

Briselē, 2021. gada 3. jūnijā
(OR. en)

9471/21

Starpiestāžu lieta:
2021/0136(COD)

TELECOM 242
COMPET 457
MI 432
DATAPROTECT 156
JAI 670
IA 108
CODEC 826

PRIEKŠLIKUMS

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore <i>Martine DEPREZ</i>
Saņemšanas datums:	2021. gada 3. jūnijs
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs <i>Jeppe TRANHOLM-MIKKELSEN</i>
K-jas dok. Nr.:	COM(2021) 281 final
Temats:	Priekšlikums - EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko Regulu (ES) Nr. 910/2014 groza attiecībā uz Eiropas digitālās identitātes regulējuma izveidi

Pielikumā ir pievienots dokuments COM(2021) 281 *final*.

Pielikumā: COM(2021) 281 *final*



Briselē, 3.6.2021.
COM(2021) 281 final

2021/0136 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA,
ar ko Regulu (ES) Nr. 910/2014 groza attiecībā uz Eiropas digitālās identitātes
regulējuma izveidi

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Šis paskaidrojuma raksts ir pievienots priekšlikumam Eiropas Parlamenta un Padomes regulai, ar ko groza Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulu (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū (*eIDAS*)¹. Juridiskā instrumenta mērķis ir nodrošināt pārrobežu lietošanas vajadzībām:

- piekļuvi ļoti drošiem un uzticamiem elektroniskās identitātes risinājumiem,
- to, ka, sniedzot sabiedriskus un privātus pakalpojumus, var paļauties uz uzticamiem un drošiem digitālās identitātes risinājumiem,
- to, ka fiziskas un juridiskas personas ir pilnvarotas lietot digitālās identitātes risinājumus,
- to, ka šie risinājumi ir saistīti ar dažādiem atribūtiem un ļauj mērķtiecīgi koplietot identitātes datus vienīgi konkrēta pieprasītā pakalpojuma vajadzībām,
- kvalificētu uzticamības pakalpojumu pieņemšanu ES un vienlīdzīgus nosacījumus to sniegšanai.

Tirgū parādās jauna vide, kurā uzmanība ir pārvirzīta no stingru digitālo identitāšu nodrošināšanas un lietošanas uz īpašu ar šīm identitātēm saistītu atribūtu nodrošināšanu un paļaušanos uz tiem. Aug pieprasījums pēc elektroniskās identitātes risinājumiem, kas šīs iespējas var sniegt, nodrošinot lielāku efektivitāti un augsta līmeņa uzticamību tādiem privātā un publiskā sektora pakalpojumiem visā ES, kuros ir nepieciešams identificēt un autentificēt lietotājus ar augstu uzticamības līmeni.

eIDAS regulas izvērtējums² atklāja, ka pašreizējā *eIDAS* regula nespēj apmierināt šīs jaunās tirgus prasības galvenokārt, tāpēc ka tā aprobežojas ar publisko sektoru, tiešsaistes privātajiem pakalpojumu sniedzējiem ir ierobežotas iespējas un sarežģīti pieslēgties sistēmai, paziņoto *eID* risinājumu pieejamība nav pietiekama visās dalībvalstīs un tā nav pietiekami elastīga, lai būtu piemērota dažādiem lietošanas gadījumiem. Turklāt identitātes risinājumi, kas neietilpst *eIDAS* darbības jomā, piemēram, tie, kurus piedāvā sociālo mediju nodrošinātāji un finanšu iestādes, rada bažas par privātumu un datu aizsardzību. Tie nevar efektīvi reaģēt uz jaunām tirgus prasībām un nesniedzas pāri robežām, lai risinātu īpašas tādu nozaru vajadzības, kurās identificēšana ir jutīga un kur vajadzīga augsta līmeņa noteiktība.

Kopš 2018. gada septembrī stājās spēkā regulas *eID* daļa, tikai 14 dalībvalstis ir paziņojušas vismaz vienu *eID* shēmu. Tādējādi tikai 59 % ES iedzīvotāju ir piekļuve uzticamām un drošām *eID* shēmām pāri robežām. Tikai septiņas shēmas ir pilnīgi mobilas un reaģē uz pašreizējām lietotāju cerībām. Tā kā ne visi tehniskie mezgli, kas nodrošina savienojumu ar *eIDAS* sadarbības regulējumu, darbojas pilnībā, pārrobežu piekļuve ir ierobežota; ļoti maz sabiedriskiem tiešsaistes pakalpojumiem, kas pieejami vietējā tirgū, var piekļūt pāri robežām, izmantojot *eIDAS* tīklu.

¹ OV L 257/73, 28.8.2014.

² [Pievienot atsauci, tiklīdz tā ir pieņemta.]

Piedāvājot Eiropas digitālās identitātes regulējumu, pamatojoties uz pārskatītu pašreizējo regulējumu, līdz 2030. gadam vismaz 80 % iedzīvotāju vajadzētu būt iespējai izmantot digitālu *ID* risinājumu, lai piekļūtu galvenajiem sabiedriskajiem pakalpojumiem. Turklāt drošībai un kontrolei, ko piedāvā Eiropas digitālās identitātes regulējums, būtu jāsniedz pilsoņiem un iedzīvotājiem pilnīga pārliecība par to, ka Eiropas digitālās identitātes regulējums sniedz ikvienam līdzekļus, lai kontrolētu to, kam ir piekļuve viņu digitālajam dvīnim un tieši kuriem dati. Tam būs vajadzīga arī augsta līmeņa drošība attiecībā uz visiem digitālās identitātes nodrošināšanas aspektiem, tostarp Eiropas digitālās identitātes maku un digitālās identitātes datu vākšanas, glabāšanas un izpaušanas infrastruktūru.

Turklāt pašreizējais *eIDAS* regulējums neattiecas uz elektronisko atribūtu, piemēram, medicīnisko sertifikātu vai profesionālās kvalifikācijas, nodrošināšanu, kas apgrūtinā šādu akreditācijas datu juridiskas atzīšanas nodrošināšanu elektroniskā formātā visā Eiropā. Turklāt *eIDAS* regula neļauj lietotājiem ierobežot identitātes datu koplietošanu, ciktāl tas ir absolūti nepieciešams pakalpojuma sniegšanai.

Lai gan *eIDAS* regulas izvērtējums liecina, ka uzticamības pakalpojumu sniegšanas regulējums ir bijis diezgan veiksmīgs, nodrošinot augsta līmeņa uzticamību un lielākās daļas uzticamības pakalpojumu apgūšanu un lietošanu, ir jādara vairāk, lai panāktu pilnīgu saskaņošanu un pieņemšanu. Kvalificētu tīmekļa vietņu autentifikācijas sertifikātu gadījumā iedzīvotājiem jāspēj uz tiem paļauties un gūt labumu no drošas un uzticamas informācijas par to, kas atbild par tīmekļa vietni, tādējādi mazinot krāpšanu.

Turklāt, lai reaģētu uz tirgus dinamiku un tehnoloģiju attīstību, ar šo priekšlikumu pašreizējais *eIDAS* uzticamības pakalpojumu saraksts ir paplašināts ar trim jauniem kvalificētiem uzticamības pakalpojumiem, proti, elektronisko arhivēšanas pakalpojumu sniegšanu, elektroniskajām virsgrāmatām un attālinātā elektroniskā paraksta un elektroniskā zīmoga radīšanas ierīcēm.

Šajā priekšlikumā piedāvāta arī saskaņota pieeja drošībai pilsoņiem, kuri paļaujas uz Eiropas digitālo identitāti, kas tos pārstāv tiešsaistē, un tiešsaistes pakalpojumu sniedzējiem, kuri varēs pilnībā paļauties uz digitālās identitātes risinājumiem un tos pieņemt neatkarīgi no tā, kur tie ir izsniegti. Šis priekšlikums paredz izmaiņas Eiropas digitālās identitātes risinājumu izdevējiem, nodrošinot kopēju tehnisko arhitektūru un atsauču regulējumu, kā arī kopīgus standartus, kas jāizstrādā sadarbībā ar dalībvalstīm. Lai nepieļautu to, ka jaunu digitālās identitātes risinājumu izstrāde dalībvalstīs palielina sadrumstalotību, ko izraisa atšķirīgu valstu risinājumu lietošana, ir vajadzīga saskaņota pieeja. Saskaņota pieeja arī stiprinās vienoto tirgu, jo tas ļautu pilsoņiem, citiem iedzīvotājiem un uzņēmumiem veikt identifikāciju tiešsaistē droši, ērti un vienoti visā ES, lai piekļūtu gan sabiedriskiem, gan privātiem pakalpojumiem. Lietotāji varētu paļauties uz uzlabotu elektroniskās identitātes un uzticamības pakalpojumu ekosistēmu, kas ir atzīta un pieņemta visā Savienībā.

Lai izvairītos no sadrumstalotības un šķēršļiem atšķirīgo standartu dēļ, Komisija vienlaikus ar šo priekšlikumu pieņems ieteikumu. Šajā ieteikumā būs izklāstīts kopējas pieejas atbalsta process, kas ļautu dalībvalstīm un citām ieinteresētajām personām sabiedriskajā un privātajā sektorā ciešā sadarbībā ar Komisiju izstrādāt rīkkopu, lai nepieļautu atšķirīgas pieejas un Eiropas digitālās identitātes regulējuma īstenošanas apdraudēšanu nākotnē.

- **Saskanība ar pašreizējiem noteikumiem konkrētajā politikas jomā**

Šā priekšlikuma pamatā ir pašreizējā *eIDAS* regula, dalībvalstu kā juridiskās identitātes nodrošinātāju loma un regulējums elektronisko uzticamības pakalpojumu sniegšanai Eiropas

Savienībā. Priekšlikums papildina un ir pilnīgi saskanīgs ar citiem ES līmeņa politikas instrumentiem, kuru mērķis ir izmantot digitālās pasaules iekšējā tirgus priekšrocības, jo īpaši, palielinot pilsoņu iespējas piekļūt pakalpojumiem pāri robežām. Šajā saistībā ar priekšlikumu tiek veikts Eiropadomes³ un Eiropas Komisijas priekšsēdētāja⁴ noteiktais politiskais uzdevums nodrošināt ES mēroga publisku elektronisko identitāšu regulējumu, kas sniedz ikvienam pilsonim vai iedzīvotājam piekļuvi drošai Eiropas e-identitātei, kuru var izmantot jebkurā vietā ES, lai veiktu identifikāciju un autentifikāciju nolūkā piekļūt pakalpojumiem publiskajā un privātajā sektorā, ļaujot pilsoņiem kontrolēt, kādi dati tiek paziņoti un kā tie tiek izmantoti.

- **Saskanība ar citām Savienības politikas jomām**

Priekšlikums saskan ar digitalizācijas prioritātēm, kas noteiktas stratēģijā “Eiropas digitālās nākotnes veidošana”⁵, un atbalstīs paziņojumā par digitālo desmitgadi norādīto mērķu sasniegšanu⁶. Personas datu apstrāde saskaņā ar šo regulu jāveic, pilnībā ievērojot Vispārīgo datu aizsardzības regulu (turpmāk “VDAR”)⁷. Turklāt ar šo regulu tiek ieviesti īpaši datu aizsardzības pasākumi.

Lai garantētu augsta līmeņa drošību, priekšlikums saskan arī ar Savienības politiku kibernetikas jomā⁸. Priekšlikums ir izstrādāts, lai mazinātu sadrumstalotību, piemērojot vispārīgas kibernetikas prasības uzticamības pakalpojumu sniedzējiem, kurus regulē ar *eIDAS* regulu.

Šis priekšlikums ir saskanīgs arī ar citām nozaru politikas jomā, kuru pamatā ir elektronisko identitāšu, atribūtu elektronisko apliecinājumu un citu uzticamības pakalpojumu lietošana. Tas ietver Vienotās digitālās vārtejas regulu⁹, prasības, kas jāievēro finanšu nozarē saistībā ar noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanu, sociālās drošības akreditācijas datu kopīgošanas, digitālās vadītāja apliecības vai nākotnes digitālo ceļošanas dokumentu iniciatīvas un citas iniciatīvas, kas paredzētas administratīvā sloga mazināšanai pilsoņiem un uzņēmumiem, kuri pilnībā paļaujas uz iespējām, ko sniedz procedūru digitālā pārveidošana gan publiskajā, gan privātajā sektorā. Turklāt maks ļaus izmantot kvalificētus elektroniskos parakstus, kas var atvieglot politisko līdzdalību¹⁰.

³ <https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf>

⁴ 2020. gada 16. septembra runa par stāvokli Savienībā, sk. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

⁵ Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un Sociālo lietu komitejai un Reģionu komitejai “Eiropas digitālās nākotnes veidošana”.

⁶ Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un Sociālo lietu komitejai un Reģionu komitejai “Digitālais kompass līdz 2030. gadam – Eiropas ceļam digitālajā gadu desmitā”.

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, OV L 119, 4.5.2016., 1. lpp.

⁸ https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

⁹ Eiropas Parlamenta un Padomes Regula (ES) 2018/1724 (2018. gada 2. oktobris), ar ko izveido vienotu digitālo vārteju, lai sniegtu piekļuvi informācijai, procedūrām un palīdzības un problēmu risināšanas pakalpojumiem, OV L 295, 21.11.2018., 1. lpp.

¹⁰ Eiropas Demokrātijas rīcības plāns, COM/2020/790 final.

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

• Juridiskais pamats

Šīs iniciatīvas mērķis ir atbalstīt Savienības pāreju uz digitālo vienoto tirgu. Pārrobežu sabiedriskajiem un privātajiem pakalpojumiem kļūstot arvien digitalizētākiem, ļaujoties uz digitālās identitātes risinājumu lietošanu, pastāv risks, ka ar pašreizējo tiesisko regulējumu iedzīvotāji turpinās saskarties ar šķēršļiem un nevarēs pilnībā netraucēti izmantot tiešsaistes pakalpojumus visā ES un saglabāt savu privātumu. Pastāv arī risks, ka pašreizējā uzticamības pakalpojumu tiesiskā regulējuma nepilnības varētu palielināt sadrumstalotību un mazināt uzticamību, ja to atstātu tikai dalībvalstu ziņā. Tādējādi LESD 114. pants ir noteikts kā attiecīgais šīs iniciatīvas juridiskais pamats.

• Subsidiaritāte (neekskluzīvas kompetences gadījumā)

Pilsoniem un uzņēmumiem vajadzētu būt iespējai gūt labumu no pieejamiem ļoti drošiem un uzticamiem digitālās identitātes risinājumiem, kurus var izmantot visā ES, un no atribūtu, kas saistīti ar identitāti, elektronisko apliecinājumu pārnēsāmības. Jaunākie tehnoloģiju sasniegumi, tirgus un lietotāju pieprasījums paredz, ka ir jābūt pieejamam lielākam skaitam lietotājam ērtu pārrobežu risinājumu, kas ļauj piekļūt tiešsaistes pakalpojumiem ES, ko *eIDAS* regula tās pašreizējā formātā nevar piedāvāt.

Lietotāji arvien vairāk pierod pie globāli pieejamiem risinājumiem, piemēram, pieņemot vienotu pierakstīšanās risinājumu lietošanu, ko lielākas sociālo mediju platformas piedāvā, lai piekļūtu tiešsaistes pakalpojumiem. Dalībvalstis pašas nevar novērst problēmas, ko tas rada attiecībā uz lielo pakalpojumu sniedzēju ietekmi tirgū, kam vajadzīga sadarbība un uzticamas *eID* ES līmenī. Turklāt vienā dalībvalstī izsniegti un pieņemti atribūtu elektroniskie apliecinājumi, piemēram, elektronisks veselības sertifikāts, citās dalībvalstīs bieži netiek juridiski atzīti un pieņemti. Tas rada risku, ka dalībvalstis turpina izstrādāt sadrumstalotus valstu risinājumus, kuri nevar darboties pāri robežām.

Lai gan uzticamības pakalpojumu sniegšana ir lielā mērā reglamentēta un darbojas saskaņā ar pašreizējo juridisko praksi, arī valstu prakse rada palielinātas sadrumstalotības risku.

Galū galā ES līmeņa intervence ir vislabāk piemērota, lai sniegtu pilsoniem un uzņēmumiem līdzekļus pārrobežu identifikācijas veikšanas un personas identitātes atribūtu un akreditācijas datu apmaiņai, izmantojot ļoti drošus un uzticamus digitālās identitātes risinājumus, kas atbilst ES datu aizsardzības noteikumiem. Tam vajadzīga uzticama un droša *eID* un tiesiskais regulējums, kas tos sasaista ar atribūtiem un akreditācijas datiem ES līmenī. Tikai ar ES līmeņa intervenci var paredzēt saskaņotus nosacījumus, kas nodrošinātu lietotāja kontroli un piekļuvi pārrobežu tiešsaistes digitāliem pakalpojumiem un sadarbības regulējumam, atvieglojot tiešsaistes pakalpojumu palaušanos uz drošu digitālās identitātes risinājumu lietošanu neatkarīgi no tā, kurā vietā ES tas ir izsniegts vai kur dzīvo pilsonis. Kā lielā mērā izklāstīts *eIDAS* regulas pārskatā, ir maz ticams, ka valstu intervence būtu vienlīdz lietderīga un efektīva.

• Proporcionalitāte

Šī iniciatīva ir proporcionāla izvirzītajiem mērķiem, nodrošinot piemērotu instrumentu, lai izveidotu sadarbības struktūru, kas vajadzīga, lai izveidotu ES digitālās identitātes ekosistēmu, pamatojoties uz dalībvalstu izdotajām juridiskajām identitātēm un kvalificētu un nekvalificētu digitālās identitātes atribūtu nodrošināšanu. Tā nepārprotami palīdz sasniegt mērķi uzlabot digitālo vienoto tirgu, izmantojot saskaņotāku tiesisko regulējumu. Saskaņotie Eiropas digitālās identitātes maki, kas dalībvalstīm jāizdod, pamatojoties uz kopējiem tehniskajiem standartiem, arī nodrošina kopēju ES pieeju, kas dod labumu lietotājiem un personām, kas ļauj uz drošu pārrobežu elektroniskās identitātes risinājumu pieejamību. Šajā iniciatīvā uzmanība ir pievērsta pašreizējās elektroniskās identifikācijas sadarbības

infrastruktūras ierobežojumiem, pamatojoties uz dažādu valstu elektroniskās identifikācijas shēmu savstarpēju atzišanu. Ņemot vērā izvirzītos mērķus, šī iniciatīva ir uzskatāma par pietiekami proporcionālu, un izmaksas varētu būt samērīgas ar potenciālajiem ieguvumiem. Ierosinātā regula palielinās finansiālās un administratīvās izmaksas, kas jāsedz dalībvalstīm kā Eiropas digitālās identitātes maka izdevējām, kā arī uzticamības pakalpojumu un tiešsaistes pakalpojumu sniedzējiem. Tomēr šīs izmaksas varētu kompensēt būtiskais potenciālais pilsoņu un lietotāju ieguvums, ko rada tieši arvien biežāka elektroniskās identitātes un atribūtu pakalpojumu pārrobežu atzišana un pieņemšana.

