskās identifikācijas līdzekļu emitenti, kas rīkojas komerciālā vai profesionālā statusā un izmanto vārtziņu piedāvātos platformas pamatpakalpojumus nolūkā nodrošināt preces un pakalpojumus galalietotājiem vai tos izmanto šādas nodrošināšanas laikā, būtu jāuzskata par komerciālajiem lietotājiem saskaņā ar Regulas (ES) 2022/1925 2. panta 21. punktu. Tāpēc būtu jāpieprasa, lai vārtziņi bez maksas nodrošinātu efektīvu sadarbspēju ar tām pašām operētājsistēmu, aparatūras vai programmatūras funkcijām, kas ir pieejamas vai tiek izmantotas, nodrošinot savus papildu un atbalsta pakalpojumus un aparatūru, un piekļuvi tām sadarbspējas nolūkā. Tam būtu jāļauj Eiropas digitālās identitātes maku emitentiem un paziņoto elektroniskās identifikācijas līdzekļu emitentiem, izmantojot saskarnes vai līdzīgus risinājumus, savienoties ar attiecīgajām funkcijām tikpat efektīvi kā paša vārtziņa pakalpojumi vai aparatūra.

(36.g) Lai nodrošinātu šīs regulas atbilstību pašreizējām norisēm un ievērotu praksi iekšējā tirgū, Komisijas pieņemtie deleģētie un īstenošanas akti būtu regulāri jāpārskata un vajadzības gadījumā jāatjaunina. Šo atjauninājumu nepieciešamības novērtējumā būtu jāņem vērā jaunās tehnoloģijas, prakse, standarti vai tehniskās specifikācijas, kas ieviestas iekšējā tirgū.

(37) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1525 [16] 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju.

(38) Tāpēc Regula (ES) 910/2014 būtu attiecīgi jāgroza,

---

[16] 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.).

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Regulu (ES) Nr. 910/2014 groza šādi:

(1) regulas 1. pantu aizstāj ar šādu:

"Šīs regulas mērķis ir nodrošināt iekšējā tirgus pienācīgu darbību, vienlaikus cenšoties panākt elektroniskās identifikācijas līdzekļu un uzticamības pakalpojumu pienācīgu drošības līmeni. Šajā nolūkā šajā regulā:

aa) tiek izklāstīti nosacījumi, saskaņā ar kuriem dalībvalstis nodrošina un atzīst fizisku un juridisku personu elektroniskās identifikācijas līdzekļus, kuri ietverti citas dalībvalsts paziņotajā elektroniskās identifikācijas shēmā;

ab) tiek izklāstīti nosacījumi, saskaņā ar kuriem dalībvalstis nodrošina un atzīst Eiropas digitālās identitātes makus;

b) tiek izklāstīti noteikumi par uzticamības pakalpojumiem, jo īpaši attiecībā uz elektroniskiem darījumiem;

c) tiek izveidots tiesiskais regulējums attiecībā uz elektroniskajiem parakstiem, elektroniskajiem zīmogiem, elektroniskajiem laika zīmogiem, elektroniskajiem dokumentiem, elektroniskajiem piegādes pakalpojumiem, sertifikācijas pakalpojumiem tīmekļa vietņu autentifikācijai, elektronisko parakstu, elektronisko zīmogu un to sertifikātu elektronisko validāciju, tīmekļa vietņu autentifikācijas sertifikātu elektronisko validēšanu, elektronisko parakstu, elektronisko zīmogu un to sertifikātu elektronisko saglabāšanu, elektronisko arhivēšanu, atribūtu elektronisko apliecinājumu, kvalificēta attālināta elektroniskā paraksta un 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 ir paziņojušas dalībvalstis, Eiropas digitālās identitātes makiem, kurus izdod dalībvalstis, un uzticamības pakalpojumu sniedzējiem, kas veic uzņēmējdarbību Savienībā.";

b) panta 3. punktu aizstāj ar šādu:

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

(3) regulas 3. pantu groza šādi:

X) panta 1) punktu aizstāj ar šādu:

"(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 fizisku vai juridisku personu;";

a) panta 2) punktu aizstāj ar šādu:

"(2) "elektroniskās identifikācijas līdzekļi" ir materiāli un/vai nemateriāli elementi, tostarp Eiropas digitālās identitātes maki, kas ietver personas identifikācijas datus un ko izmanto, lai autentificētos tiešsaistes pakalpojumam vai attiecīgā gadījumā bezsaistes pakalpojumam;";

aa) panta 3) punktu aizstāj ar šādu:

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

b) panta 4) punktu aizstāj ar šādu:

"(4) "elektroniskās identifikācijas shēma" ir elektroniskās identifikācijas sistēma, kurā elektroniskās identifikācijas līdzekļus izsniedz fiziskām vai juridiskām personām vai tādām fiziskām personām, kas pārstāv fiziskas vai juridiskas personas;";

ba) panta 5) punktu aizstāj ar šādu:

(5) "autentifikācija" ir elektronisks process, kas dara iespējamu fiziskas vai juridiskas personas elektronisko identifikāciju vai elektronisko datu izcelsmes un integritātes apstiprināšanu;";

bb) iekļauj šādu 5.a) punktu:

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

c) panta 14) punktu aizstāj ar šādu:

"14) "elektroniskā paraksta sertifikāts" ir elektronisks apliecinājums, kas saista elektroniskā paraksta validācijas datus ar fizisku personu un apliecina vismaz minētās personas vārdu vai pseidonīmu;";

d) panta 16) punktu aizstāj ar šādu:

"16) "uzticamības pakalpojums" ir elektronisks pakalpojums, parasti par atlīdzību, kas ietver:

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

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

b) elektronisko parakstu vai elektronisko zīmogu radīšanu;

c) elektronisko parakstu vai elektronisko zīmogu validāciju;

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

e) attālinātas kvalificēta elektroniskā paraksta radīšanas ierīču vai attālinātas kvalificēta elektroniskā zīmoga radīšanas ierīču pārvaldību;

f) atribūtu elektronisko apliecinājumu izsniegšanu;

fa) atribūtu elektroniskā apliecinājuma validāciju;

g) elektronisko laika zīmogu izveidi;

ga) elektronisko laika zīmogu validāciju;

gb) elektroniski reģistrētu piegādes pakalpojumu sniegšanu;

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

h) elektronisko datu elektronisko arhivēšanu; vai

i) elektronisko datu reģistrēšanu elektroniskajā virsgrāmatā;";

da) panta 18) punktu aizstāj ar šādu:

"atbilstības novērtēšanas struktūra" ir Regulas (EK) Nr. 765/2008 2. panta 13. punktā definēta struktūra, 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;";

e) panta 21) punktu aizstāj ar šādu:

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

f) iekļauj šādu 23.a) un 23.b) punktu:

"23.a) "attālināta 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) "attālināta 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;";

g) panta 29) punktu aizstāj ar šādu:

"29) "elektroniskā zīmoga sertifikāts" ir elektronisks apliecinājums, kas saista elektroniskā zīmoga validācijas datus ar juridisku personu un apliecina minētās personas nosaukumu;";

h) panta 41) punktu aizstāj ar šādu:

"41) "validācija" ir process, kurā pārbauda un apstiprina, ka dati elektroniskā formā ir derīgi saskaņā ar šīs regulas prasībām;";

i) pievieno šādu 42) līdz 55.b) punktu:

"42) "Eiropas digitālās identitātes maks" ir elektroniskās identifikācijas līdzeklis, kas lietotājam ļauj glabāt un izgūt identitātes datus, tostarp personas identifikācijas datus, ar viņu identitāti saistītu atribūtu elektroniskus apliecinājumus, pēc pieprasījuma sniegt tos atkarīgajām pusēm un izmantot tos autentifikācijai tiešsaistē un attiecīgā gadījumā bezsaistē pakalpojumam saskaņā ar 6.a pantu; ļauj parakstīt ar kvalificētu elektronisko parakstu un zīmogu, izmantojot kvalificētus elektroniskos zīmogus;

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

44) "atribūtu elektroniskais apliecinājums" ir apliecinājums elektroniskā formā, kas ļauj autentificēt atribūtus;

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

45.a) "atribūtu elektroniskais apliecinājums, ko izdevusi par autentisku avotu atbildīga publiskā sektora struktūra vai kas izdots tās vārdā" ir atribūtu elektroniski apliecinājumi, 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.da pantu un atbilst VII pielikumā noteiktajām prasībām;

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

47) "elektroniska arhivēšana" ir pakalpojums, kas nodrošina elektronisko datu saņemšanu, glabāšanu, izguvi un dzēšanu, lai garantētu to ilgizturību un salasāmību, kā arī saglabātu to integritāti, konfidencialitāti un izcelsmes apliecinājumu visā saglabāšanas periodā;

48) "kvalificēts elektroniskās arhivēšanas pakalpojums" ir elektroniskās arhivēšanas pakalpojums, kas atbilst 45.g pantā noteiktajām prasībām;

49) "ES digitālās identitātes maka uzticamības marķējums" ir vienkārša, atpazīstama un skaidra norāde, ka Eiropas digitālās identitātes maks ir izdots saskaņā ar šo regulu;

50) "droša lietotāja autentificēšana" ir autentificēšana, izmantojot vismaz divus autentifikācijas faktorus no dažādām kategorijām, kas ir zināšanas (kaut kas ir tikai lietotājam zināms), valdījums (tas, kas ir tikai lietotāja valdījumā) vai neatņemamas īpašības (lietotājam raksturīgas īpašības) un kas ir savstarpēji neatkarīgi, proti, neatbilstība vienam kritērijam neapdraud pārējo elementu uzticamību, un kas ir izstrādāti tā, lai nodrošinātu autentificēšanas datu konfidencialitātes aizsardzību;

53) "elektroniskā virsgrāmata" ir elektronisko datu ierakstu sekvence, kas nodrošina to integritāti un hronoloģiskās secības precizitāti;

53.a) "kvalificēta elektroniskā virsgrāmata" ir elektroniskā virsgrāmata, kas atbilst 45.i pantā noteiktajām prasībām;

54) "personas dati" ir jebkura informācija, kas definēta Regulas (ES) 2016/679 4. panta 1. punktā;

55) "reģistrācijas saskaņošana" ir process, kurā personas identifikācijas dati, personas identifikācijas līdzekļi, kvalificēti elektroniski apliecinājumi par atribūtiem vai atribūtu apliecinājumi, ko izdevusi publiskā sektora struktūra, kura ir atbildīga par autentisku avotu vai kas izdoti tās vārdā, ir saskaņoti vai sasaistīti ar esošu kontu, kas pieder tai pašai personai;

55.a) "unikāls un pastāvīgs identifikators" ir identifikators, kas var sastāvēt no atsevišķiem vai vairākiem valsts vai nozares identifikācijas datiem, ir saistīts ar vienu lietotāju konkrētā sistēmā un ir pastāvīgs laikā;

55.b) "datu ieraksts" ir elektroniski dati, kas reģistrēti ar saistītiem metadatiem (vai atribūtiem), kuri atbalsta datu apstrādi;

55.c) "Eiropas digitālās identitātes maku izmantošana bezsaistē" ir mijiedarbība starp lietotāju un atkarīgo pusi fiziskā atrašanās vietā, kad makam mijiedarbības nolūkā nav jāpiekļūst attālinātām sistēmām, izmantojot elektronisko sakaru tīklus."

