Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/1550

29.7.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/1550

(2025. gada 28. jūlijs),

ar ko nosaka Eiropas Parlamenta un Padomes Regulā (ES) 2023/1543 minētās decentralizētās IT sistēmas tehniskās specifikācijas un citas prasības

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2023/1543 (2023. gada 12. jūlijs) par Eiropas e-pierādījumu sniegšanas rīkojumiem un Eiropas e-pierādījumu saglabāšanas rīkojumiem e-pierādījumu gūšanai kriminālprocesā un brīvības atņemšanas sodu izpildei pēc kriminālprocesa ([1]) un jo īpaši tās 25. panta 1. punkta a), b), c) un d) apakšpunktu,

tā kā:

(1) Lai izveidotu Regulā (ES) 2023/1543 minēto decentralizēto IT sistēmu, ir jādefinē un jāpieņem tehniskās specifikācijas, pasākumi un mērķi minētās sistēmas ieviešanai.

(2) Decentralizētajā IT sistēmā saskaņā ar Regulu (ES) 2023/1543 būtu jāiekļauj dalībvalstu un Savienības aģentūru un struktūru IT sistēmas, kā arī sadarbspējīgi *e-CODEX* piekļuves punkti, ar kuru starpniecību šīs IT sistēmas ir savstarpēji savienotas. Tādējādi decentralizētās IT sistēmas tehniskajām specifikācijām un citām prasībām būtu jāatspoguļo šis satvars.

(3) Decentralizētās IT sistēmas piekļuves punktu pamatā saskaņā ar Regulu (ES) 2023/1543 vajadzētu būt autorizētiem *e-CODEX* piekļuves punktiem, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2022/850 ([2]) 3. panta 3. punktā.

(4) Dalībvalstis var izmantot kā savu aizmugursistēmu Komisijas izstrādāto references īstenošanas programmatūru valsts IT sistēmas vietā. Lai nodrošinātu sadarbspēju, gan uz valsts IT sistēmām, gan references īstenošanas programmatūru būtu jāattiecina vienas un tās pašas tehniskās specifikācijas un prasības, kas noteiktas šajā regulā.

(5) Lai mazinātu iespējamās tehniskās problēmas, kas saistītas ar decentralizētās IT sistēmas jaudu un uzticamību, ir jānosaka robežvērtība ar minētās sistēmas starpniecību nosūtīto e-pierādījumu apjomam. Pēc sistēmas palaišanas būtu jāuzrauga šādu nosūtīšanu biežums un apjoms un vajadzības gadījumā būtu jāpielāgo robežvērtība, lai maksimāli palielinātu sistēmas efektivitāti.

(6) Lai stiprinātu decentralizētās IT sistēmas sadarbspēju un efektivitāti, būtu jānosaka prasība izmantot atbilstošus ETSI standartus. Būtu jāuzrauga turpmākā attīstība un vajadzības gadījumā jāapsver papildu ETSI standartu pieņemšana.

(7) Īrijai Regula (ES) 2023/1543 ir saistoša, tādēļ tā piedalās šīs regulas pieņemšanā.

(8) Saskaņā ar 1. un 2. pantu Protokolā Nr. 22 par Dānijas nostāju, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, Dānijai šī regula nav saistoša un nav jāpiemēro.

([1]) OV L 191, 28.7.2023., 118. lpp., ELI: http://data.europa.eu/eli/reg/2023/1543/oj.
([2]) Eiropas Parlamenta un Padomes Regula (ES) 2022/850 (2022. gada 30. maijs) par datorizētu sistēmu datu pārrobežu elektroniskai apmaiņai tiesu iestāžu sadarbības civillietās un krimināllietās jomā (*e-CODEX* sistēma) un ar ko groza Regulu (ES) 2018/1726 (OV L 150, 1.6.2022., 1. lpp., ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([3]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2025. gada 25. jūnijā sniedza atzinumu.

(10) Šajā regulā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kas izveidota ar Regulas (ES) 2023/1543 26. pantu,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Decentralizētās IT sistēmas tehniskās specifikācijas

Regulas (ES) 2023/1543 25. panta 1. punktā minētās decentralizētās IT sistēmas tehniskās specifikācijas un prasības, pasākumi un mērķi saziņai minētās regulas 19. panta nozīmē ir noteikti šīs regulas pielikumā.

2. pants

Stāšanās spēkā

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

Šī regula uzliek saistības kopumā un ir tieši piemērojama dalībvalstīs saskaņā ar Līgumiem.

Briselē, 2025. gada 28. jūlijā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

([3]) 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).

PIELIKUMS

DECENTRALIZĒTĀS IT SISTĒMAS TEHNISKĀS SPECIFIKĀCIJAS

(minētas 1. pantā)

1. **Ievads un darbības joma**

Šajā pielikumā ir noteiktas decentralizētās IT sistēmas tehniskās specifikācijas, pasākumi un mērķi Regulā (ES) 2023/1543 paredzētajām procedūrām.