Nevar izvairīties no izmaksām, kas rodas, pakalpojumu sniedzējiem un tiešsaistes pakalpojumu sniedzējiem izstrādājot jaunus standartus un pielāgojoties tiem, ja ir jāsasniedz izmantojamības un pieejamības mērķis. Iniciatīvas mērķis ir izmantot ieguldījumus, ko dalībvalstis jau veikušas savās valsts identitātes shēmās. Turklāt priekšlikuma radītās papildu izmaksas ir paredzētas, lai atbalstītu saskaņošanu, un ir pamatotas ar cerību, ka ilgtermiņā tās samazinās administratīvo slogu un atbilstības izmaksas. Arī izmaksas, kas saistītas ar digitālās identitātes autentifikācijas atribūtu pieņemšanu regulētās nozarēs, var uzskatīt par nepieciešamām un samērīgām, ciktāl tās atbalsta vispārējā mērķa sasniegšanu un nodrošina līdzekļus, ar kuriem regulētās nozares var izpildīt juridiskos pienākumus likumīgi identificēt lietotāju.

- **Juridiskā instrumenta izvēle**

Regulas kā juridiskā instrumenta izvēle ir pamatota ar vajadzību nodrošināt vienādus nosacījumus iekšējā tirgū Eiropas digitālās identitātes piemērošanai, izmantojot saskaņotu regulējumu, kura mērķis ir radīt netraucētu sadarbību un nodrošināt Eiropas pilsoņus un uzņēmumus ar sabiedriskiem un privātiem pakalpojumiem visā Savienībā ar ļoti drošām un uzticamām *eID*.

3. EX-POST IZVĒRTĒJUMU, APSPRIEŠANOS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

- **Ex post izvērtējumi / spēkā esošo tiesību aktu atbilstības pārbaudes**

Spēkā esošās *eIDAS* regulas izvērtējums tika veikts pārskatīšanas procesā, kas paredzēts *eIDAS* regulas 49. pantā. Galvenie izvērtējuma konstatējumi attiecībā uz elektronisko identitāti ir tādi, ka *eIDAS* potenciāls nav izmantots. Ir paziņots tikai ierobežots skaits *eID*, tādējādi paziņotās *eID* shēmas aptver tikai aptuveni 59 % ES pilsoņu. Turklāt paziņoto *eID* pieņemšana gan dalībvalstu, gan pakalpojumu sniedzēju līmenī ir ierobežota. Šķiet arī, ka tikai daži no pakalpojumiem, kas pieejami, izmantojot vietējo *eID*, ir saistīti ar valsts *eIDAS* infrastruktūru. Izvērtējuma pētījumā arī konstatēts, ka *eIDAS* regulas pašreizējā darbības joma un uzmanība ir pievērsta ES dalībvalstu paziņotajām *eID* shēmām un tam, ka piekļuves nodrošināšana tiešsaistes sabiedriskajiem pakalpojumiem šķiet pārāk ierobežota un nepietiekama. Lielākā daļa elektroniskās identitātes un attālinātās autentifikācijas vajadzību aizvien ir privātajā sektorā, jo īpaši tādās jomās kā bankas, telekomunikāciju un platformu operatori, kuriem ar likumu noteikts, ka jāpārbauda savu klientu identitāte. *eIDAS* regulas pievienotā vērtība attiecībā uz elektronisko identitāti ir ierobežota tās mazā pārklājuma, piemērošanas un lietošanas dēļ.

Šajā priekšlikumā noteiktās problēmas ir saistītas ar pašreizējā *eIDAS* regulējuma nepilnībām un būtiskām kontekstuālām izmaiņām attiecībā uz tirgiem, sabiedrības un tehnoloģiju sasniegumiem, kas izraisa jaunas lietotāju un tirgus vajadzības.

- **Apspriešanas ar ieinteresētajām personām**

Atklāta sabiedriskā apspriešana tika sākta 2020. gada 24. jūlijā, un tā noslēdzās 2020. gada 2. oktobrī. Kopumā Komisija saņēma 318 atbildes. Komisija saņēma arī 106 atbildes uz mērķorientētu ieinteresēto personu apsekojumu. Dalībvalstu viedokļi ir apkopoti arī dažādās divpusējās un daudzpusējās sanāksmēs un apsekojumos, kas tika organizēti kopš 2020. gada sākuma. Tas jo īpaši ietver *eIDAS* sadarbības tīklā esošo dalībvalstu pārstāvju aptauju 2020. gada jūlijā un augustā un dažādus specializētus darbseminārus. Komisija arī rīkoja padziļinātas intervijas ar nozares pārstāvjiem un divpusējās sanāksmēs tikās ar uzņēmumu pārstāvjiem no dažādām nozarēm (piemēram, e-komercija, veselības aprūpe, finanšu pakalpojumi, telekomunikāciju operatori, aprīkojuma ražotāji u. c.).

Liela daļa atklātās sabiedriskās apspriešanas respondentu atzinīgi novērtēja vienotas un vispārpieņemtas digitālās identitātes izveidi, pamatojoties uz dalībvalstu izsniegtajām juridiskajām identitātēm. Dalībvalstis lielākoties atbalsta nepieciešamību pastiprināt pašreizējo *eIDAS* regulu, sniedzot pilsoņiem iespēju piekļūt gan sabiedriskiem, gan privātiem pakalpojumiem, un atzīt nepieciešamību izveidot uzticamības pakalpojumu, kas ļautu izsniegt un izmantot pāri robežām atribūtu elektroniskos apliecinājumus. Kopumā dalībvalstis uzsvēra nepieciešamību veidot Eiropas digitālās identitātes regulējumu, pamatojoties uz valstu risinājumu pieredzi un priekšrocībām, cenšoties rast sinerģiju un gūstot labumu no veiktajiem ieguldījumiem. Daudzas ieinteresētās personas atsaucās uz to, kā Covid-19 pandēmija pierādīja drošas, attālinātas identifikācijas nozīmi visiem, lai piekļūtu sabiedriskiem un privātiem pakalpojumiem. Attiecībā uz uzticamības pakalpojumiem vairums dalībnieku ir vienprātis, ka pašreizējais regulējums ir bijis veiksmīgs, tomēr bija nepieciešami daži papildu pasākumi, lai vēl vairāk saskaņotu noteiktu praksi saistībā ar attālinātu identifikāciju un valsts pārraudzību. Ieinteresētās personas, kuru bāzē ir galvenokārt ir valsts klienti, pauda lielākas šaubas par Eiropas digitālās identitātes regulas pievienoto vērtību.

Publiskais un privātais sektors arvien vairāk uztver digitālās identitātes makus kā piemērotāko instrumentu, kas ļauj lietotājiem izvēlēties, kad un ar kuru privāto pakalpojumu sniedzēju koplietot dažādus atribūtus atkarībā no lietošanas gadījuma un attiecīgajam darījumam nepieciešamās drošības. Digitālās identitātes, kuru pamatā ir mobilajās ierīcēs droši glabāti digitālie maki, tika noteiktas kā galvenais nākotnei pielāgota risinājuma elements. Gan privātais tirgus (piemēram, *Apple*, *Google*, *Thales*), gan valdības jau iet šajā virzienā.

- **Ekspertu atzinumu pieprasīšana un izmantošana**

Priekšlikuma pamatā ir informācija, kas savākta apspriešanās ar ieinteresētajām personām *eIDAS* regulas ietekmes novērtējuma un izvērtēšanas ziņojumu vajadzībām, ņemot vērā pārskatīšanas pienākumus, kas noteikti *eIDAS* regulas 49. pantā. Tika organizētas daudzas sanāksmes ar dalībvalstu pārstāvjiem un ekspertiem.

- **Ietekmes novērtējums**

Šim priekšlikumam tika veikta ietekmes novērtēšana. Regulējuma kontroles padome 2021. gada 19. martā sniedza negatīvu atzinumu ar dažām piezīmēm. Pēc atkārtoti iesniegtā dokumenta pārskatīšanas 2021. gada 5. maijā padome sniedza pozitīvu atzinumu.

Komisija izskata dažādus politikas variantus, ar ko varētu sasniegt šīs iniciatīvas vispārīgo mērķi — nodrošināt pareizu iekšējā tirgus darbību, jo īpaši attiecībā uz ļoti drošu un uzticamu elektroniskās identitātes risinājumu nodrošināšanu un lietošanu.

Ietekmes novērtējumā pārbaudīts bāzes scenārijs, politikas varianti un to ietekme uz trim izskatītajiem politikas variantiem. Katrā variantā piedāvāta politisku apsvērumu izvēle, pamatojoties uz mērķa vērienu. Pirmajā variantā piedāvāts zems mērķis un pasākumu kopums, kura galvenais mērķis ir stiprināt pašreizējās *eIDAS* regulas efektivitāti un lietderību. Paredzot obligātu valstu *eID* paziņošanu un racionalizējot esošos pieejamos instrumentus, lai panāktu savstarpēju atzīšanu, pirmā varianta pamatā ir pilsoņu vajadzību apmierināšana, paļaujoties uz to, ka ir pieejamas dažādas valstu *eID* shēmas, kuru mērķis ir kļūt sadarbīpējām.

Otrajā variantā ir paredzēts vidēja līmeņa mērķis, un tas galvenokārt ir vērsts uz to, lai paplašinātu drošas datu apmaiņas iespējas saistībā ar identitāti, papildinot valdības *eID* un atbalstot pašreizējo pāreju uz identitātes pakalpojumiem, kuru pamatā ir atribūti. Šā varianta mērķis būtu apmierināt lietotāju pieprasījumu un izveidot jaunu kvalificētu uzticamības pakalpojumu tādu atribūtu elektronisku apliecinājumu sniegšanai, kas saistīti ar uzticamiem avotiem un izpildāmi pāri robežām. Tas paplašinātu pašreizējās *eIDAS* regulas darbības jomu un atbalstītu pēc iespējas vairāk lietošanas gadījumu, paļaujoties uz nepieciešamību ar lielu pārliecību pārbaudīt identitātes atribūtus, kas saistīti ar personu.

Trešajā un vēlamajā variantā ir paredzēts augstākais mērķis, un tas ir vērsts uz to, lai regulētu dalībvalstu izdota ļoti droša personīgā digitālās identitātes maka nodrošināšanu. Vēlamais variants tika uzskatīts par piemērotu šīs iniciatīvas mērķu sasniegšanai visefektīvākajā veidā. Lai pilnībā sasniegtu politikas mērķus, izvēlēta varianta pamatā ir lielākā daļa pasākumu, kas novērtēti saskaņā ar pirmo variantu (paļaušanās uz dalībvalstu apstiprinātām juridiskām identitātēm un savstarpēji atzītu *eID* līdzekļu pieejamību) un otro variantu (atribūtu elektroniski apliecinājumi, kas juridiski atzīti pāri robežām).

Attiecībā uz uzticamības pakalpojumu vispārējo regulējumu mērķa vēriens paredz tādu pasākumu kopumu, kuriem nav nepieciešama pakāpeniska pieeja, lai sasniegtu politikas mērķus.

Jaunais kvalificētais uzticamības pakalpojums elektronisko parakstu un zīmogu radīšanas ierīču pārvaldībai sniegtu lielu drošību, vienotību, juridisko noteiktību un patērētāju izvēles priekšrocības saistībā gan ar kvalificētu parakstu radīšanas ierīču sertifikāciju, gan prasībām, kas jāizpilda kvalificētiem uzticamības pakalpojumu sniedzējiem, kas pārvalda šādas ierīces. Jaunie noteikumi pastiprinātu uzticamības pakalpojumu sniegšanas vispārējo tiesisko un uzraudzības regulējumu.

Politikas variantu ietekme uz dažādām ieinteresēto personu kategorijām sīkāk ir paskaidrota ietekmes novērtējuma 3. pielikumā, kas papildina šo iniciatīvu. Novērtējums ir gan kvantitatīvs, gan kvalitatīvs. Ietekmes novērtējuma pētījums liecina, ka minimālās skaitliski izsakāmās izmaksas var lēst 3,2 miljardu euro apmērā, jodažas izmaksu pozīcijas nevar izteikt skaitliski. Tiek lēsts, ka kopējo skaitliski izsakāmo ieguvumu vērtība ir no 3,9 miljardiem euro līdz 9,6 miljardiem euro. Attiecībā uz plašāku ekonomisko ietekmi izvēlētajam variantam ir pozitīva ietekme uz inovāciju, starptautisko tirdzniecību un konkurētspēju, tas veicina ekonomikas izaugsmi un radīs papildu ieguldījumus digitālās identitātes risinājumos. Piemēram, paredzams, ka papildu ieguldījums 500 miljonu euro apmērā, ko izraisa izmaiņas tiesību aktos saskaņā ar 3. variantu, pēc desmit gadiem radīs ieguvumus 1,268 miljonu euro apmērā (pieņemot 67 %).

Paredzams, ka izvēlētais risinājums pozitīvi ietekmēs nodarbinātību, radot no 5000 līdz 27 000 papildu darbavieta piecos gados pēc īstenošanas. Tas skaidrojams ar papildu

ieguldījumiem un samazinātām izmaksām uzņēmumiem, kuri paļaujas uz *eID* risinājumu lietošanu.

Paredzams, ka pozitīvā ietekme uz vidi būs vislielākā trešajā variantā, kas, kā paredzams, maksimāli uzlabos *eID* ieviešanu un lietošanu, pozitīvi ietekmējot emisiju samazināšanu saistībā ar sabiedrisko pakalpojumu sniegšanu.

Elektroniskās virsgrāmatas sniedz lietotājiem pierādījumus un nemainīgu revīzijas liecību par darījumu un datu ierakstu secību, nodrošinot datu integritāti. Lai gan šis uzticamības pakalpojums nebija ietekmes novērtējuma daļa, tā pamatā ir pastāvošie uzticamības pakalpojumi, jotas apvieno datu laika zīmogošanu un to secības noteikšanu ar pārbaudi par datu sagatavotāju, kas līdzinās e-parakstīšanai. Šis uzticamības pakalpojums ir nepieciešams, lai novērstu iekšējā tirgus sadrumstalotību, nosakot vienotu Eiropas mēroga regulējumu, kas ļauj atzīt uzticamības pakalpojumus pāri robežām, atbalstot kvalificētu elektronisko virsgrāmatu lietošanu. Savukārt datu integritāte ir ļoti svarīga datu apkopošanai no decentralizētiem avotiem, pašpietiekamiem identitātes risinājumiem, īpašumtiesību piešķiršanai digitālajiem aktīviem, uzņēmējdarbības procesu reģistrēšanai, lai pārbaudītu atbilstību ilgtspējas kritērijiem, un dažādiem kapitāla tirgus lietošanas gadījumiem.

- **Normatīvā atbilstība un vienkāršošana**

Šis priekšlikums paredz pasākumus, kas attieksies uz valsts iestādēm, pilsoņiem un tiešsaistes pakalpojumu sniedzējiem. Tas samazinās valsts iestāžu administratīvās un atbilstības izmaksas un darbības izmaksas un samazinās tiešsaistes pakalpojumu sniedzēju izdevumus saistībā ar drošību. Pilsoņi gūs labumu no ietaupījumiem, samazinoties administratīvajam slogam, pilnībā paļaujoties uz digitāliem identifikācijas līdzekļiem un iespēju droši apmainīties ar digitālās identitātes atribūtiem ar vienādu juridisko vērtību pāri robežām. Elektroniskās identitātes nodrošinātāji gūs labumu arī no atbilstības izmaksu ietaupījumiem.

- **Pamattiesības**

Tā kā personas dati ietilpst dažu regulas elementu darbības jomā, ir izstrādāti pasākumi, lai nodrošinātu pilnīgu atbilstu tiesību aktiem datu aizsardzības jomā. Piemēram, ar priekšlikumu tiek uzlabotas datu koplietošanas iespējas un atļauta diskrēta datu izpaušana. Izmantojot Eiropas digitālās identitātes maku, lietotājs varēs kontrolēt datu apjomu, kas sniegts atkarīgajām personām, un tiks informēts par atribūtiem, kas nepieciešami konkrēta pakalpojuma sniegšanai. Pakalpojumu sniedzēji informē dalībvalstis par nodomu paļauties uz Eiropas digitālās identitātes maku, kas ļautu dalībvalstīm kontrolēt to, ka pakalpojumu sniedzēji varētu pieprasīt sensitīvu datu kopas, piemēram, saistībā ar veselību, tikai saskaņā ar valsts tiesību aktiem.

4. IETEKME UZ BUDŽETU

Lai optimāli sasniegtu šīs iniciatīvas mērķus, ir jāfinansē vairākas darbības gan Komisijas līmenī, kur laikposmā no 2022. līdz 2027. gadam ir paredzēts piešķirt aptuveni 60 pilnslodzes ekvivalentu, gan dalībvalstu līmenī, tām aktīvi piedaloties ekspertu grupās un komitejās, kas saistītas ar iniciatīvas darbu un kuru sastāvā ir dalībvalstu pārstāvji. Kopējie finanšu līdzekļi, kas vajadzīgi, lai īstenotu priekšlikumu 2022.–2027. gadā, būs līdz 30,825 miljoniem euro, tostarp administratīvās izmaksas 8,825 miljonu euro apmērā un darbības izdevumi līdz 22 miljonu euro apmērā, ko sedz izdevumu programma “Digitālā Eiropa” (līdz brīdim, kad panākta vienošanās). Finansējums atbalstīs izmaksas, kas saistītas ar *eID* un uzticamības pakalpojumu pamatelementu uzturēšanu, izstrādi, mītināšanu, izmantošanu un atbalstu. Tas

var atbalstīt arī dotācijas pakalpojumus pievienošanai Eiropas digitālās identitātes maka ekosistēmai, standartu un tehnisko specifikāciju izstrādei. Visbeidzot, finansējums arī atbalstīs ikgadēju apsekojumu un pētījumu veikšanu par to, cik efektīva un lietderīga ir regula tās mērķu sasniegšanā. Ar šo iniciatīvu saistītajā “finansu pārskatā” sniegts sīki izklāstīts saistīto izmaksu pārskats.