"|*5. pants*

Pseidonīmi elektroniskā darījumā

Neskarot juridiskās sekas, kas atbilstīgi valsts tiesību aktiem ir pseidonīmiem, pseidonīmu izmantošana elektroniskos darījumos nav aizliegta.";

5) II nodaļā pirms 6.a panta iekļauj šādu virsrakstu:

"I IEDAĻA

Eiropas digitālās identitātes maks";

7) regulā iekļauj šādu 6.a, 6.b, 6.c un 6.d pantu:

"*6.a pants*

Eiropas digitālās identitātes maki

1. Lai nodrošinātu, ka visām fiziskām un juridiskām personām Savienībā ir droša, uzticama un netraucēta piekļuve publiskiem un privātiem pārrobežu pakalpojumiem, katra dalībvalsts 24 mēnešu laikā pēc 11. punktā un 6.c panta 4. punktā minēto īstenošanas aktu stāšanās spēkā izdod Eiropas digitālās identitātes maku.

2. Eiropas digitālās identitātes makus izdod:

   a) dalībvalsts;

   b) atbilstīgi dalībvalsts pilnvarojumam; vai

   c) neatkarīgi no dalībvalsts, bet dalībvalsts tos atzīst.

3. Eiropas digitālās identitātes maki ir elektroniskās identifikācijas līdzekļi, kas ļauj lietotājam pārredzamā un izsekojamā veidā:

   a) droši pieprasīt, atlasīt, apvienot, glabāt, dzēst un iesniegt atribūtu un personas identifikācijas datu elektronisko apliecinājumu atkarīgajām pusēm, tostarp autentificēt tiešsaistē un attiecīgā gadījumā bezsaistē, lai izmantotu publiskos un privātos pakalpojumus, vienlaikus nodrošinot, ka ir iespējama datu selektīva izpaušana;

   b) parakstīt ar kvalificētu elektronisko parakstu un zīmogu, izmantojot kvalificētus elektroniskos zīmogus.

4. Digitālās identitātes maki jo īpaši:

a) nodrošina kopīgu saskarni:

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

(2) atkarīgajām pusēm personas identifikācijas datu un atribūtu elektronisko apliecinājumu pieprasīšanai;

(3) personas identifikācijas datu vai atribūtu elektroniska apliecinājuma sniegšanai atkarīgajām pusēm tiešsaistē un attiecīgā gadījumā arī bezsaistē;

(4) lietotājiem mijiedarbībai ar Eiropas digitālās identitātes maku un ES digitālās identitātes maka uzticamības marķējuma attēlošanai;

b) nesniedz uzticamības pakalpojumu sniedzējiem atribūtu elektronisko apliecinājumu informāciju par šo atribūtu izmantošanu pēc to izdošanas;

ba) nodrošina, ka atkarīgo pušu identitāti var apstiprināt, īstenojot autentifikācijas mehānismus saskaņā ar 6.b pantu;

c) atbilst 8. pantā noteiktajām prasībām attiecībā uz augstu uzticamības līmeni, ko *mutatis mutandis* piemēro personas identifikācijas datu pārvaldībai un izmantošanai ar maka starpniecību, tostarp elektroniskajai identifikācijai un autentifikācijai;

e) nodrošina, ka 12. panta 4. punkta d) apakšpunktā minētie personas identifikācijas dati unikāli un pastāvīgi pārstāv fizisko personu, juridisko personu vai fizisko personu, kas pārstāv fizisko vai juridisko personu, kura ir saistīta ar maku.

4.a Dalībvalstis paredz procedūras, kas ļauj lietotājam ziņot par sava maka iespējamu pazaudēšanu vai ļaunprātīgu izmantošanu un pieprasīt tā atsaukšanu.

5. Dalībvalstis nodrošina Eiropas digitālās identitātes maku validācijas mehānismus, ar kuriem:

a) nodrošina, ka var verificēt to autentiskumu un derīgumu;

d) ļauj lietotājam autentificēt atkarīgās puses saskaņā ar 6.b pantu.

6. Eiropas digitālās identitātes makus izdod saskaņā ar paziņotu augsta uzticamības līmeņa elektroniskās identifikācijas shēmu.

6.a Fiziskām personām Eiropas digitālās identitātes maku izsniegšana, izmantošana autentifikācijai un atsaukšana ir bez maksas.

6.b Neskarot 6.db pantu, dalībvalstis saskaņā ar valsts tiesību aktiem var paredzēt Eiropas digitālās identitātes maku papildu funkcijas, tostarp sadarbspēju ar esošajiem valsts elektroniskās identifikācijas līdzekļiem.

7. Lietotāji pilnībā kontrolē Eiropas digitālās identitātes maka un Eiropas digitālās identitātes maka datu izmantošanu. Eiropas digitālās identitātes maka izdevējs nevāc tādu informāciju par maka izmantošanu, kas nav nepieciešama maka pakalpojumu sniegšanai, un personas identifikācijas datus un citus personas datus, kas tiek glabāti vai attiecas uz Eiropas digitālās identitātes maka izmantošanu, neapvieno ar tādiem personas datiem no citiem pakalpojumiem, ko piedāvā šis izdevējs, vai no trešo personu pakalpojumiem, kuri nav nepieciešami maka pakalpojumu sniegšanai, ja vien lietotājs to nav skaidri pieprasījis. Personas dati, kas attiecas uz Eiropas digitālās identitātes maku nodrošināšanu, būtu jāglabā loģiski nošķirti no jebkuriem citiem datiem, kas ir Eiropas digitālās identitātes maku emitenta rīcībā. Ja Eiropas digitālās identitātes maku nodrošina privāti subjekti saskaņā ar 2. punkta b) un c) apakšpunktu, *mutatis mutandis* piemēro 45.f panta 4. punkta noteikumus.

7.a Dalībvalstis bez nepamatotas kavēšanās paziņo Komisijai turpmāk minēto informāciju:

a) struktūru, kas saskaņā ar 6.b panta 2. punktu ir atbildīga par to paziņoto atkarīgo pušu saraksta izveidi un uzturēšanu, kuras izmanto Eiropas digitālās identitātes makus;

b) struktūrām, kas atbild par Eiropas digitālās identitātes maku izdošanu saskaņā ar 6.a panta 1. punktu;

c) struktūrām, kas atbild par to, lai personas identifikācijas dati būtu saistīti ar maku saskaņā ar 6.a panta 4. punkta e) apakšpunktu;

Paziņojumā arī sniedz informāciju par mehānismu, kas ļauj validēt 12. panta 4. punktā minētos personas identifikācijas datus un atkarīgo pušu identitāti.

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

8. Šīs regulas 11. pantu *mutatis mutandis* piemēro Eiropas digitālās identitātes makam.

9. Šīs regulas 24. panta 2. punkta b), e), g) un h) apakšpunktu *mutatis mutandis* piemēro Eiropas digitālās identitātes maku izdevējiem.

10. Eiropas digitālās identitātes maku dara piekļūstamu personām ar invaliditāti saskaņā ar Direktīvā (ES) 2019/882 noteiktajām piekļūstamības prasībām.

11. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija nosaka tehniskās un darbības specifikācijas un atsauces standartus 3., 4., 5. un 7.a punktā minētajām prasībām, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maka īstenošanu. Minēto īstenošanas aktu pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

11.a Komisija nosaka tehniskās un darbības specifikācijas, kā arī atsauces standartus, lai atvieglotu to lietotāju reģistrāciju Eiropas digitālās identitātes makā, kuri izmanto vai nu elektroniskās identifikācijas līdzekļus, kas atbilst "augstam" līmenim, vai elektroniskās identifikācijas līdzekļus, kas atbilst "būtiskam" līmenim, saistībā ar papildu attālinātas reģistrācijas procedūrām, kas kopā atbilst "augsta" uzticamības līmeņa prasībām. Minēto īstenošanas aktu pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

6.b pants

Eiropas digitālās identitātes maku atkarīgās puses

1. Ja atkarīgās puses, kas sniedz privātos vai publiskos pakalpojumus, plāno izmantot Eiropas digitālās identitātes makus, kas izdoti saskaņā ar šo regulu, tās par to paziņo dalībvalstij, kurā konkrētā atkarīgā puse veic uzņēmējdarbību.

1.a Paziņošanas procedūra ir rentabla un samērīga ar risku, un tā nodrošina, ka atkarīgās puses sniedz vismaz to informāciju, kas nepieciešama, lai autentificētos Eiropas digitālās identitātes makos. Tajā būtu jānorāda vismaz dalībvalsts, kurā tie veic uzņēmējdarbību, un atkarīgās puses nosaukums un, attiecīgā gadījumā, tās reģistrācijas numurs, kāds norādīts oficiālajos reģistros.

1.b Paziņošanas prasība neskar citas paziņošanas un reģistrācijas prasības saskaņā ar Savienības vai valsts tiesību aktiem, piemēram, tās, kas piemērojamas īpašām personas datu kategorijām, attiecībā uz kurām var būt nepieciešamas papildu atļaujas piešķiršanas prasības.

