Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/2532

17.12.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/2532

(2025. gada 16. decembris),

ar ko nosaka noteikumus Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanai attiecībā uz kvalificētu elektroniskās arhivēšanas pakalpojumu atsauces standartiem un specifikācijām

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 45.j panta 2. punktu,

tā kā:

(1) Ar Eiropas Parlamenta un Padomes Regulu (ES) 2024/1183 ([2]) Regulā (ES) Nr. 910/2014 tika ieviests saraksts ar jauniem uzticamības pakalpojumiem un kvalificētiem uzticamības pakalpojumiem, citastarp arī kvalificēts elektroniskās arhivēšanas pakalpojums. Komisijai ir jāizveido šādu pakalpojumu atsauces standartu saraksts un vajadzības gadījumā jānosaka šādu pakalpojumu specifikācijas.

(2) Elektroniska arhivēšana ir pakalpojums elektronisku datu un elektronisku dokumentu saņemšanai, glabāšanai, izguvei un dzēšanai, lai nodrošinātu to ilglaicīgumu un lasāmību, kā arī saglabātu to integritāti, konfidencialitāti un izcelsmes apliecinājumu visā saglabāšanas periodā. Kvalificētiem elektroniskās arhivēšanas pakalpojumiem ir izšķiroša nozīme digitālās uzņēmējdarbības vidē, jo tie veicina pāreju no tradicionāliem procesiem papīra formātā uz elektroniskiem ekvivalentiem. Lai nodrošinātu, ka elektroniskiem datiem un elektroniskiem dokumentiem visā kvalificēta uzticamības pakalpojumu sniedzēja īstenotā saglabāšanas periodā saglabājas prezumpcija par to integritāti un izcelsmi, un lai panāktu augstu pārredzamības un uzticēšanās līmeni visu informācijas aprites cikla dalībnieku vidū, kvalificētiem elektroniskās arhivēšanas pakalpojumiem ir jānosaka vienots specifikāciju kopums.

(3) Lai palielinātu tādu kvalificētu elektroniskās arhivēšanas pakalpojumu pierādījuma spēku, drošību un uzticamību, kuros elektroniskos parakstus, elektroniskos zīmogus vai elektroniskos laika zīmogus izmanto, lai izveidotu, parakstītu, apzīmogotu vai apliecinātu, piemēram, pierādījumu arhivēšanas, pierādījumu ierakstu, notikumu ierakstu, procedūru pareizas īstenošanas ierakstu vai apstiprinājuma ziņojumu arhivēšanas datumu un laiku, būtu jāizmanto kvalificēti uzticamības pakalpojumi.

(4) Regulas (ES) Nr. 910/2014 45.j panta 2. punktā noteiktais pieņēmums par atbilstību būtu piemērojams tikai tad, ja kvalificēti elektroniskās arhivēšanas pakalpojumi atbilst šajā regulā noteiktajām prasībām. Kvalificētu elektroniskās arhivēšanas pakalpojumu atsauces standartiem būtu jāatspoguļo iedibinātā prakse un jābūt plaši atzītiem attiecīgajās nozarēs. Tie būtu jāpielāgo, lai iekļautu papildu kontroles, kas nodrošina kvalificētas elektroniskās arhivēšanas pakalpojumu drošību un uzticamību.

(5) Ja uzticamības pakalpojumu sniedzējs ievēro šajā regulā noteiktās prasības, uzraudzības iestādēm būtu jāpieņem, ka Regulas (ES) Nr. 910/2014 attiecīgās prasības ir ievērotas, un šāds pieņēmums pienācīgi jāņem vērā, piešķirot vai apstiprinot uzticamības pakalpojuma kvalifikācijas statusu. Tomēr, lai pierādītu atbilstību Regulas (ES) Nr. 910/2014 prasībām, kvalificēts uzticamības pakalpojumu sniedzējs joprojām drīkst izmantot citu praksi.

(6) Lai saglabātu tādu elektronisko datu un elektronisko dokumentu integritāti un izcelsmes apliecinājumu, kuros ir viens vai vairāki kvalificēti elektroniskie paraksti vai zīmogi, kvalificētiem elektroniskās arhivēšanas pakalpojumiem būtu jāizmanto procedūras un tehnoloģijas, kas spēj pagarināt minēto elektronisko parakstu un zīmogu uzticamību pēc tehnoloģiskā derīguma termiņa beigām, vismaz visā saglabāšanas periodā.