5. CITI ELEMENTI

• **Īstenošanas plāni un uzraudzības, novērtēšanas un ziņošanas kārtība**

Ietekme tiks uzraudzīta un novērtēta saskaņā ar Labāka regulējuma pamatnostādņēm, aptverot ierosinātās regulas īstenošanu un piemērošanu. Uzraudzības kārtība ir svarīga priekšlikuma daļa, jo īpaši, ņemot vērā pašreizējā ziņošanas regulējuma nepilnības, kā izklāstīts izvērtējuma pētījumā. Papildus ziņošanas prasībām, kas ieviestas ierosinātajā regulā nolūkā nodrošināt labāku datu un analīzes bāzi, ar uzraudzības regulējumu tiks uzraudzīts: 1) cik lielā mērā nepieciešamās izmaiņas ir ieviestas saskaņā ar pieņemtajiem pasākumiem; 2) vai ir ieviestas nepieciešamās izmaiņas attiecīgajās valstu sistēmās; 3) vai ir ievērotas nepieciešamās izmaiņas regulēto struktūru atbilstības pienākumos. Eiropas Komisija (1., 2. un 3.) un valstu kompetentās iestādes (2. un 3.) atbildēs par datu vākšanu, pamatojoties uz iepriekš noteiktiem rādītājiem.

Saistībā ar ierosinātā instrumenta piemērošanu Eiropas Komisija un valstu kompetentās iestādes, veicot ikgadējus apsekojumus, novērtēs: 1) piekļuvi *eID* līdzekļiem visiem ES pilsoņiem; 2) palielinātu *eID* shēmu atzīšanu un pieņemšanu pāri robežām; 3) pasākumus, kas paredzēti, lai stimulētu to, ka privātais sektors pieņem un attīsta jaunus digitālās identitātes pakalpojumus.

Kontekstuālo informāciju apkopos Eiropas Komisija, izmantojot ikgadējus apsekojumus par: 1) digitālo identitāšu tirgus lielumu; 2) ar digitālo identitāti saistītā publiskā iepirkuma izdevumiem; 3) to uzņēmumu īpatsvaru, kuri savus pakalpojumus piedāvā tiešsaistē; 4) tādu tiešsaistes darījumu īpatsvaru, kuros vajadzīga stingra klienta identifikācija; 5) to ES pilsoņu īpatsvaru, kuri izmanto tiešsaistes privātos un sabiedriskos pakalpojumus.

• **Detalizēts konkrētu priekšlikuma noteikumu skaidrojums**

Regulas projekta 6.a pantā noteikts, ka dalībvalstīm jāizdod Eiropas digitālās identitātes maks paziņotajā *eID* shēmā atbilstīgi kopīgiem tehniskiem standartiem pēc obligāta atbilstības novērtējuma un brīvprātīgas sertifikācijas saskaņā ar Eiropas kiberdrošības sertifikācijas regulējumu, kā noteikts Kiberdrošības aktā. Tajā iekļauti noteikumi, lai nodrošinātu, ka fiziskām un juridiskām personām ir iespēja droši pieprasīt un iegūt, uzglabāt, apvienot un izmantot personas identifikācijas datus un atribūtu elektroniskos apliecinājumus, lai veiktu autentifikāciju tiešsaistē un bezsaistē, kā arī ļautu piekļūt precēm un tiešsaistes sabiedriskiem un privātiem pakalpojumiem, ko kontrolē lietotājs. Šī sertifikācija neskar VDAR tādā nozīmē, ka personas datu apstrādes darbības, kas saistītas ar Eiropas digitālās identitātes maku, var sertificēt tikai saskaņā ar VDAR 42. un 43. pantu.

Priekšlikuma 6.b pantā ir izklāstīti īpaši noteikumi par prasībām, kas attiecas uz atkarīgajām personām, lai novērstu krāpšanu un nodrošinātu personas identifikācijas datu un Eiropas digitālās identitātes maka atribūtu elektronisko apliecinājumu autentifikāciju.

Lai vairāk elektroniskās identifikācijas līdzekļu varētu lietot pāri robežām un lai uzlabotu paziņoto elektroniskās identifikācijas shēmu savstarpējas atzīšanas procesa efektivitāti, 7. pantā ir noteikts, ka dalībvalstīm obligāti jāpaziņo vismaz viena elektroniskās

identifikācijas shēma. Turklāt 11.a pantā ir pievienoti noteikumi, kas atvieglo unikālu identifikāciju, lai nodrošinātu fizisku personu unikālu un noturīgu identifikāciju. Tas attiecas uz gadījumiem, kad identifikācija ir nepieciešama saskaņā ar tiesību aktiem, piemēram, veselības aprūpes jomā, finanšu jomā, lai izpildītu noziedzīgi iegūtu līdzekļu legalizācijas novēršanas pienākumus, vai arī tiesu vajadzībām. Šim nolūkam dalībvalstīm būs jāiekļauj unikāls un noturīgs identifikators minimālajā personas identifikācijas datu kopā. Dalībvalstu iespēja paļauties uz sertifikāciju, lai nodrošinātu atbilstību regulai un tādējādi aizstātu vienādranga pārskatīšanas procesu, uzlabo savstarpējās atzīšanas efektivitāti.

3. iedaļā ir izklāstīti jauni noteikumi par pārrobežu paļaušanos uz Eiropas digitālās identitātes maku, lai nodrošinātu, ka lietotāji var paļauties uz Eiropas digitālās identitātes maku lietošanu, lai piekļūtu tiešsaistes pakalpojumiem, ko sniedz publiskā sektora struktūras un privātie pakalpojumu sniedzēji, pieprasot stingru lietotāja autentifikāciju.

III nodaļas par uzticamības pakalpojumiem 14. pants par starptautiskiem aspektiem ir grozīts, lai dotu Komisijai iespēju pieņemt īstenošanas lēmumus, kas papildus savstarpējās atzīšanas nolīgumu izmantošanai saskaņā ar LESD 218. pantu apliecina trešās valstīs reģistrētiem uzticamības pakalpojumiem piemēroto prasību un to sniegto pakalpojumu līdzvērtīgumu.

Attiecībā uz vispārīgiem noteikumiem, kas piemērojami uzticamības pakalpojumiem, tostarp kvalificētiem uzticamības pakalpojumu sniedzējiem, ir grozīts 17., 18., 20., 21. un 24. pants, lai tos pielāgotu noteikumiem, ko ES piemēro tīkla un informācijas drošībai. Attiecībā uz metodēm, kas kvalificētiem uzticamības pakalpojumu sniedzējiem jāizmanto fizisko vai juridisko personu, kurām izsniegti kvalificēti sertifikāti, identitātes pārbaudei, ir saskaņoti un precizēti noteikumi par attālināto identifikācijas līdzekļu lietošanu, lai nodrošinātu vienādu noteikumu piemērošanu visā ES.

III nodaļā ir jauns 29.a pants, kurā noteiktas prasības kvalificētam pakalpojumam, kas paredzēts, lai pārvaldītu attālinātas elektroniskā paraksta radīšanas ierīces. Jaunais kvalificētais uzticamības pakalpojums būtu tieši saistīts ar ietekmes novērtējumā minētajiem un novērtētajiem pasākumiem un balstītos tajos, jo īpaši pasākumos par “attālinātas elektroniskās parakstīšanas sertifikācijas procesa saskaņošanu” un citos pasākumos, kuri mudina dalībvalstis saskaņot uzraudzības praksi.

Lai nodrošinātu, ka lietotāji var noteikt, kas atbild par tīmekļa vietni, 45. pants ir grozīts, pieprasot, lai tīmekļa pārlūkprogrammu nodrošinātāji atvieglotu kvalificētu sertifikātu lietošanu tīmekļa vietņu autentifikācijai.

III nodaļā ir trīs jaunas iedaļas.

Jaunajā 9. iedaļā ir iekļauti noteikumi par atribūtu elektronisko apliecinājumu juridiskajām sekām, to lietošanu noteiktās nozarēs un prasības atribūtu kvalificētiem apliecinājumiem. Lai nodrošinātu augstu uzticamības līmeni, 45.d pantā ir iekļauti noteikumi par atribūtu pārbaudi, salīdzinot ar autentiskiem avotiem. Lai pārliecinātos, ka Eiropas digitālās identitātes maku lietotāji var gūt labumu no atribūtu elektronisko apliecinājumu pieejamības un lai šie apliecinājumi tiktu izsniegti Eiropas digitālās identitātes maku vajadzībām, 45.e pantā ir iekļauta prasība. Savukārt 45.f pantā ir iekļauti papildu noteikumi par atribūtu pakalpojumu elektroniskas apliecināšanas nodrošināšanu, tostarp par personas datu aizsardzību.

Jaunā 10. iedaļa ļauj sniegt kvalificētus elektroniskās arhivēšanas pakalpojumus ES līmenī. 45.g pants par kvalificētiem elektroniskās arhivēšanas pakalpojumiem papildina 34. un 40. pantu par kvalificētu elektronisko parakstu un kvalificētu elektronisko zīmogu saglabāšanas pakalpojumiem.

Ar jauno 11. sadaļu ir izveidots uzticamības pakalpojumu regulējums attiecībā uz elektronisko virsrāmatu un kvalificētu elektronisko virsrāmatu izveidi un uzturēšanu. Elektroniska

virsrāmata apvieno datu laika zīmogošanu un to secības noteikšanu ar pārlecību par datu sagatavotāju, kas līdzinās e-parakstīšanai un sniedz papildu labumu — dod iespēju veikt decentralizētāku pārvaldību, kas ir piemērota daudzu ieinteresēto personu sadarbībai. Tas ir svarīgi dažādos lietošanas gadījumos, kuros var izmantot elektroniskās virsrāmatas.

Elektroniskās virsrāmatas palīdz uzņēmumiem samazināt izmaksas, padarot daudzu ieinteresēto personu koordināciju efektīvāku, drošāku, un tās atvieglo regulatīvo uzraudzību. Ja nav Eiropas regulējuma, pastāv risks, ka valstu likumdevēji noteiks atšķirīgus valsts standartus. Lai novērstu sadrumstalotību, ir jānosaka vienots Eiropas mēroga regulējums, kas ļaus atzīt uzticamības pakalpojumus pāri robežām, atbalstot elektronisko virsrāmatu lietošanu. Šis Eiropas mēroga mezglu operatoru standarts tiks piemērots neatkarīgi no citiem ES sekundārajiem tiesību aktiem. Ja elektroniskās virsrāmatas tiek izmantotas, lai atbalstītu obligāciju emisiju un/vai tirdzniecību, vai kryptoaktīvu vajadzībām, lietošanas gadījumiem vajadzētu būt saderīgiem ar visiem piemērojamajiem finanšu noteikumiem, piemēram, Finanšu instrumentu tirgu direktīvu¹¹, Maksājumu pakalpojumu direktīvu¹² un Regulu par kryptoaktīvu tirgiem¹³. Ja lietošanas gadījumi ir saistīti ar personas datiem, pakalpojumu sniedzējiem būs jāievēro VДАР.

75 % no visiem elektronisko virsrāmatu lietošanas gadījumiem banku un finanšu jomā bija 2017. gadā. Pašlaik elektronisko virsrāmatu lietošanas gadījumi kļūst arvien daudzveidīgāki — 17 % saziņas un plašsaziņas līdzekļu jomā; 15 % apstrādes rūpniecībā un dabas resursu jomā, 10 % valdības sektorā, 8 % apdrošināšanas jomā, 5 % mazumtirdzniecībā, 6 % transporta jomā, 5 % komunālo pakalpojumu jomā¹⁴.

Visbeidzot, VI nodaļā ir jauns 48.b pants, lai nodrošinātu statistikas apkopošanu par Eiropas digitālās identitātes maka lietošanu nolūkā uzraudzīt grozītās regulas efektivitāti.

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 un Direktīvu 2011/61/ES, *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 Priekšlikums Eiropas Parlamenta un Padomes regulai par kryptoaktīvu tirgiem un ar ko groza Direktīvu (ES) 2019/1937, COM/2020/593 final.

¹⁴ *Gartner, Blockchain Evolution, 2020. gads.*

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 atzinumu¹⁵,

saskaņā ar parasto likumdošanas procedūru,

tā kā:

- (1) Komisija 2020. gada 19. februāra paziņojumā "Eiropas digitālās nākotnes veidošana"¹⁶ 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.
- (2) Savos 2020. gada 1.–2. oktobra secinājumos¹⁷ Eiropadome aicināja Komisiju ierosināt izstrādāt drošas publiskas elektroniskas identifikācijas, tostarp sadarbīgu 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"¹⁸ 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 un vienoti identificēties visā Savienībā. 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, universitātes grādu, kas likumīgi atzīts un akceptēts visur Savienībā. Eiropas digitālās identitātes regulējuma mērķis ir panākt pāreju no paļaušanās vienīgi uz valsts digitālās identitātes

¹⁵ OV C (..), (..), (..) lpp.

¹⁶ COM/2020/67 final

¹⁷ <https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/>

¹⁸ COM/2021/118 final/2

risinājumiem uz Eiropas līmenī derīgu atribūtu elektronisko apliecinājumu sniegšanu. Atribūtu elektronisko apliecinājumu sniedzējiem būtu jāgūst labums no skaidra un vienota noteikumu kopuma, un valsts iestādēm vajadzētu būt iespējai paļauties uz noteikta formāta elektroniskiem dokumentiem.

- (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 sadarbībai. 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. 2016/679¹⁹ 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.
- (7) Jāparedz saskaņoti nosacījumi, lai izveidotu dalībvalstu izdotu Eiropas digitālās identitātes maku regulējumu, kam būtu jānodrošina 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, 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 atbilstību Savienības tiesību aktiem vai valsts tiesību aktiem, kas atbilst Savienības tiesību aktiem, pakalpojumu sniedzējiem būtu jāpaziņo dalībvalstīm par nodomu paļauties uz Eiropas digitālās identitātes makiem. Tas ļaus dalībvalstīm pasargāt lietotājus no krāpšanas un novērst identitātes datu un atribūtu elektronisko apliecinājumu nelikumīgu lietošanu, kā arī nodrošināt, ka atkarīgās personas var pārbaudīt sensitīvo datu, piemēram, veselības datu, apstrādi saskaņā ar Savienības tiesību aktiem vai valsts tiesību aktiem.
- (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” pārlicības 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

¹⁹ 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.

pārstāvības pilnvaras un e-pilnvaras, dalībvalstīm būtu jāizdod Eiropas digitālās identitātes maki, pamatojoties uz kopīgiem standartiem, lai nodrošinātu nepārtrauktu sadarbību 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.

- (10) Lai sasniegtu augstu drošības un uzticamības līmeni, šajā regulā ir noteiktas prasības Eiropas digitālās identitātes makiem. Eiropas digitālās identitātes maku atbilstība šīm prasībām būtu jāapstiprina akreditētām publiskā vai privātā sektora struktūrām, ko norīkojušas dalībvalstis. Paļāvībai uz sertifikācijas shēmu, kuras pamatā ir ar dalībvalstīm saskaņotu standartu pieejamība, būtu jānodrošina augsts uzticamības un sadarbības līmenis. Veicot sertifikāciju, jo īpaši būtu jāpaļaujas uz attiecīgajām Eiropas kiberdrošības sertifikācijas shēmām, kas izveidotas saskaņā ar Regulu (ES) 2019/881²⁰. Šāda sertifikācija nedrīkstētu skart sertifikāciju attiecībā uz personas datu apstrādi saskaņā ar Regulu (EK) 2016/679.
- (11) Eiropas digitālās identitātes makiem būtu jāgarantē augstākais drošības līmenis personas datiem, kurus izmanto autentifikācijai, neatkarīgi no tā, vai šie dati tiek glabāti lokāli vai mākonddatošanas risinājumos atkarībā no dažādiem riska līmeņiem. Biometrijas lietošana autentifikācijas vajadzībām ir viena no identifikācijas metodēm, kas nodrošina augstu ticamības līmeni, jo īpaši, ja to lieto kopā ar citiem autentifikācijas elementiem. Tā kā biometrija ir unikāls personas raksturlielums, lai to lietotu, ir jāveic organizatoriski un drošības pasākumi, kas ir proporcionāli riskam, ko šāda apstrāde var radīt fizisku personu tiesībām un brīvībām, un kas atbilst Regulai 2016/679.
- (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 sadarbību, 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. 2019/1157²¹ 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.

²⁰ 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.

²¹ 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.).

- (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 identitātes karšu shēmām saskaņā ar Regulu 910/2014.
- (15) Pašreizējo paziņošanas un profesionālizvērtēšanas 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 sadarbības 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 vai brīvprātīgas IKT drošības sertifikācijas shēmas, piemēram, sertifikācijas shēmas, 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 sadarbību un drošību.
- (17) Pakalpojumu sniedzēji izmanto identitātes datus, ko nodrošina personu identifikācijas datu kopums, kas pieejams no elektroniskās identifikācijas shēmām saskaņā ar Regulu (ES) Nr. 910/2014, lai salīdzinātu citas dalībvalsts lietotājus ar attiecīgā lietotāja juridisko identitāti. Tomēr, neraugoties uz *eIDAS* datu kopas lietošanu, daudzos gadījumos precīzas atbilstības nodrošināšanai ir vajadzīga papildu informācija par lietotāju un īpašas unikālas identifikācijas procedūras valsts līmenī. Lai vēl vairāk atbalstītu elektroniskās identifikācijas līdzekļu lietojamību, ar šo regulu būtu jāpieprasa dalībvalstīm veikt īpašus pasākumus, ar kuriem nodrošina pareizu identitātes atbilstību elektroniskās identifikācijas procesā. Tajā pašā nolūkā ar šo regulu būtu jāpaplašina obligātais datu minimālais kopums un jāpieprasa unikāla un noturīga elektroniskā identifikatora lietošana saskaņā ar Savienības tiesību aktiem gadījumos, kad pēc lietotāja pieprasījuma ir nepieciešams juridiski identificēt lietotāju unikālā un noturīgā veidā.
- (18) Saskaņā ar Direktīvu (ES) 2019/882²² 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

²² 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.).

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.

- (21) Šīs regulas pamatā vajadzētu būt Savienības aktiem, kas nodrošina sāncensīgus un godīgus tirgus digitālajā nozarē. Jo īpaši tās pamatā vajadzētu būt Regulai XXX/XXXX [Digitālo tirgu akts], 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 XXX/XXXX [Digitālo tirgu akts] 6. panta 1. 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 [Digitālo tirgu akta] 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, viedtālrunu drošajiem elementiem, un sadarboties ar tām, izmantojot Eiropas digitālās identitātes makus vai dalībvalstu paziņotos elektroniskās identifikācijas līdzekļus.
- (22) Lai racionalizētu uzticamības pakalpojumu sniedzējiem uzliktos kibernetikas 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 kibernetikas draudiem. 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 nozaušanās, tīkla kabeļa bojājumi vai incidenti, kas radušies saistībā ar personu identificēšanu. Kibernetikas 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 un nodrošināt, ka saņēmēju identifikācija tiek nodrošināta ar augstāku ticamības līmeni nekā sūtītāja identifikācija.
- (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 lietotāji, tos jāpieņem privātiem pakalpojumu sniedzējiem. Privātām atkarīgām personām, kuras sniedz pakalpojumus transporta, enerģētikas, banku un 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 tiešsaistes identifikācijai. 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 darbību 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 maksus, 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 18 mēnešos pēc to ieviešanas būtu jānovērtē šo noteikumu efektivitāte attiecībā uz Eiropas digitālās identitātes maku pieejamību lietotājiem un lietojamību un jāpārskata noteikumi, lai nodrošinātu to pieņemšanu, izmantojot deleģētos aktus, ņemot vērā minēto novērtējumu.