1.c Dalībvalstis var atbrīvot atkarīgās puses no paziņošanas prasības, ja Savienības vai valsts tiesību aktos nav paredzētas īpašas paziņošanas vai reģistrācijas prasības, lai piekļūtu informācijai, kas sniegta, izmantojot Eiropas digitālās identitātes maku. Atbrīvotajām atkarīgajām pusēm var nebūt nepieciešams autentificēties Eiropas digitālās identitātes makā.

1.d Atkarīgās puses, kurām sniegts paziņojums saskaņā ar šo pantu, nekavējoties informē dalībvalsti par jebkādām turpmākām izmaiņām sākotnēji sniegtajā informācijā.

2. Atkarīgās puses nodrošina 6.a panta 4. punkta ba) apakšpunktā minēto autentifikācijas mehānismu īstenošanu.

3. Atkarīgo pušu atbildībā ir veikt procedūru, ar ko autentificē personas un validē to atribūtu elektronisko apliecinājumu, kuru izcelsme ir no Eiropas digitālās identitātes makiem, kas izsniegti, izmantojot kopējo saskarni saskaņā ar 6.a panta 4. punkta a) apakšpunkta 2. punktu.

4. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija nosaka tehniskās un darbības specifikācijas 1., 1.a, un 1.d punktā minētajām prasībām, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 11. punktā. Minēto īstenošanas aktu pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

6.c pants

Eiropas digitālās identitātes maku sertifikācija

1. Eiropas digitālās identitātes maku atbilstību 6.a panta 3., 4. un 5. punktā noteiktajām prasībām, 6.a panta 7. punktā noteiktajai prasībai par loģisko nošķiršanu un attiecīgā gadījumā 6.a panta 11.a punktā noteiktajām prasībām sertificē atbilstības novērtēšanas struktūras, kas akreditētas saskaņā ar Kiberdrošības akta 60. pantu un shēmām, specifikācijām, standartiem un procedūrām, uz kurām atsaucas saskaņā ar 4. punkta a), aa) un aaa) apakšpunktu, un ko izraudzījušās dalībvalstis. Sertifikācija nepārsniedz piecus gadus ar nosacījumu, ka regulāri reizi divos gados tiek veikts neaizsargātības novērtējums. Ja neaizsargātības tiek konstatētas un netiek novērstas 3 mēnešu laikā, sertifikāciju anulē.

2. Attiecībā uz atbilstību 6.a panta 7. punktā minētajām datu aizsardzības prasībām sertifikāciju saskaņā ar 1. punktu var papildināt ar sertifikāciju saskaņā ar Regulas (ES) 2016/679 42. pantu.

3. Eiropas digitālās identitātes maku vai to daļu atbilstību attiecīgajām kiberdrošības prasībām, kas izklāstītas 6.a panta 3., 4., 5., 7. un attiecīgā gadījumā 11.a punktā, sertificē 1. punktā minētās atbilstības novērtēšanas struktūras saskaņā ar attiecīgajām kiberdrošības sertifikācijas shēmām, ievērojot Regulu (ES) 2019/881, jo uz tām ir atsauce saskaņā ar 4. punkta a) un aa) apakšpunktu.

3.a Uz sertificētiem Eiropas digitālās identitātes makiem neattiecas 7. un 9. pantā minētās prasības.

4. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka:

a) to kiberdrošības sertifikācijas shēmu sarakstu saskaņā ar Regulu (ES) 2019/881, kas nepieciešamas Eiropas digitālās identitātes maku sertifikācijai, kā minēts 3. punktā;

aa) specifikācijas, procedūras un atsauces standartus to izmantošanai saskaņā ar attiecīgajām kiberdrošības sertifikācijas shēmām, kas uzskaitītas saskaņā ar a) apakšpunktu;

aaa) 1. punktā minētās sertifikācijas nolūkā – to specifikāciju, procedūru un atsauces standartu sarakstu, ar kuriem nosaka kopīgas sertifikācijas prasības, kas nav iekļautas attiecīgajās kiberdrošības sertifikācijas shēmās saskaņā ar Regulu (ES) 2019/881, lai pierādītu, ka Eiropas digitālais identitātes maks atbilst 1. punktā minētajām prasībām;

b) tehniskās, procesuālās, organizatoriskās un darbības specifikācijas 1. punktā minēto atbilstības novērtēšanas struktūru iecelšanai un – attiecībā uz sertificēšanas prasībām, kas noteiktas saskaņā ar aaa) apakšpunktu – šo struktūru izmantoto sertifikācijas shēmu un saistīto novērtēšanas metožu, kā arī to izsniegto sertifikātu un sertifikācijas ziņojumu uzraudzībai un pārskatīšanai;

5. Dalībvalstis paziņo Komisijai 1. punktā minēto publisko vai privāto struktūru nosaukumus un adreses. Komisija minēto informāciju dara pieejamu dalībvalstīm.

6. Šā panta 4. punktā minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

6.d pants

Sertificēto Eiropas digitālās identitātes maku saraksta publicēšana

1. Dalībvalstis bez nepamatotas kavēšanās informē Komisiju par Eiropas digitālās identitātes makiem, kas izdoti saskaņā ar 6.a pantu un ko sertificējušas 6.c panta 1. punktā minētās struktūras. Tās arī bez nepamatotas kavēšanās informē Komisiju par sertifikācijas anulēšanu.

2. Pamatojoties uz saņemto informāciju, Komisija izveido, publicē un atjaunina mašīnlasāmu sarakstu, kurā uzskaitīti sertificētie Eiropas digitālās identitātes maki.

3. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija nosaka 1. un 2. punkta vajadzībām piemērojamos formātus un procedūras, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 11. punktā. Minēto īstenošanas aktu pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

6.da pants

Eiropas digitālās identitātes maku drošības prasību pārkāpums

1. Ja attiecībā uz Eiropas digitālās identitātes makiem, kas izdoti saskaņā ar 6.a pantu, vai 6.a panta 5. punkta a), d) vai e) apakšpunktā minētajiem validācijas mehānismiem ir noticis pārkāpums vai tie daļēji kompromitēti tādā veidā, kas ietekmē to uzticamību vai citu Eiropas digitālās identitātes maku uzticamību, attiecīgo maku izdevējs bez nepamatotas kavēšanās aptur Eiropas digitālās identitātes maka izdošanu un atsauc tā izmantošanu. Dalībvalsts, kurā attiecīgie maki tika izdoti, bez liekas kavēšanās informē dalībvalstis un Komisiju. Attiecīgā maka izdevējs vai dalībvalsts attiecīgi informē atkarīgās puses un lietotājus.

2. Ja 1. punktā minētais pārkāpums vai kompromitējums ir novērsts, maka izdevējs atjauno Eiropas digitālās identitātes maka izdošanu un izmantošanu. Dalībvalsts, kurā attiecīgie maki tika izdoti, bez liekas kavēšanās informē dalībvalstis un Komisiju. Attiecīgo maku izdevējs vai dalībvalsts bez liekas kavēšanās informē atkarīgās puses un lietotājus.

3. Ja 1. punktā minētais pārkāpums vai kompromitējums nav novērsts trīs mēnešu laikā pēc apturēšanas, attiecīgā dalībvalsts anulē attiecīgo Eiropas digitālās identitātes maku un attiecīgi informē citas dalībvalstis un Komisiju. Ja to attaisno pārkāpuma smagums, attiecīgo Eiropas digitālās identitātes maku anulē bez nepamatotas kavēšanās.

4. Komisija bez nepamatotas kavēšanās publicē *Eiropas Savienības Oficiālajā Vēstnesī* 6.d pantā minētā saraksta attiecīgos grozījumus.

5. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija papildus precizē 1., 2. un 3. punktā minētos pasākumus, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 11. punktā. Minēto īstenošanas aktu pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

6.db pants

Eiropas digitālās identitātes maku izmantošana pārrobežu mērogā

1. Ja dalībvalstis prasa elektronisko identifikāciju, izmantojot elektroniskās identifikācijas līdzekļus un autentifikāciju, lai piekļūtu publiskas iestādes sniegtam tiešsaistes pakalpojumam, tās lietotāja autentifikācijai arī akceptē Eiropas digitālās identitātes makus, kas izdoti saskaņā ar šo regulu.

2. Ja privātām atkarīgajām pusēm, kas sniedz pakalpojumus, izņemot mikrouzņēmumus un mazos uzņēmumus, kā tie definēti Komisijas Ieteikumā 2003/361/EK, saskaņā ar valsts vai Savienības tiesību aktiem tiešsaistes identifikācijai jāizmanto droša lietotāju autentifikācija tiešsaistes identifikācijai vai ja droša lietotāju autentifikācija ir nepieciešama saskaņā ar līgumsaistībām, tostarp tādās jomās kā transports, enerģētika, banku un finanšu pakalpojumi, sociālais nodrošinājums, veselības aprūpe, dzeramais ūdens, pasta pakalpojumi, digitālā infrastruktūra, izglītība vai telesakari, privātas atkarīgās puses – ne vēlāk kā 12 mēnešus pēc Eiropas digitālās identitātes maku izdošanas saskaņā ar 6.a panta 1. punktu un tikai pēc lietotāja brīvprātīga pieprasījuma – arī akceptē saskaņā ar šo regulu izdoto Eiropas digitālās identitātes maku izmantošanu attiecībā uz minimālajiem datiem, kas nepieciešami konkrētajam tiešsaistes pakalpojumam, kura vajadzībām tiek pieprasīta lietotāja autentifikācija.

3. Ja ļoti lielas tiešsaistes platformas, kas definētas Regulas [atsauce uz DPA regulu] 25. panta 1. punktā, prasa lietotājiem autentificēties, lai piekļūtu tiešsaistes pakalpojumiem, tās arī akceptē saskaņā ar šo regulu izdoto Eiropas digitālās identitātes maku izmantošanu lietotāja autentifikācijai tikai pēc lietotāja brīvprātīga pieprasījuma un attiecībā uz minimālajiem datiem, kas nepieciešami konkrētajam tiešsaistes pakalpojumam, kura vajadzībām tiek pieprasīta lietotāja autentifikācija.