([1]) OV L 257, 28.8.2014., 73. lpp., ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Eiropas Parlamenta un Padomes Regula (ES) 2024/1183 (2024. gada 11. aprīlis), ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi (OV L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(7) Komisija regulāri novērtē jaunās tehnoloģijas, praksi, standartus un tehniskās specifikācijas. Saskaņā ar Regulas (ES) 2024/1183 75. apsvērumu Komisijai šī regula būtu jāpārskata un vajadzības gadījumā jāatjaunina nolūkā nodrošināt tās atbilstību globālajām norisēm, jaunām tehnoloģijām, praksei, standartiem un tehniskajām specifikācijām un nolūkā ievērot paraugpraksi iekšējā tirgū.

(8) Šajā regulā paredzētajām personas datu apstrādes darbībām piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([3]) un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([4]).

(9) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([5]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2025. gada 21. oktobrī sniedza savu atzinumu ([6]).

(10) Šajā regulā noteiktie pasākumi saskan ar atzinumu, ko sniegusi ar Regulas (ES) Nr. 910/2014 48. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Ar kvalificētu elektronisko parakstu parakstītu vai ar kvalificētu elektronisko zīmogu apzīmogotu dokumentu elektroniska arhivēšana

1. Arhivējot elektroniskus datus vai elektroniskus dokumentus, kas satur kvalificētus elektroniskos parakstus vai kvalificētus elektroniskos zīmogus, kvalificētu elektroniskās arhivēšanas pakalpojumu sniedzēji nodrošina, ka tiek saglabāta minēto kvalificēto elektronisko parakstu vai kvalificēto elektronisko zīmogu uzticamība, arī pēc to tehnoloģiskā derīguma termiņa beigām, un ka vismaz līdz juridiskās vai līgumiskās saglabāšanas perioda beigām tiek saglabāta kvalificēto elektronisko parakstu un zīmogu integritāte un izcelsmes precizitāte.

2. Šā panta 1. punkta vajadzībām kvalificētu elektroniskās arhivēšanas pakalpojumu sniedzēji drīkst izmantot kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumu vai kvalificētu elektronisko zīmogu kvalificētas saglabāšanas pakalpojumu.

2. pants

Kvalificētu elektroniskās arhivēšanas pakalpojumu atsauces standarti un specifikācijas

Regulas (ES) Nr. 910/2014 45.j panta 2. punktā minētie atsauces standarti un specifikācijas ir noteiktas šīs regulas pielikumā.

([3]) 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., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) 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., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([6]) EDAU oficiālās piezīmes par projektu īstenošanas regulai, ar ko nosaka noteikumus Regulas (ES) Nr. 910/2014 piemērošanai attiecībā uz kvalificētu elektroniskās arhivēšanas pakalpojumu atsauces standartiem un specifikācijām.

3. pants

Stāšanās spēkā

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

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

Briselē, 2025. gada 16. decembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

PIELIKUMS

Kvalificētu elektroniskās arhivēšanas pakalpojumu atsauces standartu un specifikāciju saraksts

Standartu CEN/TS 18170:2025 (“CEN/TS 18170”) piemēro ar šādiem pielāgojumiem.

a) Normatīvās atsauces (2. punkts)

— ETSI EN 319 401 V3.1.1 (2024-06) “Elektroniskie paraksti un uzticamības infrastruktūras (ESI). Vispārējās politikas prasības uzticamības pakalpojumu sniedzējiem”.

— ETSI EN 319 421 V1.3.1 (2025-07) “Elektroniskie paraksti un infrastruktūras (ESI). Politikas un drošības prasības uzticamības pakalpojumu sniedzējiem, kas izdod laika zīmogus”.

— ISO 14721:2025 “Kosmosa datu sistēmu prakse. Atvērtas arhīvu informācijas sistēmas (*OAIS*) atsauces modelis”.