- (29) Eiropas digitālās identitātes makam tehniski būtu jādod iespēja selektīvi atklāt atribūtus atkarīgām personām. Šī funkcija ir kļuvusi par galveno struktūras elementu, tādējādi uzlabojot ērtību un personas datu aizsardzību, tostarp minimējot personas datu apstrādi.
- (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.
- (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 pieteikšanos kontā un darbību uzsākšanu maksājumu pakalpojumu jomā.
- (32) Tīmekļa vietņu autentifikācijas pakalpojumi sniedz lietotājiem pārlicību, ka par šo tīmekļa vietni atbild īsta un likumīga vienība. Minētie pakalpojumi palīdz veidot uzticēšanos un ticamību, veicot darbīmdarbību tiešsaistē, jo lietotāji uzticēsies autentificētai tīmekļa vietnei. Tīmekļa vietņu autentifikācijas pakalpojumu lietošana tīmekļa vietnēs ir brīvprātīga. 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 ir noteikti minimālie drošības un atbildības pienākumi. Šajā nolūkā tīmekļa pārlūkprogrammām būtu jānodrošina atbalsts un sadarbība ar kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem saskaņā ar Regulu (ES) Nr. 910/2014. Tām būtu jāatzīst un jāparāda kvalificēti tīmekļa vietņu autentifikācijas sertifikāti, lai nodrošinātu augstu ticamības līmeni, ļaujot tīmekļa vietņu īpašniekiem apliecināt savu identitāti kā tīmekļa vietnes īpašniekiem un ļaujot lietotājiem ar lielu noteiktību identificēt tīmekļa vietņu īpašniekus. Lai vēl vairāk 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 un uzticēšanos, ir svarīgi nodrošināt tiesisko regulējumu nolūkā atvieglot kvalificētu elektronisko arhivēšanas pakalpojumu pārrobežu atzīšanu. Minētais regulējums varētu arī pavērt jaunas tirgus iespējas Savienības uzticamības pakalpojumu sniedzējiem.
- (34) Kvalificētās elektroniskās virsrāmātās dati tiek reģistrēti tā, lai nodrošinātu datu ierakstu unikalitāti, autentiskumu un pareizu secību pret viltojumiem drošā veidā. Elektroniska virsrāmata apvieno datu laika zīmogošanas ietekmi ar pārliecību par datu sagatavotāju, kas līdzinās e-parakstīšanai, un tai ir papildu priekšrocība — tā dod iespēju īstenot decentralizētākas pārvaldības modeļus, kas ir piemēroti daudzu ieinteresēto personu sadarbībai. Piemēram, tā sniedz uzticamu revīzijas izsekojamību par preču izcelsmi pārrobežu tirdzniecībā, atbalsta intelektuālā īpašuma tiesību aizsardzību, nodrošina elastīgumu elektroenerģijas tirgos, nodrošina pamatu progresīviem paša kontrolētas identitātes risinājumiem un atbalsta efektīvākus un pārveidojošākus sabiedriskos pakalpojumus. Lai novērstu iekšējā tirgus sadrumstalotību, ir svarīgi noteikt Eiropas mēroga tiesisko regulējumu, kas ļauj atzīt uzticamības pakalpojumus pāri robežām, reģistrējot datus elektroniskajās virsrāmātās.
- (35) Kvalificētu uzticamības pakalpojumu sniedzēju sertifikācijai būtu jānodrošina juridiska noteiktība lietošanas gadījumos, kas balstās uz elektroniskām virsrāmātām. Neatkarīgi no lietošanas gadījumiem šā elektronisko virsrāmātu un kvalificētu elektronisko virsrāmātu uzticamības pakalpojuma sertifikācijai, kā arī kvalificēta elektronisko virsrāmātu uzticamības pakalpojuma sniedzēja sertifikācijai būtu jāatbilst Savienības tiesību aktiem vai valsts tiesību aktiem saskaņā ar Savienības tiesību aktiem. Lietošanas gadījumiem, kas saistīti ar personas datu apstrādi, jāatbilst Regulai (ES) 2016/679. Lietošanas gadījumiem, kas saistīti ar kryptoaktīviem, vajadzētu būt saderīgiem ar visiem piemērojamajiem finanšu noteikumiem, piemēram, Finanšu instrumentu tirgu direktīvu²³, Maksājumu pakalpojumu direktīvu²⁴ un Regulu par kryptoaktīvu tirgiem²⁵.
- (36) Lai nepieļautu sadrumstalotību un šķēršļus atšķirīgo standartu un tehnisko ierobežojumu dēļ un 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 jāsadarbības atbilstīgi Komisijas ieteikumā XXX/XXXX [Rīkkopa saskaņotai pieejai Eiropas digitālās identitātes regulējumam]²⁶ paredzētajam regulējumam nolūkā noteikt rīkkopu Eiropas digitālās identitātes regulējumam.

²³ Eiropas Parlamenta un Padomes Direktīva 2014/65/ES (2014. gada 15. maijs) par finanšu instrumentu tirgiem un ar kuru groza Direktīvu 2002/92/EK un Direktīvu 2011/61/ES, *OV L 173, 12.6.2014., 349.–496. lpp.*

²⁴ 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.*

²⁵ Priekšlikums Eiropas Parlamenta un Padomes regulai par kryptoaktīvu tirgiem un ar ko groza Direktīvu (ES) 2019/1937 – COM(2020)593 final.

²⁶ [Pievienot atsauci, tiklīdz tā ir pieņemta.]

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 sadarbības 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 apspriešanas un Eiropas digitālās identitātes regulējuma pieņemšanas procesa rezultātu un tas jāataino.

(37) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1525 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju²⁷.

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

IR PIENĒMUŠI 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:

- (a) tiek izklāstīti nosacījumi, saskaņā ar kuriem dalībvalstis nodrošina un atzīst fizisku un juridisku personu elektroniskās identifikācijas līdzekļus, kuri ietverti citas dalībvalsts paziņotā elektroniskās identifikācijas shēmā;
- (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, elektroniski reģistrētiem piegādes pakalpojumiem, sertifikācijas pakalpojumiem tīmekļa vietņu autentifikācijai, elektronisko arhivēšanu un atribūtu elektronisko apliecinājumu, attālinātu elektroniskā paraksta un zīmoga radīšanas ierīču pārvaldību un elektroniskajām virsrāmām;
- (d) tiek izklāstīti nosacījumi, saskaņā ar kuriem dalībvalstis izdod Eiropas digitālās identitātes makus.”;

(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

²⁷ 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.).

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 citām juridiskām vai procesuālām saistībām atbilstīgi nozarei specifiskām prasībām attiecībā uz formātu ar attiecīgajām juridiskajām sekām.”;

(3) regulas 3. pantu groza šādi:

(a) panta 2) punktu aizstāj ar šādu:

“2) “elektroniskās identifikācijas līdzekļi” ir materiāli un/vai nemateriāli elementi, tostarp Eiropas digitālās identitātes maki vai personas apliecības saskaņā ar Regulu (ES) 2019/1157, kas ietver personas identifikācijas datus un ko izmanto, lai autentificētos tiešsaistes vai bezsaistes pakalpojumam.”;

(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 juridiskas personas.”;

(c) panta 14) punktu aizstāj ar šādu:

“14) “elektroniskā paraksta sertifikāts” ir elektronisks apliecinājums vai apliecinājumu kopums, 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, elektronisko zīmogu vai elektronisko laika zīmogu, elektroniski reģistrētu piegādes pakalpojumu un ar minētajiem pakalpojumiem saistītu atribūtu elektronisko apliecinājumu un sertifikātu radīšanu, verifikāciju un validāciju;
- (b) tīmekļa vietņu autentifikācijas sertifikātu radīšanu, verifikāciju un validāciju;
- (c) ar minētajiem pakalpojumiem saistītu elektronisko parakstu, zīmogu vai sertifikātu saglabāšanu;
- (d) elektronisko dokumentu elektronisko arhivēšanu;
- (e) attālinātu elektroniskā paraksta un zīmoga radīšanas ierīču pārvaldību;
- (f) elektronisko datu reģistrēšanu elektroniskajā virsgrāmatā.”;

(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 paraksta radīšanas ierīce” ir kvalificēta elektroniskā paraksta radīšanas ierīce, kurā kvalificēts uzticamības pakalpojumu sniedzējs parakstītāja vārdā ģenerē, pārvalda vai dublē elektroniskā paraksta radīšanas datus;
- 23.b) “attālināta kvalificēta zīmoga radīšanas ierīce” ir kvalificēta elektroniskā zīmoga radīšanas ierīce, kurā kvalificēts uzticamības pakalpojumu sniedzējs zīmoga radītāja vārdā ģenerē, pārvalda vai dublē elektroniskā paraksta radīšanas datus;”;
- (g) panta 29) punktu aizstāj ar šādu:
- “29) “elektroniskā zīmoga sertifikāts” ir elektronisks apliecinājums vai apliecinājumu kopums, kas saista elektroniskā zīmoga validācijas datus ar juridisku personu un apliecina minētās personas nosaukumu;”;
- (h) panta 41) punktu aizstāj ar šādu:
- “41) “validācija” ir elektroniskā paraksta vai zīmoga vai personas identifikācijas datu, vai atribūtu elektroniskā apliecinājuma verifikācija un derīguma apstiprināšana;”;
- (i) pievieno šādu 42) līdz 55) punktu:
- “42) “Eiropas digitālās identitātes maks” ir produkts un pakalpojums, kas lietotājam ļauj glabāt identitātes datus, akreditācijas datus un atribūtus, kas saistīti ar lietotāja identitāti, pēc pieprasījuma sniegt tos atkarīgajām pusēm un izmantot tos autentifikācijai tiešsaistē un bezsaistē pakalpojumam saskaņā ar 6.a pantu, un radīt kvalificētus elektroniskos parakstus un zīmogus;
- 43) “atribūts” ir fiziskas vai juridiskas personas vai subjekta iezīme, parametrs vai kvalitāte elektroniskā formā;
- 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;
- 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 valsts tiesību aktos atzīts par autentisku;
- 47) “elektroniskā arhivēšana” ir pakalpojums, kas nodrošina elektronisko datu vai dokumentu saņemšanu, glabāšanu, dzēšanu un nosūtīšanu, lai visā saglabāšanas periodā garantētu to integritāti, izcelsmes precizitāti un juridiskās iezīmes;

- 48) “kvalificēts elektroniskās arhivēšanas pakalpojums” ir pakalpojums, kas atbilst 45.g pantā noteiktajām prasībām;
- 49) “ES digitālās identitātes maka uzticamības marķējums” ir vienkārša, atpazīstama un skaidra norāde, ka digitālās identitātes maks ir izdots saskaņā ar šo regulu;
- 50) “droša lietotāju autentifikācija” ir autentifikācija, kuras pamatā ir divu vai vairāku tādu neatkarīgu elementu izmantošana, kas kategorizēti kā lietotāja zināšanas, valdījums un neatņemamas īpašības, tādā veidā, ka ar vienu elementu saistīts pārkāpums neapdraud citu elementu uzticamību, un kura ir izstrādāta tā, lai aizsargātu autentifikācijas datu konfidencialitāti;
- 51) “lietotāja konts” ir mehānisms, kas lietotājam ļauj piekļūt publiskiem vai privātiem pakalpojumiem saskaņā ar pakalpojumu sniedzēja paredzētajiem noteikumiem;
- 52) “akreditācijas dati” ir pierādījums par personas spējām, pieredzi, tiesībām vai atļauju;
- 53) “elektroniskā virsgrāmata” ir viltojumdrošs elektronisks datu reģistrs, kas nodrošina tajā ietverto datu autentiskumu un integritāti, to datuma un laika precizitāti un to hronoloģisko secību;
- 54) “personas dati” ir jebkura informācija, kas definēta Regulas (ES) 2016/679 4. panta 1. punktā;
- 55) “unikāla identifikācija” ir process, kurā personas identifikācijas dati vai personas identifikācijas līdzekļi tiek saskaņoti vai sasaistīti ar esošu kontu, kas pieder tai pašai personai.”;

(4) regulas 5. pantu aizstāj ar šādu:

“5. pants

Pseidonīmi elektroniskā darījumā

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

(5) regulas II nodaļas virsrakstu aizstāj ar šādu:

“I IEDAĻA

ELEKTRONISKĀ IDENTIFIKĀCIJA”;

(6) regulas 6. pantu svīturo;

(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 12 mēnešu laikā pēc šīs regulas stāšanās spēkā izdod Eiropas digitālās identitātes maku.
2. Eiropas digitālās identitātes makus izdod:

- (a) dalībvalsts;
 - (b) atbilstīgi dalībvalsts pilnvarojumam;
 - (c) neatkarīgi, bet dalībvalsts tos atzīst.
3. Eiropas digitālās identitātes maks lietotājam ļauj:
- (a) drošā, lietotājam pārredzamā un izsekojamā veidā pieprasīt un iegūt, saglabāt, atlasīt, apvienot un koplietot personas identifikācijas juridiskos datus un atribūtu elektronisko apliecinājumu, kas nepieciešami, lai tiešsaistē un bezsaistē autentificētos publisko un privāto tiešsaistes pakalpojumu izmantošanai;
 - (b) parakstīties, izmantojot kvalificētus elektroniskos parakstus.
4. Digitālās identitātes maki jo īpaši:
- (a) nodrošina kopīgu saskarni:
 - (1) kvalificētiem un nekvalificētiem uzticamības pakalpojumu sniedzējiem, kas izdod kvalificētus un nekvalificētus atribūtu elektroniskos apliecinājumus vai citus kvalificētus un nekvalificētus sertifikātus, šādu apliecinājumu un sertifikātu izdošanai Eiropas Digitālās identitātes makam;
 - (2) atkarīgajām pusēm personas identifikācijas datu un atribūtu elektronisko apliecinājumu pieprasīšanai un validēšanai;
 - (3) personas identifikācijas datu, atribūtu elektronisko apliecinājumu vai citu datu, piemēram, akreditācijas datu, uzrādīšanai atkarīgajām pusēm lokālā režīmā, kurā makam nav nepieciešama piekļuve internetam;
 - (4) lietotājiem mijiedarbībai ar Eiropas digitālās identitātes maku un ES digitālās identitātes maka uzticamības marķējuma attēlošanai;
 - (b) nodrošina, ka uzticamības pakalpojumu sniedzēji, kas sniedz kvalificētus atribūtu apliecinājumus, nevar saņemt nekādu informāciju par šo atribūtu izmantošanu;
 - (c) atbilst prasībām, kas 8. pantā noteiktas augstam uzticamības līmenim, jo īpaši prasībām par identitātes pierādīšanu un verifikāciju un elektroniskās identifikācijas līdzekļu pārvaldību un autentifikāciju;
 - (d) nodrošina mehānismu, kas atkarīgajai pusei ļauj autentificēt lietotāju un saņemt atribūtu elektroniskos apliecinājumus;
 - (e) nodrošina, ka 12. panta 4. punkta d) apakšpunktā minētie personas identifikācijas dati unikāli un pastāvīgi apliecina fizisko vai juridisko personu, ar kuru tie saistīti.
5. Dalībvalstis nodrošina Eiropas digitālās identitātes maku validācijas mehānismus, ar kuriem:
- (a) nodrošina, ka var verificēt to autentiskumu un derīgumu;
 - (b) ļauj atkarīgajām pusēm verificēt atribūtu apliecinājumu derīgumu;

- (c) ļauj atkarīgajām pusēm un kvalificētiem uzticamības pakalpojumu sniedzējiem verificēt attiecināto personas identifikācijas datu autentiskumu un derīgumu.
6. Eiropas digitālās identitātes makus izdod saskaņā ar paziņotu augsta uzticamības līmeņa elektroniskās identifikācijas shēmu. Fiziskas personas Eiropas digitālās identitātes makus var izmantot bez maksas.
 7. Lietotājs pilnībā kontrolē Eiropas digitālās identitātes maku. 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 datus, kas attiecas uz Eiropas digitālās identitātes maku nodrošināšanu, glabā fiziski un loģiski nošķirti no citiem glabātajiem datiem. Ja Eiropas digitālās identitātes maku nodrošina privāti subjekti saskaņā ar 1. punkta b) un c) apakšpunktu, *mutatis mutandis* piemēro 45.f.panta 4. punkta noteikumus.
 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 dalībvalstīm, kas izdod Eiropas digitālās identitātes makus.
 10. Eiropas digitālās identitātes maku dara pieklūstamu personām ar invaliditāti saskaņā ar Direktīvas (ES) 2019/882 I pielikumā noteiktajām pieklūstamības prasībām.
 11. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija nosaka tehniskās un darbības specifikācijas un atsauces standartus 3., 4. un 5. punktā minētajām prasībām, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maka īstenošanu. Šo 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 plāno izmantot Eiropas digitālās identitātes makus, kas izdoti saskaņā ar šo regulu, tās par to paziņo dalībvalstij, kurā konkrētā atkarīgā puse veic uzņēmējdarbību, lai nodrošinātu atbilstību prasībām, kas Savienības tiesību aktos vai valsts tiesību aktos noteiktas konkrētu pakalpojumu sniegšanai. Paziņojot par nodomu izmantot Eiropas digitālās identitātes makus, tās informē arī par Eiropas digitālās identitātes maka paredzēto izmantojumu.
2. Dalībvalstis ievieš kopīgu mehānismu atkarīgo pušu autentifikācijai.
3. Atkarīgo pušu atbildībā ir veikt procedūru, ar ko autentificē personas identifikācijas datus un atribūtu elektronisko apliecinājumu, kuru izcelsme ir no Eiropas digitālās identitātes makiem.
4. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija nosaka tehniskās un darbības specifikācijas 1. un 2. punktā minētajām prasībām, šādā nolūkā

pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 10. punktā.

6.c pants

Eiropas digitālās identitātes maku sertifikācija

1. Eiropas digitālās identitātes makus, kuri ir sertificēti vai par kuriem ir izdots atbilstības apliecinājums saskaņā ar kiberdrošības shēmu, ievērojot Regulu (ES) 2019/881, un atsaucies uz kuriem ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, uzskata par atbilstīgiem 6.a panta 3., 4. un 5. punktā noteiktajām attiecīgajām kiberdrošības prasībām, ciktāl kiberdrošības sertifikāts vai atbilstības apliecinājums vai tā daļas attiecas uz minētajām prasībām.
2. Atbilstību 6.a panta 3., 4. un 5. punktā noteiktajām prasībām attiecībā uz personas datu apstrādes darbībām, ko veic Eiropas digitālās identitātes maku izdevējs, sertificē saskaņā ar Regulu (ES) 2016/679.
3. Eiropas digitālās identitātes maku atbilstību 6.a panta 3., 4. un 5. punktā noteiktajām prasībām sertificē akreditētas publiskas vai privātas struktūras, ko izraudzījušās dalībvalstis.
4. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem izveido 3. punktā minēto Eiropas digitālās identitātes maku sertifikācijas standartu sarakstu.
5. Dalībvalstis paziņo Komisijai 3. punktā minēto publisko vai privāto struktūru nosaukumus un adreses. Komisija minēto informāciju dara pieejamu dalībvalstīm.
6. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 47. pantu attiecībā uz tādu īpašu kritēriju izstrādi, kuri jāievēro 3. punktā minētajām izraudzītajām struktūrām.