4. Lai veicinātu Eiropas digitālās identitātes maku plašu pieejamību un izmantojamību šīs regulas darbības jomā, Komisija sadarbībā ar dalībvalstīm rosina un sekmē rīcības kodeksu izstrādi. Šie rīcības kodeksi sekmē to, ka šīs regulas darbības jomā tiek akceptēti elektroniskās identifikācijas līdzekļi, tostarp Eiropas digitālās identitātes maki, un ka tos jo īpaši akceptē pakalpojumu sniedzēji, kas lietotāju autentifikācijai izmanto trešo personu elektroniskās identifikācijas pakalpojumus. Komisija ciešā sadarbībā ar visām attiecīgajām ieinteresētajām personām sekmēs šādu rīcības kodeksu izstrādi un mudinās pakalpojumu sniedzējus rīcības kodeksu izstrādi pabeigt 12 mēnešu laikā pēc šīs regulas pieņemšanas un tos efektīvi īstenot 18 mēnešu laikā pēc šīs regulas pieņemšanas.

5. Komisija 24 mēnešu laikā pēc Eiropas digitālās identitātes maku ieviešanas novērtē, vai, pamatojoties uz pierādījumiem, kas liecina par Eiropas digitālās identitātes maku pieprasījumu, pieejamību un izmantojamību, jāuzdod vēl citiem privātiem tiešsaistes pakalpojumu sniedzējiem tikai pēc lietotāja brīvprātīga pieprasījuma akceptēt Eiropas digitālās identitātes maka izmantošanu. Novērtēšanas kritēriji ir šādi: lietotāju bāzes apjoms, pakalpojumu sniedzēju klātbūtne pārrobežu mērogā, tehnoloģiju attīstība, izmantošanas modeļu attīstība un patērētāju pieprasījums.

8) pirms regulas 7. panta iekļauj šādu virsrakstu:

"II IEDAĻA

ELEKTRONISKĀS IDENTIFIKĀCIJAS SHĒMAS";

9) regulas 7. panta ievadteikumu aizstāj ar šādu:

"Saskaņā ar 9. panta 1. punktu dalībvalstis, kas to vēl nav izdarījušas, 24 mēnešu laikā pēc 6.a panta 11. punktā un 6.c panta 4. punktā minēto īstenošanas aktu stāšanās spēkā paziņo vismaz vienu elektroniskās identifikācijas shēmu, kas ietver vismaz vienu identifikācijas līdzekli ar augstu uzticamības līmeni. Par elektroniskās identifikācijas shēmu var paziņot saskaņā ar 9. panta 1. punktu ar noteikumu, ka ir izpildīti visi šie nosacījumi:";

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

"2. Komisija *Eiropas Savienības Oficiālajā Vēstnesī* publicē to elektroniskās identifikācijas shēmu sarakstu, par kurām iesniegts paziņojums saskaņā ar šā panta 1. punktu, un pamatinformāciju par tām.

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

12) regulā iekļauj šādu 11.a pantu:

"*11.a pants*

Ierakstu saskaņošana

1. Ja autentifikācijai izmanto paziņotos elektroniskās identifikācijas līdzekļus vai Eiropas digitālās identitātes makus, dalībvalstis, rīkojoties kā atkarīgās puses, nodrošina ierakstu saskaņošanu.

2. Dalībvalstis Eiropas digitālās identitātes maku izdošanas vajadzībām 12. panta 4. punkta d) apakšpunktā minētajā personas identifikācijas datu minimālajā kopumā iekļauj vismaz vienu unikālu un pastāvīgu identifikatoru atbilstīgi Savienības un valsts tiesību aktiem, lai pēc lietotāja pieprasījuma identificētu lietotāju tikai tajos pārrobežu gadījumos, kad lietotāja identifikācija ir prasīta tiesību aktos.

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

2.aa Dalībvalstis saskaņā ar valsts tiesību aktiem var paredzēt, ka Eiropas digitālās identitātes maka lietotājs var pieprasīt, lai unikālais un pastāvīgais identifikators, kas iekļauts personas identifikācijas datu minimālajā kopumā un kas saistīts ar maku saskaņā ar 6.a panta 4. punkta e) apakšpunktu, tiktu aizstāts ar citu dalībvalsts izdotu unikālu un pastāvīgu identifikatoru.

3. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija papildus precizē 1. punktā minētos pasākumus, šādā nolūkā pieņemot īstenošanas aktu. Minēto īstenošanas aktu pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

3.a Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija precizē 2. un 2.aa punktā minētos pasākumus, šādā nolūkā pieņemot īstenošanas aktu. Minēto īstenošanas aktu pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

13) Regulas 12. pantu groza šādi:

Sadarbība un sadarbspēja

a) panta 3. punkta d) apakšpunktu svītro;

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

"d) atsauci uz personas identifikācijas datu minimālo kopumu, kas vajadzīgs, lai unikāli un pastāvīgi apliecinātu fizisku vai juridisku personu vai fizisku personu, kas pārstāv fizisku vai juridisku personu;";

ba) panta 5. punktā iekļauj c) apakšpunktu:

"c) līdzīga pieeja attiecībā uz tiešsaistes pakalpojumiem, kuros atļauts izmantot Eiropas digitālās identitātes makus, kas izdoti saskaņā ar šo regulu;";

c) panta 6. punkta a) apakšpunktu aizstāj ar šādu:

"a) informācijas, pieredzes un labas prakses apmaiņu attiecībā uz elektroniskās identifikācijas shēmām un jo īpaši tehniskajām prasībām, kas ir saistītas ar sadarbspēju, ierakstu saskaņošanu un uzticamības līmeņiem;";

ca) panta 6. punktā iekļauj e) apakšpunktu:

"e) informācijas, pieredzes un labas prakses apmaiņu un pamatnostādņu izdošanu attiecībā uz to, kā var projektēt, izstrādāt un ieviest tiešsaistes pakalpojumus, lai paļautos uz Eiropas digitālās identitātes makiem."

14) iekļauj šādu 12.a un 12.b pantu:

"*12.a pants*

Elektroniskās identifikācijas shēmu sertifikācija

1. Paziņojamo elektroniskās identifikācijas shēmu atbilstību šajā regulā noteiktajām prasībām sertificē, lai apliecinātu šādu shēmu vai to daļu atbilstību 8. panta 2. punktā noteiktajām prasībām attiecībā uz elektroniskās identifikācijas shēmu uzticamības līmeņiem saskaņā ar attiecīgo kiberdrošības sertifikācijas shēmu, ievērojot Regulu (ES) 2019/881 vai tās daļas, ciktāl kiberdrošības sertifikāts vai tā daļas aptver 8. panta 2. punktā noteiktās prasības attiecībā uz elektroniskās identifikācijas shēmu uzticamības līmeņiem. Sertifikācija nepārsniedz piecus gadus ar nosacījumu, ka regulāri reizi divos gados tiek veikts neaizsargātības novērtējums. Ja neaizsargātības tiek konstatētas un netiek novērstas 3 mēnešu laikā, sertifikāciju anulē.

   Sertifikāciju saskaņā ar Regulu (EK) Nr. 765/2008 veic dalībvalstu izraudzītas akreditētas valsts vai privātas atbilstības novērtēšanas struktūras.

2. Elektroniskās identifikācijas shēmu salīdzinošo izvērtēšanu, kas minēta 12. panta 6. punkta c) apakšpunktā, nepiemēro elektroniskās identifikācijas shēmām vai šādu shēmu daļām, kas sertificētas saskaņā ar 1. punktu.

2.a Neatkarīgi no šā panta 2. punkta dalībvalstis var pieprasīt no paziņotājas dalībvalsts papildu informāciju par elektroniskās identifikācijas shēmām vai to daļām, kas sertificētas saskaņā ar šā panta 2. punktu.

3. Dalībvalstis paziņo Komisijai 1. punktā minēto valsts vai privātā sektora iestāžu nosaukumus un adreses. Komisija minēto informāciju dara pieejamu dalībvalstīm.";

"12.b pants

Piekļuve aparatūrai un programmatūras funkcijām

Eiropas digitālās identitātes maku izdevēji un paziņoto elektroniskās identifikācijas līdzekļu izdevēji, kas rīkojas komerciālā vai profesionālā statusā un izmanto platformas pamatpakalpojumus, kā noteikts Regulas (ES) 2022/1925 2. panta 2. punktā, nolūkā nodrošināt Eiropas digitālās identitātes maku pakalpojumus un elektroniskās identifikācijas līdzekļus galalietotājiem vai tos izmanto šādas nodrošināšanas laikā, ir komerciālie lietotāji saskaņā ar Regulas (ES) 2022/1925 2. panta 21. punktu.

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

"1. Neatkarīgi no šā panta 2. punkta uzticamības pakalpojumu sniedzēji ir atbildīgi par zaudējumu, kas apzināti vai nolaidības dēļ radīts jebkurai fiziskai vai juridiskai personai tādēļ, ka nav ievēroti šajā regulā minētie pienākumi.

Pienākumu pierādīt nekvalificēta uzticamības pakalpojumu sniedzēja nodomu vai nolaidību uzņemas fiziska vai juridiska persona, kas iesniedz prasību par šā punkta pirmajā daļā minēto zaudējumu.

Tiek uzskatīts, ka ir bijis nodoms vai nolaidība no kvalificēta uzticamības pakalpojumu sniedzēja puses, ja vien minētais kvalificēts uzticamības pakalpojumu sniedzējs nepierāda, ka šā punkta pirmajā daļā minētais zaudējums ir noticis bez nodoma vai nolaidības no minētā kvalificēta uzticamības pakalpojumu sniedzēja puses."

18) regulas 14. pantu aizstāj ar šādu:

"*14. pants*

Starptautiskie aspekti

1. Ja trešās valsts vai starptautiskas organizācijas sniegtie uzticamības pakalpojumi ir atzīti saskaņā ar īstenošanas lēmumu vai nolīgumu, kas saskaņā ar Līguma 218. pantu noslēgts starp Savienību un attiecīgo trešo valsti vai starptautisku organizāciju, tad uzticamības pakalpojumus, ko sniedz pakalpojumu sniedzēji, kas veic uzņēmējdarbību trešā valstī, vai starptautsika organizācija, atzīst kā juridiski līdzvērtīgus kvalificētiem uzticamības pakalpojumiem, ko sniedz kvalificēti uzticamības pakalpojumu sniedzēji, kas veic uzņēmējdarbību Savienībā.