— *ACM-ECCG* Eiropas Kiberdrošības sertifikācijas grupas kriptogrāfijas jautājumu apakšgrupa – “Saskaņoti kriptogrāfijas mehānismi”, ko publicējusi Eiropas Savienības Kiberdrošības aģentūra (*ENISA*).

— Komisijas Īstenošanas regula (ES) 2024/482 ([1]).

— Komisijas Īstenošanas regula (ES) 2024/3144 ([2]).

— ISO/IEC 15408:2022 (1.–5. daļa) “Informācijas drošība, kiberdrošība un privātuma aizsardzība. IT drošības vērtēšanas kritēriji”.

— FIPS PUB 140-3 (2019) “Drošības prasības kriptogrāfijas moduļiem”.

b) Politikas un prakses paziņojums (6.1. punkts)

— Piemēro CEN/TS 18170 6.1. punkta prasības.

— Piemēro ETSI EN 319 401 5. punkta prasības.

— Elektroniskās arhivēšanas uzticamības pakalpojumu sniedzējs (*EATSP*) saskaņā ar uzņēmējdarbības prasībām un attiecīgiem normatīvajiem aktiem, citastarp saskaņā ar to īstenošanas aktu prasībām, kas pieņemti, ievērojot Regulas (ES) Nr. 910/2014 [i.2] 24. panta 5. punktu, izveido procedūras uzraudzības iestādes informēšanai par visām izmaiņām elektroniskās arhivēšanas uzticamības pakalpojuma sniegšanā un par nodomu pārtraukt minētās darbības.

— *EATSP* kompetento uzraudzības iestādi informē vismaz:

— vienu mēnesi pirms jebkādu izmaiņu ieviešanas,

— trīs mēnešus pirms plānotās uzticamības pakalpojuma sniegšanas pārtraukšanas.

c) Noteikumi (6.2. punkts)

— Piemēro CEN/TS 18170 6.2. punkta prasības.

— Abonentus un puses, kas izmanto elektroniskās arhivēšanas uzticamības pakalpojumu, pirms līgumattiecību uzsākšanas skaidrā, visaptverošā un viegli pieejamā veidā publiski pieejamā telpā un individuāli informē par precīziem noteikumiem.

([1]) Komisijas Īstenošanas regula (ES) 2024/482 (2024. gada 31. janvāris) par to, kā vienotos kritērijos balstītas Eiropas kiberdrošības sertifikācijas shēmas (*EUCC*) pieņemšanas sakarā piemērojama Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (OV L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Komisijas Īstenošanas regula (ES) 2024/3144 (2024. gada 18. decembris) par Īstenošanas regulas (ES) 2024/482 grozījumiem attiecībā uz piemērojamajiem starptautiskajiem standartiem un par tās labojumiem (OV L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

d) Cilvēkresursi (7.3. punkts)

— Piemēro CEN/TS 18170 7.3. punkta prasības.

— *EATSP* darbinieki, kas pilda uzticamības funkcijas, un attiecīgā gadījumā apakšuzņēmēji, kas pilda uzticamības funkcijas, spēj izpildīt prasību par "ekspertu zināšanām, pieredzi un kvalifikāciju", izmantojot oficiālu apmācību un apliecinājumus vai faktisku pieredzi, vai abu kombināciju. Tas ietver regulārus atjauninājumus (vismaz reizi 12 mēnešos) par jauniem apdraudējumiem un pašreizējo drošības praksi.

e) Kriptogrāfiskās kontroles un uzraudzība (7.6. punkts)

— Arhivēšanas sistēmai jāgarantē datu un dokumentu konfidencialitāte visā arhīva dzīves ciklā no to deponēšanas līdz likvidēšanai.

— Piemēro ETSI EN 319 401 7.5. apakšpunktā "Kriptogrāfijas kontroles" noteiktās prasības.

— Elektroniskajā arhivēšanas sistēmā arhivējamo datu izcelsmi apliecina *EATSP*. Ja *EATSP* šim nolūkam izmanto elektroniskos parakstus vai elektroniskos zīmogus, minētajiem elektroniskajiem parakstiem vai elektroniskajiem zīmogiem ir jābūt kvalificētiem.