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 3. punktā minētās struktūras. Tās arī bez nepamatotas kavēšanās informē Komisiju par sertifikācijas anulēšanu.
2. Pamatojoties uz saņemto informāciju, Komisija izveido, publicē un atjaunina sarakstu, kurā uzskaitīti sertificētie Eiropas digitālās identitātes maki.
3. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija nosaka 1. punkta vajadzībām piemērojamos formātus un procedūras, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 10. punktā.”;

(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 12 mēnešu laikā pēc šīs regulas stāšanās spēkā paziņo vismaz vienu elektroniskās identifikācijas shēmu, ietverot vismaz vienu identifikācijas līdzekli.”;

(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.”;

(11) regulā iekļauj šādu 10.a pantu:

“10.a pants

Eiropas digitālās identitātes maku drošības prasību pārkāpums

1. Ja attiecībā uz Eiropas digitālās identitātes makiem, kas izdoti saskaņā ar 6.a pantu, un 6.a panta 5. punkta a), b) un c) apakšpunktā minētajiem validācijas mehānismiem ir noticis pārkāpums vai tie daļēji kompromitēti tādā veidā, kas ietekmē to uzticamību vai citu Eiropas digitālās identitātes maku uzticamību, izdevēja dalībvalsts nekavējoties aptur Eiropas digitālās identitātes maku izdošanu un atsauc tā spēkā esību, un attiecīgi informē citas dalībvalstis un Komisiju.
2. Ja 1. punktā minētais pārkāpums vai kompromitējums ir novērsts, izdevēja dalībvalsts bez nepamatotas kavēšanās atjauno Eiropas digitālās identitātes maku izdošanu un izmantošanu un informē citas dalībvalstis un Komisiju.
3. Ja 1. punktā minētais pārkāpums vai kompromitējums nav novērsts trīs mēnešu laikā pēc apturēšanas vai atsaukšanas, attiecīgā dalībvalsts anulē attiecīgo Eiropas digitālās identitātes maku un attiecīgi informē citas dalībvalstis un Komisiju par anulēšanu. Ja to attaisno pārkāpuma smagums, attiecīgo Eiropas digitālās identitātes maku anulē nekavējoties.
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. un 3. punktā minētos pasākumus, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 10. punktā.”;

(12) regulā iekļauj šādu 11.a pantu:

“11.a pants

Unikāla identifikācija

1. Ja autentifikācijai izmanto paziņotos elektroniskās identifikācijas līdzekļus un Eiropas digitālās identitātes makus, dalībvalstis nodrošina unikālu identifikāciju.
2. Dalībvalstis šīs regulas vajadzībām 12. panta 4. punkta d) apakšpunktā minētajā personas identifikācijas datu minimālajā kopumā iekļauj unikālu un pastāvīgu identifikatoru atbilstīgi Savienības tiesību aktiem, lai pēc lietotāja pieprasījuma identificētu lietotāju gadījumos, kad lietotāja identifikācija ir prasīta tiesību aktos.

3. Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija papildus precizē 1. un 2. punktā minētos pasākumus, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 10. punktā.”;
- (13) regulas 12. pantu groza šādi:
- (a) panta 3. punkta c) un d) apakšpunktu svītrot;
- (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.”;
- (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 sadarbību, unikālu identifikāciju un uzticamības līmeņiem.”;
- (14) regulā iekļauj šādu 12.a pantu:

“12.a pants

Elektroniskās identifikācijas shēmu sertifikācija

1. Paziņoto elektroniskās identifikācijas shēmu atbilstību 6.a pantā, 8. un 10. pantā noteiktajām prasībām var sertificēt publiskas vai privātas struktūras, ko izraudzījušās dalībvalstis.
 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. Dalībvalstis var izmantot sertifikātu vai Savienības atbilstības apliecinājumu, kas izdots saskaņā ar attiecīgo Eiropas kiberdrošības sertifikācijas shēmu, kura izveidota, ievērojot Regulu (ES) 2019/881, lai pierādītu šādu shēmu atbilstību 8. panta 2. punktā noteiktajām prasībām attiecībā uz elektroniskās identifikācijas shēmu uzticamības līmeņiem.
 3. Dalībvalstis paziņo Komisijai 1. punktā minēto publisko vai privāto struktūru nosaukumus un adreses. Komisija minēto informāciju dara pieejamu dalībvalstīm.”;
- (15) aiz 12 a. panta iekļauj šādu virsrakstu:

“III IEDAĻA

ELEKTRONISKĀS IDENTIFIKĀCIJAS LĪDZEKĻU IZMANTOŠANA PĀRROBEŽU MĒROGĀ”;

- (16) regulā iekļauj šādu 12.b un 12.c pantu:

“12.b pants

Eiropas digitālās identitātes maku izmantošana pārrobežu mērogā

1. Ja dalībvalstis saskaņā ar valsts tiesību aktiem vai administratīvo praksi prasa elektronisko identifikāciju, izmantojot elektroniskās identifikācijas līdzekļus un autentifikāciju, lai piekļūtu publiskas iestādes sniegtam tiešsaistes

pakalpojumam, tās arī akceptē Eiropas digitālās identitātes makus, kas izdoti saskaņā ar šo regulu.

2. Ja privātām atkarīgajām pusēm, kas sniedz pakalpojumus, saskaņā ar valsts vai Savienības tiesību aktiem tiešsaistes identifikācijai jāizmanto droša lietotāju autentifikācija 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 arī akceptē saskaņā ar 6.a pantu izdoto Eiropas digitālās identitātes maku izmantošanu.
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 6.a pantu izdoto Eiropas digitālās identitātes maku izmantošanu tikai pēc lietotāja brīvprātīga pieprasījuma un attiecībā uz obligātajiem atribūtiem, kas nepieciešami konkrētajam tiešsaistes pakalpojumam, kuram prasīta autentifikācija, piemēram, pierādījums par vecumu.
4. Lai veicinātu Eiropas digitālās identitātes maku plašu pieejamību un izmantojamību šīs regulas darbības jomā, Komisija rosina un sekmē pašregulējošu rīcības kodeksu ("rīcības kodeksi") izstrādi Savienības līmenī. Šie rīcības kodeksi nodrošina, 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 18 mēnešu laikā pēc Eiropas digitālās identitātes maku ieviešanas novērtē, vai, pamatojoties uz pierādījumiem, kas liecina par Eiropas digitālās identitātes maku pieejamību un izmantojamību, jāuzdod vēl citiem privātiem tiešsaistes pakalpojumu sniedzējiem pēc lietotāja brīvprātīga pieprasījuma akceptēt Eiropas digitālās identitātes maku izmantošanu. Novērtēšanas kritēriji var būt: lietotāju bāzes apjoms, pakalpojumu sniedzēja klātbūtne pārrobežu mērogā, tehnoloģiju attīstība, izmantošanas modeļu attīstība. Komisija ir pilnvarota, pamatojoties uz šo novērtējumu, pieņemt deleģētos aktus attiecībā uz šā panta 1.–4. punktā noteikto Eiropas digitālās identitātes maku atzīšanas prasību pārskatīšanu.
6. Šā panta vajadzībām uz Eiropas digitālās identitātes makiem neattiecas 7. un 9. pantā minētās prasības.

12.c pants

Citu elektroniskās identifikācijas līdzekļu savstarpēja atzīšana

1. Ja kādā dalībvalstī saskaņā ar valsts tiesību aktiem vai administratīvo praksi ir vajadzīga elektroniskā identifikācija, izmantojot elektroniskās identifikācijas līdzekļus un autentifikāciju, lai piekļūtu publiskas iestādes sniegtam tiešsaistes pakalpojumam, tad citā dalībvalstī izdoti elektroniskās identifikācijas līdzekļi pirmajā dalībvalstī tiek atzīti, lai veiktu pārrobežu autentifikāciju piekļuvei

minētajam tiešsaistes pakalpojumam, ar noteikumu, ka ir izpildīti šādi nosacījumi:

- (a) elektroniskās identifikācijas līdzekļi ir izdoti saskaņā ar elektroniskās identifikācijas shēmu, kas iekļauta 9. pantā minētajā sarakstā;
- (b) elektroniskās identifikācijas līdzekļu uzticamības līmenis atbilst tādām uzticamības līmenim, kas ir līdzvērtīgs vai augstāks par uzticamības līmeni, kādu attiecīgā publiskā iestāde noteikusi piekļuvei minētajam tiešsaistes pakalpojumam attiecīgajā dalībvalstī, un jebkurā gadījumā nav zemāks par būtisku uzticamības līmeni;
- (c) attiecīgā publiskā iestāde attiecīgajā dalībvalstī izmanto būtisku vai augstu uzticamības līmeni saistībā ar piekļuvei minētajam tiešsaistes pakalpojumam.

Šāda atzīšana notiek vēlākais 6 mēnešus pēc tam, kad Komisija publicējusi pirmās daļas a) apakšpunktā minēto sarakstu.

- 2. Elektroniskās identifikācijas līdzekļus, kas izdoti 9. pantā minētajā sarakstā iekļautas elektroniskās identifikācijas shēmas tvērumā un kas atbilst zēmam uzticamības līmenim, publiskās iestādes var atzīt, lai veiktu pārrobežu autentifikāciju piekļuvei minēto iestāžu sniegtam tiešsaistes pakalpojumam.”;

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

- “1. Neskarot šā panta 2. punktu, uzticamības pakalpojumu sniedzēji ir atbildīgi par zaudējumu, kas tīši vai nolaidības dēļ radīts kādai fiziskai vai juridiskai personai tādēļ, ka nav izpildīti šajā regulā noteiktie pienākumi un kibēdrošības riska pārvaldības pienākumi, kas noteikti Direktīvas XXXX/XXXX [TID2] 18. pantā.”;

(18) regulas 14. pantu aizstāj ar šādu:

“14. pants

Starptautiskie aspekti

- 1. Komisija saskaņā ar 48. panta 2. punktu var pieņemt īstenošanas aktus, kuros paredz nosacījumus, saskaņā ar kuriem trešās valsts prasības, kas piemērojamas uzticamības pakalpojumu sniedzējiem, kuri veic uzņēmējdarbību tās teritorijā, un to sniegtajiem uzticamības pakalpojumiem, var uzskatīt par līdzvērtīgām prasībām, kas piemērojamas kvalificētiem uzticamības pakalpojumu sniedzējiem, kuri veic uzņēmējdarbību Savienībā, un to sniegtajiem kvalificētajiem uzticamības pakalpojumiem.
- 2. Ja Komisija ir pieņēmusi īstenošanas aktu saskaņā ar 1. punktu vai noslēgusi starptautisku nolīgumu par uzticamības pakalpojumu savstarpēju atzīšanu saskaņā ar Līguma 218. pantu, uzticamības pakalpojumus, ko sniedz pakalpojumu sniedzēji, kuri veic uzņēmējdarbību attiecīgajā trešā valstī, uzskata par līdzvērtīgiem kvalificētiem uzticamības pakalpojumiem, ko sniedz kvalificēti uzticamības pakalpojumu sniedzēji, kuri veic uzņēmējdarbību Savienībā.”;

(19) regulas 15. pantu aizstāj ar šādu:

“15. pants

Piekļūstamība personām ar invaliditāti

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

(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 visiem būtiskiem drošības pārkāpumiem vai integritātes zudumu, par ko tā uzzinājusi, pildot savus uzdevumus. 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);”;

(2) punkta f) apakšpunktu aizstāj ar šādu:

“f) sadarbību ar uzraudzības iestādēm, kas izveidotas saskaņā ar Regulu (ES) 2016/679, jo īpaši bez nepamatotas kavēšanās tās informējot par kvalificēto uzticamības pakalpojumu sniedzēju revīziju rezultātiem, ja ir notikuši personas datu aizsardzības noteikumu pārkāpumi, un par drošības pārkāpumiem, kas ir 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. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem sīkāk precizē 4. punktā minētos uzraudzības iestāžu uzdevumus un nosaka 6. punktā minētā pārskata formātu un procedūras. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.”;

(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 iestāde pieprasa valsts kompetentajai iestādei 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.”;

(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.”;

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

“Ja personas datu aizsardzības noteikumi, iespējams, ir pārkāpti, uzraudzības iestāde par revīzijas rezultātiem informē Regulā (ES) 2016/679 noteiktās uzraudzības iestādes.”;

(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 attiecīgā sniegtā pakalpojuma kvalifikācijas statusu un pieprasīt, lai tas – attiecīgā gadījumā noteiktā termiņā – izpildītu Direktīvas XXXX/XXXX [TID2] prasības. Uzraudzības iestāde informē 22. panta 3. punktā minēto struktūru, lai atjauninātu 22. panta 1. punktā minētos uzticamības sarakstus.

Uzraudzības iestāde informē kvalificēto uzticamības pakalpojumu sniedzēju par tā kvalifikācijas statusa vai attiecīgā pakalpojuma kvalifikācijas statusa anulēšanu.

4. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka identifikācijas numuru šādiem standartiem:

- (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 atbilstības novērtēšanas ziņojuma sniegšanai.

Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.”;

(23) regulas 21. pantu groza šādi:

(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 trīs dienu laikā pēc to pabeigšanas sniedz informāciju par rezultātiem.

Ja uzraudzības iestāde secina, ka uzticamības pakalpojumu sniedzējs un tā sniegtie uzticamības pakalpojumi atbilst pirmajā daļā minētajām 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 šā panta 1. un 2. punkta vajadzībām. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.”;

(24) regulas 23. pantā iekļauj šādu 2.a punktu:

“2.a Šā panta 1. un 2. punkts attiecas arī uz uzticamības pakalpojumu sniedzējiem, kuri veic uzņēmējdarbību trešās valstīs, un uz to sniegtajiem pakalpojumiem, ar nosacījumu, ka tie ir atzīti Savienībā saskaņā ar 14. pantu.”;

(25) regulas 24. pantu groza šādi:

(a) panta 1. punktu aizstāj ar šādu:

“1. Izdodot kvalificētu sertifikātu vai kvalificētu atribūtu elektronisko apliecinājumu uzticamības pakalpojumam, kvalificēts uzticamības pakalpojumu sniedzējs verificē tās fiziskās vai juridiskās personas identitāti, kurai tiek 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 pazīņotus elektroniskās identifikācijas līdzekļus, kas atbilst 8. pantā noteiktajām prasībām attiecībā uz būtisku vai 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 fiziskās 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, ja citi līdzekļi nav pieejami.”;

(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:

(1) punkta d) apakšpunktu aizstāj ar šādu:

“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.”;

(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 un attiecīgā gadījumā citām attiecīgajām struktūrām par visiem pārkāpumiem vai traucējumiem, kuri saistīti ar fā) apakšpunkta i), ii) un iii) punktā minēto pasākumu īstenošanu un kuri būtiski ietekmē sniegto uzticamības pakalpojumu vai tajā glabātos personas datus.”;
- (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 elektronisko apliecinājumu atsaukšanai.”;
- (e) panta 5. punktu aizstāj ar šādu:

“5. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka identifikācijas numurus standartiem, kas attiecas uz 2. punktā minētajām prasībām. Uzskata, ka atbilstība šajā pantā noteiktajām prasībām ir panākta tad, ja uzticamas sistēmas un produkti atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.”;
- (f) pantam pievieno šādu 6. punktu:

“6. Komisija tiek pilnvarota pieņemt deleģētos aktus attiecībā uz 2. punkta fā) apakšpunktā minētajiem papildu pasākumiem.”;
- (26) regulas 28. panta 6. punktu aizstāj ar šādu:

“6. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka kvalificētu elektroniskā paraksta sertifikātu standartu identifikācijas numurus. Uzskata, ka atbilstība I pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā paraksta sertifikāts atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.”;

- (27) regulas 29. pantam pievieno šādu 1.a punktu:
- “1.a Elektroniskā paraksta radīšanas datu ģenerēšanu, pārvaldību un dublēšanu parakstītāja vārdā 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 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 dublē tikai rezerves kopijas vajadzībām ar nosacījumu, ka ir izpildītas šādas prasības:
dublēto datu kopu drošības līmenim jābūt tādām pašām, kāds tas ir oriģinālajām datu kopām;
dublēto datu kopu skaits nedrīkst pārsniegt minimālo skaitu, kāds nepieciešams pakalpojuma nepārtrauktības nodrošināšanai;
 - (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 minētā sertifikācija ir derīga 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 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 minētajiem standartiem.”
 - (b) panta 3. punktu aizstāj ar šādu:

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

(32) regulas 34. pantu 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 minētajiem standartiem.
3. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojuma standartu identifikācijas numurus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.”;

(33) regulas 37. pantu groza šādi:

(a) pantā iekļauj šādu 2.a punktu:

“2.a Uzskata, ka uzlabots elektroniskais zīmogs atbilst 36. pantā un šā panta 5. punktā minētajām prasībām, ja uzlabots elektroniskais zīmogs atbilst 4. punktā minētajiem standartiem.”;

(b) panta 4. punktu aizstāj ar šādu:

“4. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka uzlabotu elektronisko zīmogu standartu identifikācijas numurus. Minētos īstenošanas aktus pieņem saskaņā ar 48. panta 2. punktā minēto pārbaudes procedūru.”;

(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 minētajiem standartiem.”;

(b) panta 6. punktu aizstāj ar šādu:

“6. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka kvalificētu elektroniskā zīmoga sertifikātu 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 elektroniskā zīmoga radīšanas ierīču pārvaldībai

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

(36) regulas 42. pantu groza šādi:

(a) pantā iekļauj šādu jaunu 1.a punktu:

“1.a Uzsaka, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja datuma un laika sasaiste ar datiem un precīzais laika avots atbilst 2. punktā minētajiem standartiem.”;

(b) panta 2. punktu aizstāj ar šādu:

“2. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka 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.”;

(37) regulas 44. pantu groza šādi:

(a) pantā iekļauj šādu 1.a punktu:

“1.a Uzsaka, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja datu nosūtīšanas un saņemšanas process atbilst 2. punktā minētajiem 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 standartu identifikācijas numurus. Minētos īstenošanas aktus 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. Kvalificētus tīmekļa vietņu autentifikācijas sertifikātus uzskata par atbilstīgiem IV pielikumā noteiktajām prasībām, ja tie atbilst 3. punktā minētajiem 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 sadarbību 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.
3. Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka specifikācijas un identifikācijas numurus

standartiem, kas attiecas uz 1. 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.
2. Kvalificētam atribūtu elektroniskajam apliecinājumam 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.