2. Ar 1. punktā minētajiem īstenošanas lēmumiem un nolīgumiem nodrošina, ka prasības, kuras piemērojamas kvalificētiem uzticamības pakalpojumu sniedzējiem, kas veic uzņēmējdarbību Savienībā, un to sniegtajiem kvalificētiem uzticamības pakalpojumiem, ievēro uzticamības pakalpojumu sniedzēji trešā valstī vai starptautiskās organizācijās 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.

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

3. Šā panta 1. punktā minētos īstenošanas lēmumus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā."

19) regulas 15. pantu aizstāj ar šādu:

"*15. pants*

Pieejamība personām ar invaliditāti

Uzticamības pakalpojumus un tiešo lietotāju produktus, ko izmanto, sniedzot minētos pakalpojumus, dara piekļūstamus personām ar invaliditāti saskaņā piekļūstamības prasībām, kas noteiktas Direktīvā (ES) 2019/882 par produktu un pakalpojumu piekļūstamības prasībām.";

20) regulas 17. pantu groza šādi:

a) panta 4. punktu groza šādi:

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

"c) attiecīgo dalībvalstu attiecīgo valsts kompetento iestāžu, kas izraudzītas saskaņā ar Direktīvu (ES) XXXX/XXXX [TID2], informēšanu par jebkādiem būtiskiem drošības pārkāpumiem vai integritātes zudumu, par ko tās uzzina, pildot savus pienākumus. Ja būtiskais drošības pārkāpums vai integritātes zudums attiecas uz citām dalībvalstīm, uzraudzības iestāde informē attiecīgās dalībvalsts vienoto kontaktpunktu, kas izraudzīts saskaņā ar Direktīvu (ES) XXXX/XXXX (TID2), un saskaņā ar šīs regulas 17. pantu izraudzītās uzraudzības iestādes citās attiecīgajās dalībvalstīs. Ja informētā uzraudzības iestāde uzskata, ka drošības pārkāpuma vai integritātes zuduma publiskošana ir sabiedrības interesēs, tā informē sabiedrību vai pieprasa, lai to izdarītu uzticamības pakalpojumu sniedzējs;";

2) punkta f) apakšpunktu aizstāj ar šādu:

"f) sadarbību ar kompetentajām uzraudzības iestādēm, kas izveidotas saskaņā ar Regulu (ES) 2016/679, 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;";

b) panta 6. punktu aizstāj ar šādu:

"6. Katru gadu līdz 31. martam katra uzraudzības iestāde iesniedz Komisijai pārskatu par iepriekšējā kalendārajā gadā veiktajām galvenajām darbībām.";

c) panta 8. punktu aizstāj ar šādu:

"8. Komisija 12 mēnešu laikā pēc šīs regulas stāšanās spēkā pieņem pamatnostādnes par to, kā uzraudzības iestādes veic 4. punktā minētos uzdevumus, un, izmantojot īstenošanas aktus, kas pieņemti saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru, nosaka 6. punktā minētā ziņojuma formātus un procedūras.";

21) Regulas 18. pantu groza šādi:

a) regulas 18. panta nosaukumu aizstāj ar šādu:

"Savstarpēja palīdzība un sadarbība";

b) panta 1. punktu aizstāj ar šādu:

"1. Uzraudzības iestādes sadarbojas, lai apmainītos ar labu praksi un informāciju par uzticamības pakalpojumu sniegšanu.";

c) pievieno šādu 4. un 5. punktu:

"4. Uzraudzības iestādes un valstu kompetentās iestādes saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) XXXX/XXXX [TID2] sadarbojas un palīdz cita citai, lai nodrošinātu, ka uzticamības pakalpojumu sniedzēji atbilst prasībām, kas noteiktas šajā regulā un Direktīvā (ES) XXXX/XXXX [TID2]. Uzraudzības iestādes pieprasa valsts kompetentajām iestādēm saskaņā ar Direktīvu XXXX/XXXX [TID2] veikt uzraudzības darbības, lai pārbaudītu uzticamības pakalpojumu sniedzēju atbilstību Direktīvā XXXX/XXXX [TID2] noteiktajām prasībām, pieprasītu uzticamības pakalpojumu sniedzējiem novērst visas neatbilstības minētajām prasībām, laikus sniegtu visu ar uzticamības pakalpojumu sniedzējiem saistīto uzraudzības darbību rezultātus un informētu uzraudzības iestādes par attiecīgajiem incidentiem, kas paziņoti saskaņā ar Direktīvu XXXX/XXXX [TID2].

5. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem izveido procesuālo kārtību, kas vajadzīga 1. punktā minētās uzraudzības iestāžu sadarbības veicināšanai. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

(21.a)regulā iekļauj šādu 19.a pantu:

"Prasības nekvalificētiem uzticamības pakalpojumu sniedzējiem"

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

a) īsteno atbilstīgu rīcībpolitiku un veic attiecīgus pasākumus, ar ko pārvalda juridiskos, uzņēmējdarbības, operacionālos un citus tiešos vai netiešos riskus, kuri apdraud nekvalificētā uzticamības pakalpojuma sniegšanu. Neatkarīgi no Direktīvas (ES) XXXX/XXX [TID2] 18. panta noteikumiem minētie pasākumi ir vismaz šādi:

i) pasākumi, kas saistīti ar procedūrām, kuras piemēro, lai reģistrētos pakalpojumam un iepazītos ar pakalpojumu;

ii) pasākumi, kas saistīti ar procesuālajām vai administratīvajām pārbaudēm;

iii) pasākumi, kas saistīti ar pakalpojumu pārvaldību un īstenošanu.

b) paziņo uzraudzības iestādei, identificējamām skartajām personām, sabiedrībai, ja tas ir sabiedrības interesēs, un attiecīgā gadījumā citām attiecīgajām kompetentajām iestādēm par visiem pārkāpumiem vai traucējumiem pakalpojuma sniegšanā vai to pasākumu īstenošanā, kas minēti a) apakšpunkta i), ii) un iii) punktā un kuri būtiski ietekmē sniegto uzticamības pakalpojumu vai tajā glabātos personas datus; šādu paziņojumu veic bez nepamatotas kavēšanās un jebkurā gadījumā ne vēlāk kā 24 stundu laikā pēc tam, kad minētie pārkāpumi vai traucējumi kļuvuši zināmi.

2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka 1. punkta a) apakšpunktā minēto pasākumu tehniskos raksturlielumus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

(22) 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) XXXX/XXXX [TID2] 18. pantā. Kvalificētie uzticamības pakalpojumu sniedzēji trīs darba dienās pēc izrietošā atbilstības novērtēšanas ziņojuma saņemšanas to iesniedz uzraudzības iestādei.";

aa) iekļauj šādu punktu:

1.a Dalībvalstis var paredzēt, ka kvalificēti uzticamības pakalpojumu sniedzēji laikus informē uzraudzības iestādi par plānotajām revīzijām un ļauj uzraudzības iestādei pēc pieprasījuma piedalīties novērotāja statusā.

b) panta 2. punkta pēdējo teikumu aizstāj ar šādu:

"Ja personas datu aizsardzības noteikumi, iespējams, ir pārkāpti, uzraudzības iestāde bez nepamatotas kavēšanās informē kompetentās uzraudzības iestādes saskaņā ar Regulu (ES) 2016/679.";

c) panta 3. un 4. punktu aizstāj ar šādiem:

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

Ja minētais pakalpojumu sniedzējs – attiecīgā gadījumā uzraudzības iestādes noteiktajā termiņā – nav labojis neizpildi, uzraudzības iestāde, jo īpaši ņemot vērā minētās neizpildes apmēru, ilgumu un sekas, var anulēt minētā pakalpojumu sniedzēja vai tā sniegtā skartā pakalpojuma kvalifikācijas statusu.

3.a Ja valsts kompetentās iestādes saskaņā ar Direktīvu (ES) XXXX/XXXX [TID2] ir informējušas uzraudzības iestādi par to, ka kvalificētais uzticamības pakalpojumu sniedzējs nepilda kādu no Direktīvas (ES) XXXX/XXXX [TID2] 18. pantā noteiktajām prasībām, uzraudzības iestāde, jo īpaši ņemot vērā minētās neizpildes apmēru, ilgumu un sekas, var anulēt minētā pakalpojumu sniedzēja vai tā sniegtā skartā pakalpojuma kvalifikācijas statusu.

3.b Ja uzraudzības iestādes saskaņā ar Regulu (ES) 2016/679 ir informējušas uzraudzības iestādi par to, ka kvalificētais uzticamības pakalpojumu sniedzējs nepilda kādu no Regulā (ES) 2016/679 noteiktajām prasībām, uzraudzības iestāde, jo īpaši ņemot vērā minētās neizpildes apmēru, ilgumu un sekas, var anulēt minētā pakalpojumu sniedzēja vai tā sniegtā skartā pakalpojuma kvalifikācijas statusu.

3.c Uzraudzības iestāde informē kvalificēto uzticamības pakalpojumu sniedzēju par tā kvalifikācijas statusa vai attiecīgā pakalpojuma kvalifikācijas statusa anulēšanu. Uzraudzības iestāde informē 22. panta 3. punktā minēto struktūru, lai atjauninātu 22. panta 1. punktā minētos uzticamības sarakstus, un Direktīvā XXXX [TID2] minēto valsts kompetento iestādi.

4. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka tehniskās specifikācijas un standartu identifikācijas numurus:

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, 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 48. panta 2. punktā minēto pārbaudes procedūru.";

(23) regulas 21. pantu groza šādi:

"1. Ja uzticamības pakalpojumu sniedzēji plāno sākt sniegt kvalificētos uzticamības pakalpojumus, tie uzraudzības iestādei iesniedz paziņojumu par savu nodomu kopā ar atbilstības novērtēšanas struktūras izdotu atbilstības novērtēšanas ziņojumu, kurā apstiprināta šajā regulā un Direktīvas (ES) XXXX/XXXX [TID2] 18. pantā noteikto prasību izpilde.";

a) panta 2. punktu aizstāj ar šādu:

"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 XXXX [TID2] 18. pantā noteiktajām prasībām, uzraudzības iestāde pieprasa, lai kompetentās iestādes, kas minētas Direktīvā XXXX [TID2], veic uzraudzības darbības šajā sakarā un bez nepamatotas kavēšanās un ne vēlāk kā divus mēnešus pēc tam, kad šo pieprasījumu saņēmušas Direktīvā XXXX [TID2] minētās kompetentās iestādes, sniedz informāciju par rezultātiem. Ja divos mēnešos no paziņojuma saņemšanas verificēšana nav pabeigta, Direktīvā XXXX [TID2] minētās kompetentās iestādes informē uzraudzības iestādi, norādot kavēšanās iemeslus un termiņu, līdz kuram verifikācija jāpabeidz.