— Kad *EATSP* digitāli paraksta digitālu objektu vai tā daļu vai digitālu ierakstu vai tā daļu, *EATSP* privāto paraksta atslēgu tur un izmanto vai nu kvalificētā elektroniskā paraksta vai zīmoga radīšanas ierīcē, vai drošā kriptogrāfiskā ierīcē, kas ir uzticama sistēma, kura sertificēta saskaņā ar:

a) vienotiem informācijas tehnoloģiju drošības izvērtēšanas kritērijiem, kas noteikti ISO/IEC 15408 vai Vienotajos informācijas tehnoloģiju drošības izvērtēšanas kritērijos, CC:2022. redakcija, 1.–5. daļa, ko publicējuši Vienošanās par vienotu kritēriju sertifikātu atzīšanu IT drošības jomā dalībnieki, un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

b) vienotos kritērijos balstīto Eiropas kiberdrošības sertifikācijas shēmu (Komisijas Īstenošanas regula (ES) 2024/482, Komisijas Īstenošanas regula (ES) 2024/3144), un sertificēta saskaņā ar *EAL* 4 vai augstāku standartu; vai

c) FIPS PUB 140-3 3. līmeni (līdz 31.12.2030.).

— Šī sertifikācija attiecas uz drošības mērķrādītāju vai aizsardzības profilu vai uz moduļa konstrukciju un drošības dokumentāciju, kas atbilst šā dokumenta prasībām, pamatojoties uz riska analīzi un ņemot vērā fiziskos un citus netehniskos drošības pasākumus.

— Ja drošas kriptogrāfijas ierīcei piemēro *EUCC* (Īstenošanas regula (ES) 2024/482, Komisijas Īstenošanas regula (ES) 2024/3144) sertifikāciju, šo ierīci konfigurē un izmanto saskaņā ar minēto sertifikāciju.

— *EATSP* uzrauga kriptogrāfijas algoritma, kas tika un tiek izmantots, stiprumu. Ja tiek uzskatīts, ka kāds no izmantotajiem algoritmiem vai parametriem kļūst nepiemērots, kā noteikts riska pārvaldībā, *EATSP* vai nu atjaunina saistīto arhivēšanas politiku, vai izveido jaunu arhivēšanas profilu, lai apstrādātu *AIP* un definētu un veiktu atbilstošus pasākumus.

— Kriptogrāfijas algoritmu izvērtējums un tas, kā tos izmanto *EATSP*, atbilst saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi *ENISA* (*ACM-ECCG*).

— *EATS* tehniskie komponenti pirms saziņas autentificē cits citu, pamatojoties uz kriptogrāfiskiem paņēmieniem.

f) Tīkls (7.9. punkts)

— Piemēro ETSI EN 319 401 7.8. apakšpunktā "Tīkla drošība" noteiktās prasības.

— Ievainojamības skenēšanu, kas prasīta ETSI EN 319 401 REQ-7.8-13, veic vismaz reizi ceturksnī.

— Ielaušanās testu, kas prasīts ETSI EN 319 401 REQ-7.8-17X, veic vismaz reizi gadā.

— Ugunsmūri ir konfigurēti tā, lai novērstu visus tos protokolus un piekļuves, kas nav vajadzīgas *EATSP* darbībai.

g) Pierādījumu vākšana (7.11. punkts)

— Piemēro ETSI EN 319 401 7.10. apakšpunktā "Pierādījumu vākšana" noteiktās prasības, citastarp attiecībā uz kritiskiem un nekritiskiem notikumiem (sk. 13.2. apakšpunktu).

h) *EATSP* izbeigšana un izbeigšanas plāns (7.13. punkts)

— Piemēro CEN/TS 18170 7.13. punkta prasības.

— *EATSP* izbeigšanas plāns atbilst prasībām, kas noteiktas īstenošanas aktos, kuri pieņemti saskaņā ar Regulas (ES) Nr. 910/2014 24. panta 5. punktu.

i) Uzticams notikumu laiks (13.3.1. punkts)

— Piemēro CEN/TS 18170 13.3.1. punkta prasības.

— Izmantojot laika zīmogus, *EATSP* izmanto kvalificētu laika zīmogu.