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 vai publiskā iestāde to nav īpaši atļāvusi. Šādā gadījumā akceptē arī kvalificētus atribūtu elektroniskos apliecinājumus no citām dalībvalstīm.

45.c pants

Prasības kvalificētam atribūtu apliecinājumam

1. Kvalificēts atribūtu elektroniskais apliecinājums atbilst V pielikumā noteiktajām prasībām. Kvalificētu atribūtu elektronisko apliecinājumu uzskata par atbilstīgu V pielikumā noteiktajām prasībām, ja tas atbilst 4. punktā minētajiem 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 standartu identifikācijas numurus, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 10. punktā.

45.d pants

Atribūtu verifikācija attiecībā pret autentiskiem avotiem

1. Dalībvalstis 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 ar elektroniskiem līdzekļiem verificēt atribūta autentiskumu tieši attiecībā pret attiecīgo autentisko avotu valsts līmenī vai ar tādu izraudzītu starpnieku palīdzību, kas valsts līmenī atzīti saskaņā ar valsts vai Savienības tiesību aktiem.
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 verificācijas procedūrām, šādā nolūkā pieņemot īstenošanas aktu par Eiropas digitālās identitātes maku īstenošanu, kā minēts 6.a panta 10. punktā.

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 piedāvātiem pakalpojumiem.
2. Personas datus, kas attiecas uz atribūtu elektroniskā apliecinājuma pakalpojumu sniegšanu, glabā loģiski nošķirti no citiem glabātajiem datiem.
3. Personas datus, kas attiecas uz kvalificēta atribūtu elektroniskā apliecinājuma pakalpojumu sniegšanu, glabā fiziski un loģiski nošķirti no citiem glabātajiem datiem.
4. Kvalificēta atribūtu elektroniskā apliecinājuma pakalpojumu sniedzēji šādus pakalpojumus sniedz kā atsevišķa juridiskā persona.

10. IEDAĻA

KVALIFICĒTI ELEKTRONISKĀS ARHIVĒŠANAS PAKALPOJUMI

45.g pants

Kvalificēti elektroniskās arhivēšanas pakalpojumi

Elektronisko dokumentu kvalificētu elektroniskās arhivēšanas pakalpojumu var sniegt tikai kvalificēts uzticamības pakalpojumu sniedzējs, kas izmanto tādas procedūras un tehnoloģijas, ar kurām var nodrošināt elektroniskā dokumenta uzticamību ilgāk par tehnoloģiskā derīguma termiņu.

Divpadsmit mēnešu laikā pēc šīs regulas stāšanās spēkā Komisija ar īstenošanas aktiem nosaka elektroniskās arhivēšanas pakalpojumu standartu identifikācijas numurus. 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 kvalificētu elektronisko virsgrāmatu attiecas prezumpcija par tajā ietverto datu unikalitāti un autentiskumu, to datuma un laika precizitāti un to hronoloģisko secību virsgrāmatā.

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 nodrošina virsgrāmatā reģistrēto datu ierakstu unikalitāti, autentiskumu un pareizu secību;
 - (c) tās nodrošina datu pareizu hronoloģisko secību virsgrāmatā un datu ieraksta datuma un laika precizitāti;
 - (d) tajā datus reģistrē tā, lai visas turpmākās datu izmaiņas būtu uzreiz nosakāmas.
2. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja elektroniskā virsgrāmata atbilst 3. punktā minētajiem standartiem.
3. Komisija ar īstenošanas aktiem var noteikt identifikācijas numurus standartiem, kas attiecas uz procesiem datu kopuma izpildei un reģistrēšanai kvalificētā elektroniskajā virsgrāmatā un tās radīšanai. 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 un kvalificēto uzticamības pakalpojumu darbību.
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 digitālā maka izmantošana;
 - (c) infrastruktūras incidenti un dīkstāve valsts līmenī, kas neļauj izmantot digitālās identitātes maka lietotni.
3. Šā panta 2. punktā minētos statistikas datus dara publiski pieejamus atvērtā un plaši izmantotā mašīnlasāmā formātā.

4. Katru gadu līdz 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 24 mēnešu laikā pēc tās stāšanās spēkā. Komisija jo īpaši izvērtē, vai ir lietderīgi grozīt šīs regulas darbības jomu vai konkrētus tās noteikumus, ņemot vērā šīs regulas piemērošanā gūto pieredzi, kā arī tehnoloģiskos sasniegumus un attīstību tirgus un tiesiskajā jomā. Vajadzības gadījumā minētajam ziņojumam pievieno šīs regulas grozījumu priekšlikumu.
2. Izvērtējuma ziņojumā iekļauj novērtējumu par šīs regulas darbības jomas aptverto identifikācijas līdzekļu, tostarp 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 paziņoto elektroniskās identifikācijas līdzekļu un Eiropas digitālās identitātes maka 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 [datums – OV: lūgums ievietot četru gadu laikposmu 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 [datums – PB: lūgums ievietot četru gadu laikposmu pēc šīs regulas stāšanās spēkā] turpina uzskatīt par kvalificētiem elektroniskā paraksta sertifikātiem saskaņā ar šo regulu.”;

(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.

2. 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 –
priekšsēdētājs*

*Padomes vārdā –
priekšsēdētājs*

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Eiropas Parlamenta un Padomes Regula par Eiropas digitālās identitāte regulējumu, ar ko groza *eIDAS* regulu

1.2. Attiecīgā rīcībpolitikas joma

Rīcībpolitikas joma: iekšējais tirgus
digitālajam laikmetam gatava Eiropa

1.3. Priekšlikums/iniciatīva attiecas uz:

☐ jaunu darbību

☐ jaunu darbību, pamatojoties uz izmēģinājuma projektu/sagatavošanas darbību²⁸

☒ spēkā esošas darbības turpināšanu

☐ vienas vai vairāku darbību apvienošanu vai pārorientēšanu uz citu/jaunu darbību

1.4. Mērķi

1.4.1. Vispārīgie mērķi

Šīs iniciatīvas vispārīgais mērķis ir nodrošināt pareizu iekšējā tirgus darbību, jo īpaši attiecībā uz sabiedrisko un privāto pakalpojumu pārrobežu un starpnozaru sniegšanu un lietošanu, pamatojoties uz ļoti drošu un uzticamu elektroniskās identitātes risinājumu pieejamību un lietošanu. Šis mērķis ir daļa no stratēģiskajiem mērķiem, kas noteikti paziņojumā "Eiropas digitālās nākotnes veidošana".

1.4.2. Konkrētie mērķi

Konkrētais mērķis Nr. 1:

nodrošināt piekļuvi uzticamiem un drošiem digitālās identitātes risinājumiem, kurus var izmantot pāri robežām, apmierinot lietotāju gaidas un tirgus pieprasījumu.

Konkrētais mērķis Nr. 2:

nodrošināt to, ka, sniedzot sabiedriskus un privātus pakalpojumus, var paļauties uz uzticamiem un drošiem digitālās identitātes risinājumiem pāri robežām.

Konkrētais mērķis Nr. 3:

nodrošināt pilsoņiem pilnīgu kontroli pār saviem personas datiem un garantēt to drošību, izmantojot digitālās identitātes risinājumus.

Konkrētais mērķis Nr. 4:

nodrošināt vienlīdzīgus nosacījumus kvalificētu uzticamības pakalpojumu sniegšanai ES un to pieņemšanai.

²⁸

Kā paredzēts Finanšu regulas 58. panta 2. punkta a) vai b) apakšpunktā.

1.4.3. Paredzamie rezultāti un ietekme

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz labuma guvējiem/mērķgrupām.

Kopumā paredzams, ka lielāko labumu no iniciatīvas gūs galalietotāji/pilsoņi, tiešsaistes pakalpojumu sniedzēji, maka lietotņu nodrošinātāji un publiskie un privātie digitālās identitātes pakalpojumu sniedzēji. Paredzams, ka šī iniciatīva nodrošinās piekļuvi uzticamiem un drošiem digitālās identitātes risinājumiem, kurus var izmantot pāri robežām, apmierinot lietotāju gaidas un tirgus pieprasījumus; nodrošinās, ka, sniedzot sabiedriskos un privātos pakalpojumus, varēs paļauties uz uzticamiem un drošiem pārrobežu digitālās identitātes risinājumiem; nodrošinās pilsoņiem pilnīgu kontroli pār saviem personas datiem un garantēs viņu drošību, izmantojot digitālās identitātes risinājumus; nodrošinās vienlīdzīgus nosacījumus kvalificētu uzticamības pakalpojumu sniegšanai ES un to pieņemšanai.

Papildus iespējai piekļūt gan sabiedriskiem, gan privātiem pakalpojumiem pilsoņi un uzņēmumi gūs tiešu labumu no ērtas un lietotājdraudzīgas maka autentifikācijas saskarnes un varēs iesaistīties darījumos, kuriem nepieciešama visu līmeņu uzticamība (piemēram, no pieteikšanās sociālajos medijos līdz e-veselības lietojumprogrammām).

Pastiprināta integrēta privātuma pieeja varētu dot papildu priekšrocības, jo makam nebūtu vajadzīgi starpnieki atribūtu apliecināšanas procesā, tādējādi dodot iespēju pilsoņiem tieši sazināties ar pakalpojumu un akreditācijas datu sniedzējiem. Paaugstināta maka datu drošība novērstu identitātes zādzības, tādējādi novēršot finansiālus zaudējumus Eiropas pilsoņiem un uzņēmumiem.

Attiecībā uz ekonomikas izaugsmi paredzams, ka standartu sistēmas ieviešana mazinās nenoteiktību tirgus dalībnieku vidū, un paredzams, ka tas pozitīvi ietekmēs arī inovāciju.

Svarīgi, ka ir paredzams, ka tas nodrošinās iekļaujošāku piekļuvi sabiedriskajiem un privātajiem pakalpojumiem, kas saistīti ar tādiem sabiedriskiem labumiem kā izglītība un veselības aprūpe, kuri pašlaik ir grūti pieejami dažām sociālajām grupām. Piemēram, dažiem pilsoņiem ar invaliditāti, bieži vien cilvēkiem ar ierobežotām pārvietošanās spējām vai lauku rajonos dzīvojošiem, var būt sliktāka piekļuve pakalpojumiem, kuriem parasti nepieciešama fiziska klātbūtne, ja tie netiek sniegti uz vietas.

1.4.4. Veiktspējas rādītāji

Norādīt, pēc kādiem rādītājiem seko līdzī progresam un sasniegumiem.

Uzraudzības un izvērtēšanas aspekts un attiecīgie mērķi	Rādītājs	Atbildība par vākšanu	Avots(-i)
Lietojums			

Nodrošināt piekļuvi <i>eID</i> līdzekļiem visiem ES pilsoņiem	To Eiropas pilsoņu un uzņēmumu skaits, kuriem izsniegtas paziņotas <i>eID</i> / Eiropas digitālās identitātes māki, un izsniegto identitātes akreditācijas datu (atribūtu apliecinājumu) skaits	Eiropas Komisija un valstu kompetentās iestādes (VKI)	Ilgadējais apsekojums / VKI apkopotie uzraudzības un izvērtēšanas dati
Nodrošināt piekļuvi <i>eID</i> līdzekļiem visiem ES pilsoņiem	To Eiropas pilsoņu un uzņēmumu skaits, kuri aktīvi izmanto paziņotas <i>eID</i> / Eiropas digitālās identitātes mākus un identitātes akreditācijas datus (atribūtu apliecinājumus)	Eiropas Komisija un valstu kompetentās iestādes (VKI)	Ilgadējais apsekojums / VKI apkopotie uzraudzības un izvērtēšanas dati
Palielināt <i>eID</i> shēmu pārrobežu atpazīstamību un pieņemšanu, cenšoties panākt vispārēju pieņemšanu	To tiešsaistes pakalpojumu sniedzēju skaits, kuri pieņem paziņotas <i>eID</i> / Eiropas digitālās identitātes mākus un identitātes akreditācijas datus (atribūtu apliecinājumus)	Eiropas Komisija	Ilgadējs apsekojums
Palielināt <i>eID</i> shēmu pārrobežu atpazīstamību un pieņemšanu, cenšoties panākt vispārēju pieņemšanu	Tiešsaistes darījumu skaits, ko veic ar paziņotām <i>eID</i> / Eiropas digitālās identitātes mākiem un identitātes akreditācijas datiem (kopā un pārrobežu)	Eiropas Komisija	Ilgadējs apsekojums
Stimulēt pieņemšanu privātajā sektorā un jaunu digitālās identitātes pakalpojumu attīstību	Jaunu privāti izsniegtu atribūtu apliecināšanas pakalpojumu skaits, kas atbilst standartiem integrācijai Eiropas digitālās identitātes makā	Eiropas Komisija un valstu kompetentās iestādes (VKI)	Ilgadējs apsekojums
Kontekstuāla informācija			
Stimulēt pieņemšanu privātajā sektorā un jaunu digitālās identitātes pakalpojumu attīstību	Digitālās identitātes tirgus apmērs	Eiropas Komisija	Ilgadējs apsekojums
Stimulēt pieņemšanu privātajā sektorā un jaunu digitālās identitātes pakalpojumu attīstību	Ar digitālo identitāti saistīta publiskā iepirkuma izmaksas	Eiropas Komisija un valstu kompetentās iestādes	Ilgadējs apsekojums

Palielināt <i>eID</i> shēmu pārrobežu atpazīstamību un pieņemšanu, cenšoties panākt vispārēju pieņemšanu	% uzņēmumu, kuri nodarbojas ar preču vai pakalpojumu e-tirdzniecību	Eiropas Komisija	<i>Eurostat</i>
Palielināt <i>eID</i> shēmu pārrobežu atpazīstamību un pieņemšanu, cenšoties panākt vispārēju pieņemšanu	Tādu tiešsaistes darījumu īpatsvars, kuros ir vajadzīga stingra klienta identifikācija (kopā)	Eiropas Komisija	Ilgadējs apsekojums
Nodrošināt piekļuvi <i>eID</i> līdzekļiem visiem ES pilsoņiem	% privātpersonu, kuras nodarbojas ar e-komerciju % privātpersonu, kuriem ir piekļuve tiešsaistes sabiedriskajiem pakalpojumiem	Eiropas Komisija	<i>Eurostat</i>

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, ieskaitot sīku iniciatīvas izvēršanas grafiku

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs. Dalībvalstīm 24–48 mēnešos (orientējoši) pēc šīs regulas pieņemšanas būs jāizdod Eiropas digitālās identitātes maks. Komisija tiks pilnvarota 12–24 mēnešos (orientējoši) pēc šīs regulas pieņemšanas pieņemt īstenošanas aktus, kuros būs noteiktas tehniskās specifikācijas un atsaucē standarti Eiropas digitālās identitātes regulējuma tehniskajai arhitektūrai.

1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē “Savienības iesaistīšanās pievienotā vērtība” ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.

Eiropas līmeņa rīcības pamatojums (*ex ante*)

Nemot vērā pilsoņu, uzņēmumu un tiešsaistes pakalpojumu sniedzēju pieaugošo pieprasījumu pēc digitālās identitātes risinājumiem, kas ir lietotājdraudzīgi, droši un ievēro privātumu un kurus var izmantot pāri robežām, turpmāka rīcība ES līmenī var būt vērtīgāka nekā atsevišķu dalībvalstu rīcība, kā noteikts *eIDAS* regulas izvērtējumā.

Sagaidāmā Savienības pievienotā vērtība (*ex post*)

Saskaņotāka pieeja ES līmenī, kuras pamatā ir būtiska pāreja no paļaušanās tikai uz digitālās identitātes risinājumiem uz atribūtu elektronisko apliecinājumu sniegšanu, nodrošinātu pilsoņiem un uzņēmumiem piekļuvi sabiedriskiem un privātiem pakalpojumiem jebkurā vietā ES, paļaujoties uz pārbaudītiem identitātes

pierādījumiem un atribūtiem. Tiešsaistes pakalpojumu sniedzēji varētu akceptēt digitālās identitātes risinājumus neatkarīgi no to izdošanas vietas, palaujoties uz kopēju Eiropas pieeju uzticamībai, drošībai un sadarbībai. Gan lietotāji, gan pakalpojumu sniedzēji var gūt labumu arī no vienādas juridiskās vērtības, kura visā ES piešķirta atribūtu elektroniskajiem apliecinājumiem, kas ir sevišķi svarīgi, ja ir vajadzīga koordinēta rīcība, piemēram, attiecībā uz digitālajiem veselības sertifikātiem. Uzticamības pakalpojumi, kas sniedz atribūtu elektroniskus apliecinājumus, gūtu labumu arī no tā, ka to pakalpojumiem būtu pieejams Eiropas tirgus. Piemēram, apjomradītu ietaupījumu dēļ ES līmenī ir vieglāk kompensēt izmaksas, lai nodrošinātu ļoti uzticamu un drošu vidi kvalificēta uzticamības pakalpojuma sniegšanai. Tikai ES regulējums var nodrošināt juridisko identitāšu pilnīgu pārrobežu pārnēsāšanu un ar to saistīto atribūtu elektronisku apliecināšanu, dodot iespēju uzticēties citu dalībvalstu izteiktajiem apgalvojumiem par identitāti.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

eIDAS Regula (Regula 910/2014) (*eIDAS*) ir vienīgais uzticamas fizisku un juridisku personu elektroniskās identifikācijas (*eID*) un uzticamības pakalpojumu pārrobežu regulējums. Lai gan *eIDAS* ir neapstrīdama loma iekšējā tirgū, kopš tās pieņemšanas daudz kas ir mainījies. *eIDAS*, kas pieņemta 2014. gadā, ir balstīta valstu *eID* sistēmās, ievērojot dažādus standartus, un pievēršot uzmanību salīdzinoši nelielam iedzīvotāju un uzņēmumu elektroniskās identifikācijas vajadzību segmentam: drošai pārrobežu piekļuvei sabiedriskajiem pakalpojumiem. Attiecīgie pakalpojumi lielākoties skar 3 % ES iedzīvotāju, kuri dzīvo dalībvalstī, kas nav valsts, kurā viņi ir dzimuši.

Kopš tā laika visu sabiedrības funkciju digitalizācija ir būtiski pieaugusi. Turklāt Covid-19 pandēmija ir ļoti spēcīgi ietekmējusi digitalizācijas ātrumu. Tādējādi gan sabiedrisko, gan privāto pakalpojumu sniegšana kļūst arvien digitālāka. Pilsoņi un uzņēmumi cer sasniegt augstu drošības un ērtības līmeni ikvienā tiešsaistes darbībā, piemēram, iesniedzot nodokļu deklarāciju, stājoties ārvalstu universitātē, attālināti atverot bankas kontu vai pieprasot aizdevumu, nomājot automašīnu, dibinot uzņēmumu citā dalībvalstī, autentificējoties, lai veiktu maksājumus internetā, piedaloties tiešsaistē izsludinātā konkursā un veicot daudzas citas darbības.