Ja uzraudzības iestāde secina, ka uzticamības pakalpojumu sniedzējs un tā sniegtie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām, uzraudzības iestāde vēlākais trīs mēnešos 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 mēnešos no 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. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka paziņošanas un verifikācijas formātus un procedūras 1. un 2. punkta vajadzībām. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

(25) regulas 24. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Izdodot kvalificētu sertifikātu vai kvalificētu atribūtu elektronisko apliecinājumu, kvalificēts uzticamības pakalpojumu sniedzējs verificē tās fiziskās vai juridiskās personas identitāti, kurai tiks izdots kvalificētais sertifikāts vai kvalificētais atribūtu elektroniskais apliecinājums, un vajadzības gadījumā šīs fiziskās vai juridiskās personas īpašos atribūtus.

Kvalificētais uzticamības pakalpojumu sniedzējs, tieši vai paļaujoties uz trešo personu, pirmajā daļā minēto informāciju verificē kādā no šādiem veidiem:

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

b) izmantojot kvalificētu atribūtu elektronisko apliecinājumu vai kvalificētu elektronisko parakstu, vai kvalificētu elektronisko zīmogu, kas izdots saskaņā ar a), c) vai d) apakšpunktu;

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

d) fiziskās personas vai juridiskās personas pilnvarotā pārstāvja fiziskā klātbūtnē, izmantojot atbilstīgas procedūras un saskaņā ar valsts tiesību aktiem.";

b) pantā iekļauj šādu 1.a punktu:

"1.a Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka minimālās tehniskās specifikācijas, standartus un procedūras attiecībā uz identitātes un atribūtu verifikāciju saskaņā ar 1. punkta c) apakšpunktu. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

c) panta 2. punktu groza šādi:

0) punkta a) apakšpunktu groza šādi:

"a) informē uzraudzības iestādi vismaz vienu mēnesi pirms jebkādu izmaiņu ieviešanas tās kvalificēto uzticamības pakalpojumu sniegšanā vai vismaz trīs mēnešus, ja ir nodoms pārtraukt minētās darbības. Pirms piešķirt atļauju paredzēto izmaiņu ieviešanai kvalificētajos uzticamības pakalpojumos uzraudzības iestāde var pieprasīt papildu informāciju vai atbilstības novērtējuma rezultātus. Ja trīs mēnešos no paziņojuma saņemšanas verificēšana nav pabeigta, uzraudzības iestāde informē uzticamības pakalpojumu sniedzēju, norādot kavēšanās iemeslus un termiņu, līdz kuram verifikācija jāpabeidz.

1) punkta d) un e) apakšpunktus aizstāj ar šādiem:

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

"e) izmanto uzticamas sistēmas un produktus, kas ir aizsargāti pret modifikāciju, un nodrošina to atbalstīto procesu tehnisko drošību un uzticamību, tostarp izmantojot piemērotus šifrēšanas algoritmus, atslēgu garumu un jaucējfunkcijas sistēmās, produktos un to atbalstītajos procesos;";

2) iekļauj šādus jaunus fa) un fb) apakšpunktus:

"fa) īsteno atbilstīgu rīcībpolitiku un veic attiecīgus pasākumus, ar ko pārvalda juridiskos, uzņēmējdarbības, operacionālos un citus tiešos vai netiešos riskus, kuri apdraud kvalificētā uzticamības pakalpojuma sniegšanu. Neatkarīgi no Direktīvas (ES) XXXX/XXX [TID2] 18. panta noteikumiem minētie pasākumi ir vismaz šādi:

i) pasākumi, kas saistīti ar procedūrām, kuras piemēro, lai reģistrētos pakalpojumam un iepazītos ar pakalpojumu;

ii) pasākumi, kas saistīti ar procesuālajām vai administratīvajām pārbaudēm;

iii) pasākumi, kas saistīti ar 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 pārkāpumiem vai traucējumiem pakalpojuma sniegšanā vai to pasākumu īstenošanā, kas minēti fa) apakšpunkta i), ii) un iii) punktā un kuri būtiski ietekmē sniegto uzticamības pakalpojumu vai tajā glabātos personas datus; šādu paziņojumu veic bez nepamatotas kavēšanās un jebkurā gadījumā ne vēlāk kā 24 stundas pēc incidenta.";

3) punkta g) un h) 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;";

4) punkta j) apakšpunktu svītro;

d) pantā iekļauj šādu 4.a punktu:

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

e) panta 5. punktu aizstāj ar šādu:

"5. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka tehniskās specifikācijas, procedūras un identifikācijas numurus standartiem, kas attiecas uz 2. punktā minētajām prasībām. Uzskata, ka atbilstība šajā pantā noteiktajām prasībām ir panākta tad, ja ir izpildītas minētās tehniskās specifikācijas, procedūras un standarti. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

f) pantam pievieno šādu 6. punktu:

"6. Komisija tiek pilnvarota pieņemt īstenošanas aktus, ar kuriem nosaka 2. punkta fa) apakšpunktā minēto pasākumu tehniskos raksturlielumus.";

(25.a) Regulas 26. pantu groza šādi:

2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka uzlaboto elektronisko parakstu tehniskās specifikācijas un standartu identifikācijas numurus. Uzskata, ka atbilstība prasībām attiecībā uz uzlabotiem elektroniskiem parakstiem ir panākta tad, ja uzlabotais elektroniskais paraksts atbilst minētajām specifikācijām un standartiem. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

(25.b) Regulas 27. pantu groza šādi:

panta 4. punktu svītro.

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

"6. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka kvalificēto elektronisko parakstu sertifikātu tehniskās specifikācijas un standartu identifikācijas numurus. Uzskata, ka atbilstība I pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā paraksta sertifikāts atbilst minētajām specifikācijām un standartiem. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

(27) regulas 29. pantam pievieno šādu 1.a punktu:

"1.a elektroniskā paraksta radīšanas datu ģenerēšanu un pārvaldību parakstītāja vārdā vai šāda paraksta radīšanas datu dublēšanu rezerves kopijas vajadzībām var veikt tikai kvalificēts uzticamības pakalpojumu sniedzējs, kas sniedz kvalificētu uzticamības pakalpojumu attālinātas kvalificētas elektroniskā paraksta radīšanas ierīces pārvaldībai.";

(28) regulā iekļauj šādu 29.a pantu:

"*29.a pants*

Prasības kvalificētam pakalpojumam attālinātu kvalificētu elektroniskā paraksta radīšanas ierīču pārvaldībai

1. Attālinātu kvalificētu elektroniskā paraksta radīšanas ierīču pārvaldību kā kvalificētu pakalpojumu var veikt 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 var dublēt tikai rezerves kopijas vajadzībām ar nosacījumu, ka ir izpildītas šādas prasības:

i. dublēto datu kopu drošības līmenim jābūt tādam pašam, kāds tas ir oriģinālajām datu kopām;

ii. dublēto 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 paraksta radīšanas ierīci, kas izdots saskaņā ar 30. pantu.

2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka tehniskās specifikācijas un standartu identifikācijas numurus 1. punkta vajadzībām.";

(29) regulas 30. pantā iekļauj šādu 3 a. punktu:

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

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

"3. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka formātus un procedūras, ko piemēro 1. punkta vajadzībām. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

(31) Regulas 32. pantu groza šādi:

a) panta 1. punktam pievieno šādu daļu:

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

b) panta 3. punktu aizstāj ar šādu:

"3. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka kvalificēto elektronisko parakstu validācijas specifikācijas un standartu identifikācijas numurus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

(31.a) regulā iekļauj šādu 32.a pantu:

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

1. Uzlabota elektroniskā paraksta, kura pamatā ir kvalificēts sertifikāts, validācijas procesā 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 izsniedza 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 tika izpildītas 26. pantā noteiktās prasības. Uzskata, ka atbilstība pirmajā daļā noteiktajām prasībām ir panākta tad, ja uzlabotu elektronisko parakstu, kuru pamatā ir kvalificēti sertifikāti, validācija atbilst 3. punktā minētajām specifikācijām un standartiem.

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

3. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka uzlaboto elektronisko parakstu, kuru pamatā ir kvalificēti sertifikāti, validācijas specifikācijas un standartu identifikācijas numurus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru."

(31.b) Regulas 33. pantu groza šādi:

"1. Kvalificētu elektronisko parakstu kvalificētus validēšanas pakalpojumus var sniegt tikai kvalificēts uzticamības pakalpojumu sniedzējs, kurš.";

"2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka 1. punktā minētā kvalificētā validēšanas pakalpojuma tehniskās specifikācijas un standartu identifikācijas numurus. Uzskata, ka atbilstība 1 punktā noteiktajām prasībām ir panākta tad, ja kvalificēta elektroniskā paraksta validēšanas pakalpojums atbilst minētajām specifikācijām un standartiem. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.".

(32) panta 34. punktu aizstāj ar šādu:

"*34. pants*

Kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojums

1. Kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumu var sniegt tikai kvalificēts uzticamības pakalpojumu sniedzējs, kas izmanto tādas procedūras un tehnoloģijas, ar kurām var nodrošināt kvalificētā elektroniskā paraksta uzticamību ilgāk par tehnoloģiskā derīguma termiņu.

2. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojums atbilst 3. punktā minētajām specifikācijām un standartiem.

3. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojuma tehniskās specifikācijas un standartu identifikācijas numurus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

(32.a) regulas 36. pantam pievieno jaunu 2. punktu:

2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka uzlabotu elektronisko zīmogu tehniskās specifikācijas un standartu identifikācijas numurus.