Tādējādi ir krasi pieaudzis pieprasījums pēc tiešsaistes identificēšanās un autentificēšanās līdzekļiem, kā arī ar mūsu identitāti, atribūtiem vai kvalifikāciju (identitāte, adreses, vecums, kā arī profesionālā kvalifikācija, autovadītāja apliecības un citas atļaujas un maksājumu sistēmas) saistītas informācijas digitālas apmaiņas līdzekļiem, kas būtu droši un sniegtu augstu datu aizsardzības līmeni.

Tas ir izraisījis paradigmas maiņu, virzoties uz progresīviem un ērtiem risinājumiem, kas spēj integrēt dažādus pārbaudāmus lietotāja datus un sertifikātus. Lietotāji sagaida, ka vide būs pašnoteikta un tajā varēs izmantot un koplietot dažādus akreditācijas datus un atribūtus, piemēram, jūsu valsts *eID*, profesionālos sertifikātus, sabiedriskā transporta biļetes vai dažos gadījumos pat digitālas koncertu biļetes. Tie ir tā sauktie pašapkalpošanās lietotņu maki, kas tiek pārvaldīti, izmantojot lietotāja mobilo ierīci, ļaujot droši un ērti piekļūt dažādiem sabiedriskiem un privātiem pakalpojumiem un pilnībā kontrolēt šādu piekļuvi.

1.5.4. *Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem*

Iniciatīva atbalsta Eiropas atveseļošanās centienus, nodrošinot pilsoņiem un uzņēmumiem nepieciešamos rīkus, piemēram, ērtu *eID* un uzticamības pakalpojumus, lai palīdzētu uzticami un droši veikt ikdienas darbības tiešsaistē. Tādējādi tas pilnībā atbilst DFS mērķiem.

Darbības izdevumi jāfinansē no *DEP SO5*. Tiek lēsts, ka iepirkuma līgumi, kas atbalsta standartu un tehnisko specifikāciju izstrādi, kā arī *eID* un uzticamības pakalpojumu pamatelementu uzturēšanas izmaksas veido līdz 3-4 miljoniem euro gadā. Par šī budžeta precīzu sadalījumu jālemj, izstrādājot turpmākās darba programmas. Dotācijas, kas atbalsta sabiedrisko un privāto pakalpojumu piesaisti *eID* ekosistēmai, lielā mērā atbalstītu priekšlikuma mērķu sasniegšanu. Tiek lēsts, ka pakalpojuma sniedzēja izmaksas, kas vajadzīgas, lai integrētu nepieciešamo *eID* maka *API*, ir aptuveni 25 000 EUR kā vienreizējas izmaksas vienam pakalpojumu sniedzējam. Ja būtu pieejams, tiklīdz būs apspriests budžeta sadalījums nākamajā darba programmā, budžets dotācijām līdz 0,5 miljoniem euro vienai dalībvalstij atbalstītu kritiskās pakalpojumu masas piesaisti.

Ar īstenošanas aktu izstrādi saistīto ekspertu grupas sanāksmju izmaksas tiks segtas no *DEP* administratīvās daļas pavisam līdz 0,5 miljoniem euro.

Sinerģija ar citiem instrumentiem

Šī iniciatīva nodrošinās elektroniskās identitātes un elektroniskās identitātes pakalpojumu sniegšanas regulējumu ES, uz kuru konkrētas nozares var paļauties, lai izpildītu nozares īpašās juridiskās prasības, piemēram, saistībā ar digitāliem ceļošanas dokumentiem, digitālām autovadītāju apliecībām utt. Priekšlikums ir saskaņots arī ar Regulas 2019/1157 mērķiem, kas palielina *ID* karšu un uzturēšanās dokumentu drošību. Saskaņā ar šo regulu dalībvalstīm ir pienākums līdz 2021. gada augustam ieviest jaunas personas apliecības ar atjauninātiem drošības elementiem. Pēc izstrādes dalībvalstis varētu uzlabot jaunās identitātes kartes, lai tās varētu pazinot kā *eID* shēmas, kā noteikts *IDAS* regulā.

Iniciatīva arī veicinās muitas jomas pārveidi par elektronisku vidi bez papīriem saistībā ar iniciatīvu par ES vienloga vides izveidi muitas jomā. Jānorāda arī, ka nākotnes priekšlikums veicinās Eiropas mobilitātes politiku, atvieglojot jūras transporta uzņēmēju juridiskās ziņošanas prasības, kas noteiktas saistībā ar Eiropas Jūras vienloga sistēmas vidi, kuru sāks piemērot 2025. gada 15. augustā. Tas pats attiecas uz Regulas par kravu pārvadājumu elektronisku informāciju formulējumu, kas dalībvalstu iestādēm nosaka pienākumu pieņemt elektronisku informāciju par kravu. Eiropas digitālās identitātes maka lietotne varēs arī apstrādāt akreditācijas datus, kas saistīti ar vadītājiem, transportlīdzekļiem un darbībām, kuras noteiktas ES tiesiskajā regulējumā autotransporta jomā (piemēram, digitālās vadītāja apliecības / Direktīva 2006/126/EK). Šā regulējuma kontekstā specifikāciju izstrāde turpināsies. Nākotnes iniciatīva arī varētu palīdzēt veidot nākotnes iniciatīvas sociālā nodrošinājuma koordinācijas jomā, piemēram, iespējamu Eiropas sociālā nodrošinājuma kartes izstrādi, kuras pamatā varētu būt uzticamības pamatelementi, ko sniedz identitātes, kas pazīnotas saskaņā ar *eIDAS*.

Šī iniciatīva atbalsta VDAR (2016/679) īstenošanu, ļaujot lietotājam kontrolēt, kā tiek izmantoti personas dati. Tas nodrošina augstu papildināmību ar jauno Kiberdrošības aktu un tā kopīgajām kiberdrošības sertifikācijas shēmām. Arī

unikālas lietu interneta identitātes nepieciešamība saskaņā ar *eIDAS* nodrošina atbilstību Kiberdrošības aktam un apmierina nepieciešamību aptvert plašāku dalībnieku loku papildus pilsoņiem un uzņēmumiem, piemēram, iekārtas, objektus, piegādātājus un lietu interneta ierīces.

Arī Vienotas digitālās vārtejas regulai (VDVR) ir svarīgi saskares punkti, un tā atbilst šai iniciatīvai. VDVR mērķis ir pilnībā modernizēt valsts pārvaldes pakalpojumus un atvieglot tiešsaistes piekļuvi informācijai, administratīvajām procedūrām un palīdzības pakalpojumiem, kas pilsoņiem un uzņēmumiem nepieciešami, dzīvojot vai strādājot citā ES valstī. Šī iniciatīva nodrošina pamatelementus, ar kuriem atbalsta mērķus panākt, lai vienreizējais princips darbotos saskaņā ar vienoto digitālo vārteju.

Turklāt ir saskanība ar Eiropas Datu stratēģiju un ierosināto regulu par Eiropas datu pārvaldību, proti, tiek nodrošināts regulējums datu lietojumprogrammu atbalstam gadījumos, kad nepieciešama personas identitātes datu pārsūtīšana, ļaujot lietotājiem kontrolēt datus un palikt pilnīgi anonīmiem.

1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums

Iniciatīvas pamatā būs *eID* un uzticamības pakalpojumu pamatelementi, kas tika izstrādāti saskaņā ar EISI programmu un tiek integrēti *DEP*.

Turklāt dalībvalstis var lūgt ANM finansējumu nepieciešamās infrastruktūras izveidei / uzlabošanai.

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

☐ Ierobežots ilgums

- ☐ Priekšlikuma/iniciatīvas darbības laiks: [DD.MM.]GGGG.–[DD.MM.]GGGG.
- ☐ Finansiālā ietekme uz saistību apropriācijām — no GGGG. līdz GGGG. gadam, uz maksājumu apropriācijām — no GGGG. līdz GGGG. gadam.

☒ Neierobežots ilgums

Īstenošana ar sākšanas periodu no GGGG. līdz GGGG. gadam, pēc kura turpinās normāla darbība.

1.7. Paredzētie pārvaldības veidi²⁹

☒ Komisijas īstenota tieša pārvaldība:

- ☒ ko veic tās struktūrvienības, ieskaitot personālu Savienības delegācijās;
- ☐ ko veic izpildaģentūras.

☐ Dalīta pārvaldība kopā ar dalībvalstīm

☐ Netieša pārvaldība, kurā budžeta izpildes uzdevumi uzticēti:

- ☐ trešām valstīm vai to norīkotām struktūrām;
- ☐ starptautiskām organizācijām un to aģentūrām (precizēt);
- ☐ EIB un Eiropas Investīciju fondam;
- ☐ Finanšu regulas 70. un 71. pantā minētajām struktūrām;
- ☐ publisko tiesību subjektiem;
- ☐ privāttiesību subjektiem, kas veic sabiedrisko pakalpojumu sniedzēju uzdevumus, tādā mērā, kādā tie dod pienācīgas finansiālas garantijas;
- ☐ dalībvalstu privāttiesību subjektiem, kuriem ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuri dod pienācīgas finansiālas garantijas;
- ☐ personām, kurām, ievērojot Līguma par Eiropas Savienību V sadaļu, uzticēts īstenot konkrētas KĀDP darbības un kuras ir noteiktas attiecīgajā pamataktā.

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

Piezīmes

[...]

[...]

²⁹ Sīkāku informāciju par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt *BudgWeb* tīmekļa vietnē: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

Norādīt biežumu un nosacījumus.

Regula pirmo reizi tiks pārskatīta divus gadus pēc tās pilnīgas piemērošanas un pēc tam reizi četros gados. Komisijai jāpaziņo konstatējumi Eiropas Parlamentam un Padomei.

Turklāt, piemērojot pasākumus, dalībvalstis vāc statistiku par Eiropas digitālās identitātes maka un kvalificētu uzticamības pakalpojumu lietošanu un darbību. Statistiku apkopo ziņojumā, ko katru gadu iesniedz Komisijai.

2.2. Pārvaldības un kontroles sistēma

2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums

Regula paredz saskaņotākus noteikumus *eID* un uzticamības pakalpojumu sniegšanai iekšējā tirgū, vienlaikus nodrošinot uzticamības ievērošanu un lietotāju kontroli pār saviem datiem. Šie jaunie noteikumi paredz izstrādāt tehniskās specifikācijas un standartus, kā arī uzraudzīt un koordinēt valstu iestāžu darbības. Turklāt saistītie *eID*, e-paraksta utt. pamatelementi tiks pārvaldīti un nodrošināti saskaņā ar *DEP*. Jāņem vērā arī resursi, kas vajadzīgi, lai sazinātos un apspriestu ar trešām valstīm nolīgumu par uzticamības pakalpojumu savstarpēju atzīšanu.

Lai Komisijas dienesti spētu veikt jaunus uzdevumus, tiem jāpiešķir attiecīgi resursi. Tiek lēsts, ka jaunās regulas ieviešanai būs nepieciešami 11 pilnslodzes ekvivalenti; 4-5 pilnslodzes ekvivalenti juridiskajam darbam, 4-5 pilnslodzes ekvivalenti tehniskajam darbam un 2 pilnslodzes ekvivalenti koordinācijai un starptautiskajiem pasākumiem un administratīvajam atbalstam.

2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu

Viena no galvenajām problēmām, kas liek domāt par pašreizējā tiesiskā regulējuma trūkumiem, ir valstu sistēmu nepietiekama saskaņotība. Lai novērstu šo problēmu pašreizējā iniciatīvā, būs lielā mērā jāpaļaujas uz atsauces standartiem un tehniskajām specifikācijām, kas jānosaka īstenošanas aktos.

Šo īstenošanas aktu izstrādē Komisiju atbalstīs ekspertu grupa. Turklāt Komisija jau tagad sadarbosies ar dalībvalstīm, lai vienotos par turpmākās sistēmas tehnisko būtību nolūkā novērst turpmāku sadrumstalotību priekšlikuma apspriešanas laikā.

2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)

Ekspertu grupas sanāksmju izdevumiem pietiekamas šķiet standarta iekšējās kontroles procedūras, jo viena darījuma (piemēram, ceļa izdevumu atmaksāšana delegātam pēc dalības sanāksmē, ja sanāksme notiek reālajā dzīvē) vērtība ir zema.

Arī izmēģinājuma projektos, kas jāveic saskaņā ar *DEP*, būtu jāpietiek ar parastajām *CNECT* ĢD standarta procedūrām.

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus, piemēram, krāpšanas apkarošanas stratēģijā iekļautos pasākumus.

Esošie Komisijai piemērojamie krāpšanas novēršanas pasākumi ietvers šai regulai nepieciešamās papildu apropriācijas.
--

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

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

Esošās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Nr.	Dif./nedif. 30	no EBTA valstīm ³¹	no kandidātvalstīm ³²	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē
2	02 04 05 01 izvērsšana	Dif./	JĀ	NĒ	/NĒ	NĒ
2	02 01 30 01 atbalsta izdevumi programmai "Digitālā Eiropa"	ŅS				
7	20 02 06 Administratīvie izdevumi	ŅS	NĒ			

No jauna veidojamās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Nr.	Dif./nedif.	no EBTA valstīm	no kandidātvalstīm	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē
	[XX.YY.YY.YY]		JĀ/NĒ	JĀ/NĒ	JĀ/NĒ	JĀ/NĒ

³⁰ Dif. = Dif. diferencētās apropriācijas / Nedif. nediferencētās apropriācijas.

³¹ EBTA — Eiropas Brīvās tirdzniecības asociācija.

³² Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām

3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriācijām

- ☐ Priekšlikumam/iniciatīvai nav vajadzīgas darbības apropriācijas
- ☒ Priekšlikumam/iniciatīvai ir vajadzīgas šādas darbības apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

Daudzgadu finanšu shēmas izdevumu kategorija	Nr.	2
---	-----	---

CNECT ĢD			2022. gads	2023. gads	2024. gads	2025. gads	2026. gads	2027. gads		KOPĀ
○ Darbības apropriācijas				Par budžeta sadalījumu lems, izstrādājot darba programmas. Norādītās summas ir uzturēšanai un pilnīgošanai nepieciešamais minimums ³³ .						
Budžeta pozīcija ³⁴ 02 04 05	Saistības	(1a)	2,000	4,000	4,000	4,000	4,000	4,000		22,000
	Maksājumi	(2a)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	22,000
Budžeta pozīcija	Saistības	(1b)								
	Maksājumi	(2b)								
Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķirumiem ³⁵										
Budžeta pozīcija 02 01 03 01		(3)	0,048	0,144	0,144	0,072	0,072	0,072		0,552
KOPĀ CNECT ĢD	Saistības	= 1a + 1b + 3	2,048	4,144	4,144	4,072	4,072	4,072		22,552

³³ Ja faktiskās izmaksas pārsniedz norādītās summas, izmaksas finansēs no 02 04 05 01.

³⁴ Saskaņā ar oficiālo budžeta nomenklatūru.

³⁵ Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās BA pozīcijas), netiešā pētniecība, tiešā pētniecība.

apropriācijas	Maksājumi	= 2a + 2b +3	1,048	3,144	4,144	4,072	4,072	4,072	2,000	22,552
----------------------	-----------	--------------------	-------	-------	-------	-------	-------	--------------	--------------	---------------

○ KOPĀ darbības apropriācijas	Saistības	(4)	2,000	4,000	4,000	4,000	4,000	4,000		22,000
	Maksājumi	(5)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	22,000
○ KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķirumiem		(6)	0,048	0,144	0,144	0,072	0,072	0,072		0,552
KOPĀ daudzgadu finanšu shēmas 2. IZDEVUMU KATEGORIJAS apropriācijas	Saistības	=4+ 6	2,048	4,144	4,144	4,072	4,072	4,072		22,552
	Maksājumi	=5+ 6	0,048	4,144	4,144	4,072	4,072	4,072	2,000	22,552

Daudzgaļu finanšu shēmas izdevumu kategorija	7	“Administratīvie izdevumi”
---	----------	----------------------------

Šī iedaļa būtu jāaizpilda, izmantojot administratīva rakstura budžeta datu izklājlapu, kas vispirms jānoformē [tiesību akta finanšu pārskata pielikumā](#) (iekšējo noteikumu V pielikums), kurš starpdienestu konsultāciju vajadzībām tiek augšupielādēts sistēmā *DECIDE*.

miljonos EUR (trīs zīmes aiz komata)

		2022. gads	2023. gads	2024. gads	2025. gads	2026. gads	2027. gads	KOPĀ
CNECT ĢD								
○ Cilvēkresursi		0,776	1,470	1,470	1,470	1,470	1,318	7,974
○ Citi administratīvie izdevumi		0,006	0,087	0,087	0,087	0,016	0,016	0,299
KOPĀ CNECT ĢD	Apropriācijas	0,782	1,557	1,557	1,557	1,486	1,334	8,273

KOPĀ daudzgaļu finanšu shēmas 7. IZDEVUMU KATEGORIJAS apropriācijas	(Saistību summa = maksājumu summa)	0,782	1,557	1,557	1,557	1,486	1,334	8,273
--	---------------------------------------	-------	-------	-------	-------	-------	-------	--------------

miljonos EUR (trīs zīmes aiz komata)

		2022. gads	2023. gads	2024. gads	2025. gads	2026. gads	2027. gads		KOPĀ
KOPĀ daudzgaļu finanšu shēmas 1.–7. IZDEVUMU KATEGORIJAS apropriācijas	Saistības	2,830	5,701	5,701	5,629	5,558	5,408		30,825
	Maksājumi	1,830	4,701	5,701	5,629	5,558	5,406	2,000	30,825

3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām

Saistību apropriācijas miljonos EUR (trīs zīmes aiz komata)

Norādīt mērķus un iznākumus ↓			2022. gads		2023. gads		2024. gads		2025. gads		2026. gads		2027. gads		KOPĀ	
	Veids 36	Vidējā s izmak sas	Daudzums	Izmak sas	Daudzums	Izmak sas	Daudzums	Izmak sas	Daudzums	Izmak sas	Daudzums	Izma ksas	Daudzums	Izmak sas	Ko pēj ais dau dzu ms	Kopējās izmaksas
KONKRĒTAISMĒRĶISNr. 1 ³⁷ ...			Nodrošināt piekļuvi uzticamiem un drošiem digitālās identitātes risinājumiem, kurus var izmantot pāri robežām, apmierinot lietotāju gaidas un tirgus pieprasījumu.													
Ikgadējie			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Starpsumma – konkrētais mērķis Nr. 1			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
KONKRĒTAISMĒRĶISNr. 2 ...			Nodrošināt to, ka, sniedzot sabiedriskus un privātus pakalpojumus, var paļauties uz uzticamiem un drošiem digitālās identitātes risinājumiem pāri robežām.													
Apsekojumi/pētī			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Starpsumma – konkrētais mērķis Nr. 2			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
KONKRĒTAISMĒRĶISNr. 3 ...			Nodrošināt pilsoņiem pilnīgu kontroli pār saviem personas datiem un garantēt to drošību, izmantojot digitālās identitātes risinājumus.													
Apsekojumi/pētī			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300

³⁶ Rezultāti ir attiecīgie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

³⁷ Konkrētie mērķi, kas norādīti 1.4.2. punktā “Konkrētie mērķi”.