Uzskata, ka atbilstība prasībām attiecībā uz uzlabotiem elektroniskiem zīmogiem ir panākta tad, ja uzlabotais elektroniskais zīmogs atbilst minētajām specifikācijām un standartiem. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

(33) Regulas 37. pantu groza šādi:

panta 4. punktu svītro.

(34) Regulas 38. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. Kvalificēti elektronisko zīmogu sertifikāti atbilst III pielikumā noteiktajām prasībām. Uzskata, ka atbilstība III pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā zīmoga sertifikāts atbilst 6. punktā minētajām specifikācijām un standartiem.";

b) panta 6. punktu aizstāj ar šādu:

"6. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka kvalificētu elektronisko zīmogu sertifikātu tehniskās specifikācijas un standartu identifikācijas numurus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

35) regulā iekļauj šādu 39.a pantu:

"*39.a pants*

Prasības kvalificētam pakalpojumam attālinātu kvalificēta elektroniskā zīmoga radīšanas ierīču pārvaldībai

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

35.a) regulā iekļauj šādu 40.a pantu:

"*40.a pants*

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

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

36) regulas 42. pantu groza šādi:

a) pantā iekļauj šādu jaunu 1.a punktu:

"1.a Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja datuma un laika sasaiste ar datiem un precīzais laika avots atbilst 2. punktā minētajām specifikācijām un standartiem.";

b) panta 2. punktu aizstāj ar šādu:

"2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka tehniskās specifikācijas un identifikācijas numurus standartiem, kas attiecas uz datuma un laika sasaisti ar datiem un uz precīzo laika avotu. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

36.a) regulas 43. pantam pievieno jaunu 3. punktu:

"2.a. Kvalificētu elektroniski reģistrētu piegādes pakalpojumu vienā dalībvalstī atzīst par kvalificētu elektroniski reģistrētu piegādes pakalpojumu jebkurā citā dalībvalstī.";

37) regulas 44. pantu groza šādi:

a) pantā iekļauj šādu 1.a punktu:

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

b) panta 2. punktu aizstāj ar šādu:

"2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka datu nosūtīšanas un saņemšanas procesu tehniskās specifikācijas un standartu identifikācijas numurus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

c) pievieno šādu 3. un 4. punktu:

"3. Kvalificētu elektroniski reģistrētu piegādes pakalpojumu sniedzēji var vienoties par savu sniegto kvalificēto elektroniski reģistrēto piegādes pakalpojumu sadarbspēju. Šāda sadarbspējas sistēma atbilst 1. punktā noteiktajām prasībām. Atbilstību apstiprina atbilstības novērtēšanas struktūra.

4. Komisija ar īstenošanas aktu var noteikt tehniskās specifikācijas un standartu identifikācijas numurus, lai atvieglotu datu pārsūtīšanu starp diviem vai vairākiem kvalificētiem uzticamības pakalpojumu sniedzējiem. Tehniskās specifikācijas un standartu saturs ir rentabli un samērīgi. Īstenošanas aktu pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

38) 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 IV pielikumā noteiktajām prasībām izvērtē saskaņā ar 4. punktā minētajām specifikācijām un standartiem.

2. Šā panta 1. punktā minētos kvalificētos tīmekļa vietņu autentifikācijas sertifikātus atpazīst tīmekļa pārlūkprogrammas. Šādā nolūkā tīmekļa pārlūkprogrammas nodrošina, ka identitātes dati, kas sniegti ar jebkuru metodi, tiek attēloti lietotājdraudzīgā veidā. Tīmekļa pārlūkprogrammas nodrošina atbalstu un sadarbspēju ar 1. punktā minētajiem kvalificētajiem tīmekļa vietņu autentifikācijas sertifikātiem, izņemot uzņēmumus, kurus saskaņā ar Komisijas Ieteikumu 2003/361/EK uzskata par mikrouzņēmumiem un mazajiem uzņēmumiem, pirmajos piecos gados, kad tie darbojas kā tīmekļa pārlūkošanas pakalpojumu sniedzēji.

4. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka specifikācijas un identifikācijas numurus standartiem, kas attiecas uz 1. un 2. punktā minētajiem kvalificētajiem tīmekļa vietņu autentifikācijas sertifikātiem. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

39) pēc 45. panta iekļauj šādu 9., 10. un 11. iedaļu:

"9. IEDAĻA

ATRIBŪTU ELEKTRONISKAIS APLIECINĀJUMS

45.a pants

Atribūtu elektroniskā apliecinājuma juridiskais spēks

1. Atribūtu elektroniskajam apliecinājumam ir neapšaubāms juridiskais spēks, tas ir pieņemams kā pierādījums tiesvedībā, un to nedrīkst noraidīt 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. Kvalificētu atribūtu elektronisko apliecinājumu, kas izdots vienā dalībvalstī, atzīst kā kvalificētu atribūtu elektronisko apliecinājumu visās citās dalībvalstīs.

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

45.b pants

Atribūtu elektroniskais apliecinājums sabiedrisko pakalpojumu jomā

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

45.c pants

Prasības kvalificētam elektroniskajam atribūtu apliecinājumam

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

1.a Atbilstību V pielikumā noteiktajām prasībām izvērtē saskaņā ar 4. punktā minētajām specifikācijām un standartiem.

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

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

4. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija nosaka kvalificētu atribūtu elektronisko apliecinājumu tehniskās specifikācijas un standartu identifikācijas numurus, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 11. punktā.

45.d pants

Atribūtu verifikācija attiecībā pret autentiskiem avotiem

1. Dalībvalstis 24 mēnešu laikā pēc 6.a panta 11. punktā un 6.c panta 4. punktā minēto īstenošanas aktu stāšanās spēkā nodrošina, ka vismaz attiecībā uz VI pielikumā norādītajiem atribūtiem – ja šie atribūti atkarīgi no autentiskiem avotiem publiskajā sektorā – tiek veikti pasākumi, kas ļauj kvalificētiem atribūtu elektronisko apliecinājumu nodrošinātājiem pēc lietotāja pieprasījuma un saskaņā ar valsts vai Savienības tiesību aktiem ar elektroniskiem līdzekļiem verificēt šos atribūtus.

2. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā, ņemot vērā attiecīgos starptautiskos standartus, Komisija nosaka tehnisko specifikāciju, standartu un procedūru minimumu, atsaucoties uz atribūtu un shēmu katalogu atribūtu apliecinājumam un kvalificētu atribūtu elektronisko apliecinājumu verifikācijas procedūrām, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 11. punktā.

45.da 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) kvalificētais sertifikāts, kas apliecina tādas 3. panta 45.a punktā minētās publiskās iestādes kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu, kura identificēta kā VII pielikuma b) punktā minētais izdevējs, ietver konkrētu sertificētu atribūtu kopumu automatizētai apstrādei piemērotā veidā:

i) norādot, ka izdevējiestāde saskaņā ar valsts vai Savienības 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 valsts vai Savienības tiesību aktus.

2. Dalībvalsts, kurā ir izveidotas 3. panta 45.a 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.

2.a Dalībvalstis informē Komisiju par 3. panta 45.a punktā minētajām publiskajām iestādēm. Šajā 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 45.a punktā minēto publisko iestāžu sarakstu, kas ir elektroniski parakstīts vai apzīmogots un sagatavots automatizētai apstrādei piemērotā formātā.

3. 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. Atsaukto elektroniskā apliecinājuma statusu pēc atsaukšanas neatjauno.

4. Atribūtu elektronisko apliecinājumu, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā, uzskata par atbilstīgu šā panta 1. punktā noteiktajām prasībām, ja tas atbilst 5. punktā minētajiem standartiem.

5. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 11. punktā, nosaka tāda elektroniskā atribūtu apliecinājuma tehniskās specifikācijas un standartu identifikācijas numurus, kuru izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā.

5.a Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 11. punktā, nosaka 2.a punkta vajadzībām piemērojamos formātus, procedūras, specifikācijas un standartus.

6. Regulas 3. panta 45.a punktā minētās publiskās iestādes, kas izdod atribūtu elektronisko apliecinājumu, nodrošina saskarni ar Eiropas digitālās identitātes makiem, kas izdoti saskaņā ar 6.a pantu.

45.e pants

Atribūtu elektroniskā apliecinājuma izdošana Eiropas digitālās identitātes makiem

Kvalificētu atribūtu elektronisko apliecinājumu nodrošinātāji nodrošina saskarni ar Eiropas digitālās identitātes makiem, kas izdoti saskaņā ar 6.a pantu.

45.f pants

Papildu noteikumi atribūtu elektronisko apliecinājumu pakalpojumu sniegšanai

1. Kvalificētu un nekvalificētu atribūtu 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.

4. Kvalificēta elektroniskā atribūtu apliecinājuma pakalpojumu sniedzēji īsteno funkcionālu nošķiršanu šādu pakalpojumu sniegšanai.

10. IEDAĻA

ELEKTRONISKĀS ARHIVĒŠANAS PAKALPOJUMI

45.g pants

Elektroniskās arhivēšanas pakalpojuma juridiskais spēks

1. Elektroniskajiem datiem, kas tiek glabāti, izmantojot elektroniskās arhivēšanas pakalpojumu, ir neapšaubāms juridiskais spēks, un tie ir pieņemami kā pierādījums tiesvedībā, un tos nevar noraidīt tikai elektroniskā formāta dēļ vai tādēļ, ka tie netiek glabāti, izmantojot kvalificētu elektroniskās arhivēšanas pakalpojumu.

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

3. Kvalificētu elektroniskās arhivēšanas pakalpojumu vienā dalībvalstī atzīst par kvalificētu elektroniskās arhivēšanas pakalpojumu jebkurā citā dalībvalstī.