Starpsumma – konkrētais mērķis Nr. 3	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
KONKRĒTAISMĒRĶIS Nr. 4 ...	Nodrošināt vienlīdzīgus nosacījumus kvalificētu uzticamības pakalpojumu sniegšanai ES un to pieņemšanai.													
Apsekojumi/pētī	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
Starpsumma – konkrētais mērķis Nr. 4	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
KOPĀ	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	24	1,200

3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām

- ☐ Priekšlikumam/iniciatīvai nav vajadzīgas administratīvās apropriācijas
- ☒ Priekšlikumam/iniciatīvai ir vajadzīgas šādas administratīvās apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

	2022. gads	2023. gads	2024. gads	2025. gads	2026. gads	2027. gads	KOPĀ
--	---------------	---------------	---------------	---------------	---------------	---------------	------

Daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJA							
Cilvēkresursi	0,776	1,470	1,470	1,470	1,470	1,318	7,974
Citi administratīvie izdevumi	0,006	0,087	0,087	0,087	0,0162	0,0162	0,299
Starpsumma — daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJA	0,782	1,557	1,557	1,557	1,486	1,334	8,273

Ārpus daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS³⁸							
Cilvēkresursi							
Citi administratīvie izdevumi	0,048	0,144	0,144	0,072	0,072	0,072	0 552
Iekļaut administratīvās izmaksas DEP							
Starpsumma — Ārpus daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS	0,048	0,144	0,144	0,072	0,072	0,072	0 552

KOPĀ	0,830	1,701	1,701	1,629	1,558	1,406	8,825
-------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Vajadzīgās cilvēkresursu un citu administratīvu izdevumu apropriācijas tiks nodrošinātas no ĢD apropriācijām, kas jau ir piešķirtas darbības pārvaldībai un/vai ir pārdalītas attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

³⁸ Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās BA pozīcijas), netiešā pētniecība, tiešā pētniecība.

3.2.4. Aplēstās cilvēkresursu vajadzības

- ☐ Priekšlikumam/iniciatīvai nav vajadzīgi cilvēkresursi
- ☒ Priekšlikumam/iniciatīvai ir vajadzīgi šādi cilvēkresursi:

Aplēse izsakāma ar pilnslodzes ekvivalentu

	2022. gads	2023. gads	2024. gads	2025. gads	2026. gads	2027. gads
20 01 02 01 (Galvenā mītne un Komisijas pārstāvniecības)	4	8	8	8	8	7
20 01 02 03 (Delegācijas)						
01 01 01 01 (Netiešā pētniecība)						
01 01 01 11 (Tiešā pētniecība)						
Citas budžeta pozīcijas (norādīt)						
20 02 01 (AC, END, INT, ko finansē no vispārīgajām apropriācijām)	2	3	3	3	3	3
20 02 03 (AC, AL, END, INT un JPD delegācijās)						
XX 01 xx yy zz ³⁹	– galvenajā mītnē					
	– delegācijās					
01 01 01 02 (AC, END, INT — netiešā pētniecība)						
01 01 01 12 (AC, END, INT — tiešā pētniecība)						
Citas budžeta pozīcijas (norādīt)						
KOPĀ	6	11	11	11	11	10

XX ir attiecīgā politikas joma vai budžeta sadaļa.

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

Veicamo uzdevumu apraksts:

Ierēdņi un pagaidu darbinieki	Ierēdņi galvenokārt veiks juridisku darbu, koordinācijas pasākumus un sarunas ar trešām valstīm un struktūrām, kas saistītas ar uzticamības pakalpojumu savstarpēju atzīšanu.
Ārštata darbinieki	Valstu ekspertiem būtu jāatbalsta sistēmas tehniskā un funkcionālā iestatīšana. AC būtu jāsniedz atbalsts arī tehniskajos uzdevumos, tostarp pamatelementu pārvaldībā.

³⁹ Ārštata darbiniekiem paredzēto maksimālo summu finansē no darbības apropriācijām (kādreizējām BA pozīcijām).

3.2.5. Saderība ar pašreizējo daudzgadu finanšu shēmu

Priekšlikums/iniciatīva:

- ☒ pilnībā pietiek ar līdzekļu pārvietošanu daudzgadu finanšu shēmas (DFS) attiecīgajā izdevumu kategorijā;

Aprakstīt, kas jāpārplāno, norādot attiecīgās budžeta pozīcijas un atbilstošās summas. Lielas pārplānošanas gadījumā sniedziet *Excel* tabulu.

- ☐ jāizmanto no DFS attiecīgās izdevumu kategorijas nepiešķirtās rezerves un/vai īpašie instrumenti, kas noteikti DFS regulā;

Paskaidrojiet, kas jā dara, norādot attiecīgās izdevumu kategorijas un budžeta pozīcijas, atbilstošās summas un instrumentus, kurus ierosināts izmantot.

- ☐ jāpārskata DFS.

Paskaidrojiet, kas jā dara, norādot attiecīgās izdevumu kategorijas, budžeta pozīcijas un atbilstošās summas.

3.2.6. Trešo personu iemaksas

Priekšlikums/iniciatīva:

- ☒ neparedz trešo personu līdzfinansējumu;
- ☐ paredz trešo personu sniegtu līdzfinansējumu:

Apropriācijas miljonos EUR (trīs zīmes aiz komata)

	N gads ⁴⁰	N+1 gads	N+2 gads	N+3 gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			Kopā
Norādīt līdzfinansētāju struktūru								
KOPĀ līdzfinansētās apropriācijas								

⁴⁰ N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet "N" ar paredzēto pirmo īstenošanas gadu (piemēram, (2021)). Tas pats attiecas uz turpmākajiem gadiem.

3.3. Aplēstā ietekme uz ieņēmumiem

☒ Priekšlikums/iniciatīva finansāli neietekmē ieņēmumus.

☐ Priekšlikums/iniciatīva finansāli ietekmē:

☐ pašu resursus

☐ citus ieņēmumus

Atzīmējiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām ☐

miljonos EUR (trīs zīmes aiz komata)

Budžeta pozīcija:	ieņēmumu	Kārtējā finanšu gadā pieejamās apropriācijas	Priekšlikuma/iniciatīvas ietekme ⁴¹						
			N gads	N+1 gads	N+2 gads	N+3 gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
..... pants									

Attiecībā uz piešķirtajiem ieņēmumiem norādīt attiecīgās budžeta izdevumu pozīcijas.

[...]

Citas piezīmes (piemēram, metode/formula, ko izmanto, lai aprēķinātu ietekmi uz ieņēmumiem, vai jebkura cita informācija).

[...]

⁴¹ Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t. i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 20 % apmērā.

**PIELIKUMS
TIESĪBU AKTA FINANŠU PĀRSKATAM**

Priekšlikuma/iniciatīvas nosaukums:

Priekšlikums Regulai par Eiropas digitālās identitātes regulējumu, ar ko groza *eIDAS* regulu

- 1. VAJADZĪGO CILVĒKRESURSU SKAITS UN IZMAKSAS**
- 2. CITU ADMINISTRATĪVO IZDEVUMU IZMAKSAS**
- 3. KOPĒJĀS ADMINISTRATĪVĀS IZMAKSAS**
- 4. IZMAKSU APRĒĶINĀŠANAI IZMANTOTĀS METODES**
 - 4.1. Cilvēkresursi**
 - 4.2. Citi administratīvie izdevumi**

Sākot starpdienestu apspriešanos, šis pielikums jāpievieno tiesību akta finanšu pārskatam.

Datu tabulas tiek izmantotas par avotu tiesību akta finanšu pārskatā iekļautajām tabulām. Tās paredzētas tikai un vienīgi Komisijas iekšējai lietošanai.

(49) Par vajadzīgiem uzskatīto cilvēkresursu skaits un izmaksas

- ☐ Priekšlikumam/iniciatīvai nav vajadzīgi cilvēkresursi
- ☒ Priekšlikumam/iniciatīvai ir vajadzīgi šādi cilvēkresursi:

miljonos EUR (trīs zīmes aiz komata)

HEADING 7 of the multiannual financial framework	Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL		
	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	
• Establishment plan posts (officials and temporary staff)															
20 01 02 01 - Headquarters and Representation offices	AD	4	608	7	1.064	7	1.064	7	1.064	7	1.064	6	912	38	5.776
	AST	0	-	1	152	1	152	1	152	1	152	1	152	5	760
20 01 02 03 - Union Delegations	AD														
	AST														
External staff [1]															
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC	1	82	1	82	1	82	1	82	1	82	1	82	6	492
	END	1	86	2	172	2	172	2	172	2	172	2	172	11	946
	INT														
20 02 03 – External personnel - Union Delegations	AC														
	AL														
	END														
	INT														
	JPD														
Other HR related budget lines (specify)															
Subtotal HR – HEADING 7		6	776	11	1.470	11	1.470	11	1.470	11	1.470	10	1.318	60	7.974

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

4.4.

4.5.

Ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS			2022. gads		2023. gads		2024. gads		2025. gads		2026. gads		2027. gads		KOPĀ	
			FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas
01 01 01 01 (Netiešā pētniecība) ⁴² 01 01 01 11 (Tiešā pētniecība) Cita (precizējiet)	AD															
	AST															
Ārštata darbinieki no darbības apropriācijām (kādreizējām BA pozīcijām).	– galvenajā mītnē	AC														
		END														
		INT														
	- Savienības delegācijās	AC														
		AL														
		END														
		INT														
		JPD														
01 01 01 02 Netiešā pētniecība 01 01 01 12 Tiešā pētniecība Cita (precizējiet) ⁴³	AC															
	END															
	INT															
Citas budžeta pozīcijas, kas saistītas ar cilvēkresursiem (norādīt)																

⁴² Lūdzu, izvēlieties attiecīgo budžeta pozīciju vai vajadzības gadījumā norādiet citu; ja ir skartas vairākas budžeta pozīcijas, personāls būtu jādiferencē katrā attiecīgajā budžeta pozīcijā.

⁴³ Lūdzu, izvēlieties attiecīgo budžeta pozīciju vai vajadzības gadījumā norādiet citu; ja ir skartas vairākas budžeta pozīcijas, personāls būtu jādiferencē katrā attiecīgajā budžeta pozīcijā.

Starpsumma cilvēkresursiem — ārpus 7. IZDEVUMU KATEGORIJAS															
Kopā cilvēkresursi (visas DFS izdevumu kategorijas)		6	0,776	11	1,470	11	1,470	11	1,470	11	1,470	10	1,318	60	7,974

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

4.6. Citu administratīvo izdevumu izmaksas

4.7. ☐ Priekšlikums/iniciatīva neparedz administratīvo apropriāciju izmantošanu

4.8. ☒ Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādā veidā:

miljonos EUR (trīs zīmes aiz komata)

Daudzgaļu finanšu shēmas 7. IZDEVUMU KATEGORIJA	2022. gads	2023. gads	2024. gads	2025. gads	2026. gads	2027. gads	Kopā
Galvenajā mītnē vai ES teritorijā:							
20 02 06 01 - Komandējumu un reprezentācijas izmaksas	0,006	0,015	0,015	0,015	0,015	0,015	0,081
20 02 06 02 - Konferenču un sanāksmju izmaksas							
20 02 06 03 - Komitejas ⁴⁴		0,072	0,072	0,072	0,0012	0,012	0,218
20 02 06 04 – Pētījumi un apspriedes							
20 04 – IT izdevumi (uzņēmumu) ⁴⁵							
Citas budžeta pozīcijas, kas nav saistītas ar cilvēkresursiem (vajadzības gadījumā norādīt)							
Savienības delegācijās							
20 02 07 01 – Komandējumi, konferences un reprezentācijas izmaksas							
20 02 07 02 – Darbinieku kvalifikācijas celšana							
20 03 05 – Infrastruktūra un loģistika							
Citas budžeta pozīcijas, kas nav saistītas ar cilvēkresursiem (vajadzības gadījumā norādīt)							
Starpsumma – Citi – Daudzgaļu finanšu shēmas 7. IZDEVUMU KATEGORIJA	0,006	0,087	0,087	0,087	0,016	0,016	0,299

⁴⁴ Precizēt komitejas veidu un grupu, pie kuras tā pieder.

⁴⁵ Vajadzīgs DIGIT ĢD – IT ieguldījumu grupas atzinums (sk. IT finansēšanas pamatnostādnes, C(2020)6126 final, 10.9.2020., 7. lpp.)

miljonos EUR (trīs zīmes aiz komata)

Ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA	2022. gads	2023. gads	2024. gads	2025. gads	2026. gads	2027. gads	Kopā
Izdevumi tehniskai un administratīvai palīdzībai (neietverot ārštata darbiniekus) no darbības apropriācijām (kādreizējās "BA" pozīcijas):	0,048	0,144	0,144	0,072	0,072	0,072	0,552
– galvenajā mītnē							
– Savienības delegācijās							
Citi pārvaldības izdevumi pētniecībai							
Politikas IT izdevumi darbības programmām ⁴⁶							
Uzņēmumu IT izdevumi darbības programmām ⁴⁷							
Citas budžeta pozīcijas, kas nav saistītas ar cilvēkresursiem (vajadzības gadījumā norādīt)							
Starpsumma – Citi — Ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS	0,048	0,144	0,144	0,072	0,072	0,072	0,552
Kopā citas administratīvās izmaksas (visas DFS izdevumu kategorijas)	0,054	0,231	0,231	0,159	0,088	0,088	0,851

⁴⁶ Vajadzīgs DG DIGIT – IT ieguldījumu grupas atzinums (sk. IT finansēšanas pamatnostādnes, C(2020)6126 final, 10.9.2020., 7. lpp.)

⁴⁷ Šajā postenī iekļautas vietējās administratīvās sistēmas un iemaksas uzņēmumu IT sistēmu līdzfinansējumā (sk. IT finansēšanas pamatnostādnes, C (2020) 6126 final, 10.9.2020.)

5. KOPĒJĀS ADMINISTRATĪVĀS IZMAKSAS(VISAS DFS IZDEVUMU KATEGORIJAS)

miljonos EUR (trīs zīmes aiz komata)

Kopsavilkums	2022. gads	2023. gads	2024. gads	2025. gads	2026. gads	2027. gads	Kopā
7. izdevumu kategorija – Cilvēkresursi	0,776	1,470	1,470	1,470	1,470	1,318	7,974
7. izdevumu kategorija — Citi administratīvie izdevumi	0,006	0,087	0,087	0,087	0,016	0,016	0,218
Starpsumma – 7. izdevumu kategorija							
Ārpus 7. izdevumu kategorijas – Cilvēkresursi							
Ārpus 7. izdevumu kategorijas — Citi administratīvie izdevumi	0,048	0,144	0,144	0,072	0,072	0,072	0,552
Starpsumma – Citas izdevumu kategorijas							
1. KOPA							
2. 7. IZDEVUMU KATEGORIJA un ārpus 7. IZDEVUMU KATEGORIJAS	0,830	1,701	1,701	1,629	1,558	1,406	8,825

- (1) Vajadzīgās administratīvās apropriācijas nodrošinās, izmantojot apropriācijas, kuras jau piešķirtas darbības pārvaldībai un/vai ir pārgrupētas, vajadzības gadījumā izmantojot vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

6. IZMANTOTĀS IZMAKSU APRĒĶINĀŠANAS METODES

(a) Cilvēkresursi

Šajā daļā ir izklāstīta aprēķina metode, ko izmanto nepieciešamo cilvēkresursu aplēšanai (pieņēmumi par darba slodzi, ieskaitot īpašus darbus (Sysper 2 darba profili), darbinieku kategorijas un atbilstīgās vidējās izmaksas)

1.	Daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJA
2.	Svarīgi! Galvenās mītnes katras darbinieku kategorijas vidējās izmaksas ir pieejamas BudgWeb:
3.	https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx .
4.	☐ Ierēdņi un pagaidu darbinieki
5.	7 AD ierēdņi (tostarp 1 no CNECT/F.3 2023.–2024. gadā) x 152 000 euro gadā 2023.–2027. gadā (puse no tā 2022. gadā, tā kā pieņemšana paredzēta 2022. gada vidū);
6.	1 AST ierēdnis x 152 000 euro gadā 2023.–2027. gadā (puse no tā 2022. gadā, tā kā pieņemšana paredzēta 2022. gada vidū)
7.	
8.	☐ Ārštata darbinieki
9.	AC 1 x 82 000 euro gadā 2023.–2027. gadā (puse no tā 2022. gadā, tā kā pieņemšana paredzēta 2022. gada vidū) (piemērots indeksācijas koeficients);
10.	END 2 x 86 000 euro gadā 2023.–2027. gadā (puse no tā 2022. gadā, tā kā pieņemšana paredzēta 2022. gada vidū) (piemērots indeksācijas koeficients);
11.	

12.	Ārpus daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS
13.	☐ Vienīgi amata vietas, ko finansē no pētniecības budžeta
14.	
15.	☐ Ārštata darbinieki
16.	

7. CITI ADMINISTRATĪVIE IZDEVUMI

Norādīt aprēķinu metodi, kas izmantota katrai budžeta pozīcijai un jo īpaši pamatā esošajiem pieņēmumiem (piemēram, sanāksmju skaits gadā, vidējās izmaksas utt.)

17.	Daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJA
18.	Komitejas sanāksmes divas reizes mēnesī x 12 000 euro par sanāksmi 2022.–2024. gadā, lai pieņemtu īstenošanas aktus. Pēc tam komitejas ikgadējās sanāksmes, lai pieņemtu atjauninātus īstenošanas aktus.
19.	Komandējumi galvenokārt uz Luksemburgu un Briseli, taču arī konferences, sanāksmes ar dalībvalstīm un citām ieinteresētajām personām.
20.	

21.	Ārpus daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS
22.	Ekspertu grupas sanāksmes tiek apmaksātas no DEP administratīvo izmaksu pozīcijas.
23.	Sagaidāms, ka īstenošanas akta sagatavošanas laikā (2022.–2024. gada vidus) notiks ikmēneša sanāksmes (12 000 EUR), un ārpus minētā laika perioda divreiz mēnesī paredzētas sanāksmes, lai nodrošinātu ES mēroga koordināciju saistībā ar tehnisko ieviešanu.
24.	