45.ga 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 paildzināt elektronisko datu ilgizturību un salasāmību pēc tehnoloģiskā derīguma termiņa beigām un vismaz visā juridiski vai līgumiski noteiktajā saglabāšanas periodā, vienlaikus saglabājot to integritāti un to izcelsmi;

c) tie nodrošina, ka elektroniskie dati 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, kas izgūti no kvalificēta elektroniskā arhīva, no saglabāšanas perioda sākuma līdz to izguves brīdim attiecas datu integritātes prezumpcija. Šo ziņojumu sniedz uzticamā un efektīvā veidā, un uz tā ir kvalificētā elektroniskās arhivēšanas pakalpojuma sniedzēja kvalificēts elektroniskais paraksts vai kvalificēts elektroniskais zīmogs;

2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka kvalificētu elektroniskās arhivēšanas pakalpojumu tehniskās specifikācijas un standartu identifikācijas numurus. Uzskata, ka atbilstība prasībām, kas noteiktas kvalificētiem elektroniskās arhivēšanas pakalpojumiem, ir panākta tad, ja kvalificēts elektroniskās arhivēšanas pakalpojums atbilst minētajām specifikācijām un standartiem. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.

11. IEDAĻA

ELEKTRONISKĀS VIRSGRĀMATAS

45.h pants

Elektronisko virsgrāmatu juridiskais spēks

1. Elektroniskajai virsgrāmatai ir neapšaubāms juridiskais spēks, 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.

3. Kvalificētu elektronisko virsgrāmatu vienā dalībvalstī atzīst par kvalificētu elektronisko virsgrāmatu jebkurā citā dalībvalstī.

45.i pants

Prasības kvalificētām elektroniskajām virsgrāmatām

1. Kvalificētas elektroniskās virsgrāmatas atbilst šādām prasībām:

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

   b) tās nosaka datu ierakstu izcelsmi virsgrāmatā;

   c) tās nodrošina datu ierakstu unikālo secīgo hronoloģisko secību virsgrāmatā;

   d) tajā datus reģistrē tā, lai visas turpmākās datu izmaiņas būtu uzreiz nosakāmas, nodrošinot to integritāti ilgtermiņā.

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

3. Komisija ar īstenošanas aktiem nosaka kvalificētas elektroniskās virsgrāmatas izveides un darbības tehniskās specifikācijas un standartu identifikācijas numurus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.";

40) regulā iekļauj šādu 48.a pantu:

"*48.a pants*

Ziņojumu sniegšanas prasības

1. Dalībvalstis nodrošina statistikas datu vākšanu saistībā ar Eiropas digitālās identitātes maku darbību, tiklīdz tie ir izdoti to teritorijā.

2. Statistikas dati, kas tiek vākti saskaņā ar 1. punktu, ietver šādus elementus:

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

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

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

41) regulas 49. pantu aizstāj ar šādu:

"*49. pants*

Pārskatīšana

1. Komisija pārskata šīs regulas piemērošanu un sniedz ziņojumu Eiropas Parlamentam un Padomei 36 mēnešu laikā pēc tās stāšanās spēkā. Komisija jo īpaši izvērtē 6. un 6.db panta darbības jomu un to, vai ir lietderīgi grozīt šīs regulas darbības jomu vai konkrētus tās noteikumus, ņemot vērā šīs regulas piemērošanā gūto pieredzi, kā arī klientu pieprasījumu, tehnoloģiskos sasniegumus un attīstību tirgus un tiesiskajā jomā. Vajadzības gadījumā minētajam ziņojumam pievieno šīs regulas grozījumu priekšlikumu.

2. Izvērtēšanas ziņojumā iekļauj novērtējumu par šīs regulas darbības jomā ietverto Eiropas digitālās identitātes maku pieejamību un izmantojamību un novērtē, vai jāuzdod visiem privātiem tiešsaistes pakalpojumu sniedzējiem, kas lietotāju autentifikācijai izmanto trešās personas elektroniskās identifikācijas pakalpojumus, akceptēt Eiropas digitālās identitātes maku izmantošanu.

3. Turklāt Komisija iesniedz ziņojumu Eiropas Parlamentam un Padomei reizi četros gados pēc pirmajā daļā minētā ziņojuma par panākumiem šīs regulas mērķu īstenošanā.";

42) 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 brīdim, kas ir 36 mēnešus pēc šīs regulas stāšanās spēkā, 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 brīdim, kas ir 24 mēnešus pēc šīs regulas stāšanās spēkā, turpina uzskatīt par kvalificētiem elektroniskā paraksta sertifikātiem saskaņā ar šo regulu.

2.a 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, turpina uzskatīt par tādu, saistībā ar kuru nav jāiegūst kvalifikācijas statuss šo pārvaldības pakalpojumu sniegšanai, līdz brīdim, kas ir 24 mēnešus pēc šīs regulas stāšanās spēkā.

2.b Kvalificēti uzticamības pakalpojumu sniedzēji, kuriem saskaņā ar šo regulu pirms [grozošās regulas spēkā stāšanās diena] ir piešķirts kvalifikācijas statuss, izmantojot identitātes verifikācijas metodes kvalificētu sertifikātu izdošanai saskaņā ar 24. panta 1. punktu, pēc iespējas drīz, bet ne vēlāk kā 30 mēnešus pēc grozošās regulas stāšanās spēkā iesniedz uzraudzības iestādei atbilstības novērtēšanas ziņojumu, kas apliecina atbilstību 24. panta 1. punktam. Kamēr šāds atbilstības novērtēšanas ziņojums nav iesniegts un uzraudzības iestāde nav pabeigusi tā novērtēšanu, kvalificētais uzticamības pakalpojumu sniedzējs var turpināt pamatoties uz to identitātes pārbaudes metožu izmantošanu, kuras noteiktas Regulas (ES) Nr. 910/2014 24. panta 1. punktā.";

43) regulas I pielikumu groza saskaņā ar šīs regulas I pielikumu;

44) regulas II pielikumu aizstāj ar šīs regulas II pielikuma tekstu;

45) regulas III pielikumu groza saskaņā ar šīs regulas III pielikumu;

46) regulas IV pielikumu groza saskaņā ar šīs regulas IV pielikumu;

47) regulu papildina ar jaunu V pielikumu, kas noteikts šīs regulas V pielikumā;

48) šajā regulā pievieno jaunu VI pielikumu.

52. pants

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

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

Briselē,

Eiropas Parlamenta vārdā – Padomes vārdā –

priekšsēdētājs priekšsēdētājs

I PIELIKUMS

Regulas 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

PRASĪBAS KVALIFICĒTĀM ELEKTRONISKĀ PARAKSTA RADĪŠANAS IERĪCĒM

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

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

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

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

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

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

III PIELIKUMS

Regulas 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 IV pielikuma j) punktu aizstāj ar šādu:

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

V PIELIKUMS

PRASĪBAS KVALIFICĒTAM ATRIBŪTU ELEKTRONISKAJAM APLIECINĀJUMAM

Kvalificēts atribūtu elektroniskais apliecinājums ietver:

(e) norādi, vismaz automatizētai apstrādei piemērotā formā, par to, ka apliecinājums ir izdots kā kvalificēts atribūtu elektroniskais apliecinājums;

(f) tādu datu kopumu, kas nepārprotami apliecina tā kvalificētā uzticamības pakalpojumu sniedzēja identitāti, kurš izdod kvalificēto atribūtu elektronisko apliecinājumu, ietverot vismaz informāciju par dalībvalsti, kurā pakalpojumu sniedzējs veic uzņēmējdarbību, un:

– juridiskai personai – nosaukumu un attiecīgā gadījumā reģistrācijas numuru atbilstīgi oficiālajos reģistros norādītajai informācijai,

– fiziskai personai – personas vārdu un uzvārdu;

(g) datu kopumu, kas nepārprotami apliecina subjektu, uz kuru attiecas apliecinātie atribūti. Ja tiek izmantots pseidonīms, to skaidri norāda;

(h) apliecināto atribūtu vai apliecinātos atribūtus, attiecīgā gadījumā ietverot informāciju, kas vajadzīga minēto atribūtu tvēruma noteikšanai;

(i) precīzu informāciju par apliecinājuma derīguma termiņa sākumu un beigām;

(j) apliecinājuma identifikācijas kodu, kam jābūt kvalificētā uzticamības pakalpojumu sniedzēja unikālam kodam, un attiecīgā gadījumā norādi par apliecinājumu shēmu, kuras daļa ir atribūtu apliecinājums;

(k) tā kvalificētā uzticamības pakalpojumu sniedzēja, kurš izdod apliecinājumu, kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu;

(l) vietu, kur bez maksas pieejams sertifikāts, kas apliecina g) punktā minēto kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu;

(m) informāciju par pakalpojumiem, kurus var izmantot, lai noskaidrotu kvalificētā apliecinājuma derīguma statusu, vai vietu, kur šie pakalpojumi pieejami.

VI PIELIKUMS

OBLIGĀTO ATRIBŪTU SARAKSTS

Papildus 45.d pantam dalībvalstis nodrošina, ka tiek veikti pasākumi, kas ļauj kvalificētiem atribūtu elektronisko apliecinājumu nodrošinātājiem pēc lietotāja pieprasījuma ar elektroniskiem līdzekļiem verificēt turpmāk norādīto atribūtu autentiskumu attiecībā pret attiecīgo autentisko avotu valsts līmenī vai ar tādu izraudzītu starpnieku palīdzību, kas atzīti valsts līmenī, saskaņā ar valsts vai Savienības tiesību aktiem un gadījumos, kad šie atribūti ir atkarīgi no autentiskiem avotiem publiskajā sektorā:

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. Publiskās atļaujas un licences
10. Finansiālie un uzņēmuma dati

VII PIELIKUMS

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

Elektroniskais atribūtu apliecinājums, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā, ietver šādu informāciju:

a) norādi – 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 kopumu, kas nepārprotami apliecina publisko iestādi, kura izdod atribūtu elektronisko apliecinājumu, tostarp vismaz dalībvalsti, kurā minētā publiskā iestāde ir izveidota, un tās nosaukumu un attiecīgā gadījumā tās reģistrācijas numuru, kas norādīts oficiālajos reģistros;

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

d) apliecināto atribūtu vai apliecinātos atribūtus, attiecīgā gadījumā ietverot informāciju, kas vajadzīga minēto atribūtu tvēruma noteikšanai;

e) precīzu informāciju par apliecinājuma derīguma termiņa sākumu un beigām;

f) apliecinājuma identifikācijas kodu, kam jābūt publiskās izdevējiestādes unikālam kodam, un attiecīgā gadījumā norādi par apliecinājumu shēmu, kuras daļa ir attiecīgais atribūtu apliecinājums;

g) izdevējiestādes kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu;

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

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

_____