Saskaņā ar Regulu (ES) 2023/1543 un jo īpaši tās 19. pantu decentralizētajai IT sistēmai ir jānodrošina rakstiska saziņa starp kompetentajām iestādēm un izraudzītajiem iedibinājumiem vai juridiskajiem pārstāvjiem, starp kompetentajām iestādēm, kā arī starp kompetentajām iestādēm un kompetentajām Savienības aģentūrām vai struktūrām.

2. **Definīcijas**

2.1. "hiperteksta drošas pārsūtīšanas protokols" jeb "*HTTPS*" ir šifrēta saziņa un droša savienojuma kanāli;

2.2. "izcelsmes nenoliedzamība" ir pasākumi, kas, izmantojot tādas metodes kā digitālā sertifikācija, publiskās atslēgas infrastruktūra un elektroniskie paraksti, un elektroniskie zīmogi, apliecina datu integritāti un to izcelsmi;

2.3. "saņemšanas nenoliedzamība" ir pasākumi, kas, izmantojot tādas metodes kā digitālā sertifikācija, publiskās atslēgas infrastruktūra un elektroniskie paraksti, un elektroniskie zīmogi, datu nosūtītājam apliecina, ka dati ir nonākuši pie iecerētā datu saņēmēja;

2.4. "*SOAP*" saskaņā ar Globālā tīmekļa konsorcija standartiem ir ziņojumapmaiņas protokola specifikācija apmaiņai ar strukturētu informāciju tīmekļa pakalpojumu ieviešanā datortīklos;

2.5. "esošā stāvokļa pārnese" ("*REST*") ir arhitektūras stils tīklā savienotu lietojumprogrammu izstrādei, balstoties uz tādu klienta–servera saziņas modeli, kurš nesatur informāciju par iepriekšējo stāvokli, un izmantojot standarta metodes, lai veiktu darbības ar resursiem, kas parasti ir attēloti strukturētos formātos;

2.6. "tīmekļa pakalpojums" ir programmatūras sistēma, kura paredzēta, lai atbalstītu sadarbspējīgu iekārtu sazināšanos tīklā, un kurai ir saskarne, kas aprakstīta mašīnapstrādājamā formātā;

2.7. "datu apmaiņa" ir ziņojumu, veidlapu, dokumentu un e-pierādījumu apmaiņa decentralizētajā IT sistēmā;

2.8. "*API*" ir lietojumprogrammas saskarne, kuras pamatā ir kopējs datu apmaiņas standarts un kura ļauj pakalpojumu sniedzējiem, kas izmanto pielāgotus IT risinājumus, lai apmainītos ar informāciju un datiem, kuri saistīti ar e-pierādījumu pieprasījumiem, ar automatizētiem līdzekļiem piekļūt decentralizētajām IT sistēmām;

2.9. "tīmekļa saskarne" ir lietotāja saskarne, kas ir pieejama internetā, izmantojot *HTTPS*, un kas ļauj pakalpojumu sniedzējiem manuāli piekļūt decentralizētajai IT sistēmai, lai droši sazinātos ar iestādēm un apmainītos ar informāciju un datiem, kas saistīti ar e-pierādījumu pieprasījumiem, bez nepieciešamības veidot savu īpašu infrastruktūru;

2.10. "ETSI standarti" ir tehniskās specifikācijas un standarti, ko izstrādājis Eiropas telesakaru standartu institūts (ETSI), lai nodrošinātu informācijas un komunikācijas tehnoloģiju sadarbspēju, drošību un efektivitāti. Tie nodrošina satvarus, protokolus un paraugpraksi plašam tehnoloģiju klāstam, tostarp mobilajiem tīkliem, radiosakariem, kiberdrošībai un interneta infrastruktūrai;

2.11. "jaucējkods" ir fiksēta garuma izvade, ko rada kriptogrāfiskā jaucējfunkcija, kad to piemēro patvaļīga garuma ievadei. Kriptogrāfiskā jaucējfunkcija ir veidota tā, lai nodrošinātu drošības pamatpazīmes, tostarp izturību pret inversiju, otru izturību pret inversiju un izturību pret kolīzijām, garantējot tās noturību pret inversijas un kolīzijas uzbrukumiem;

2.12. "*e-CODEX* sistēma" ir sistēma, kas minēta Regulas (ES) 2022/850 3. panta 1. punktā;

2.13. "ES e-tiesiskuma pamatleksikas" ir ES e-tiesiskuma pamatleksikas, kā definēts Regulas (ES) 2022/850 pielikuma 4. punktā;

2.14. "*ebMS*" ir *ebXML* ziņojumu pakalpojums, proti, ziņojumapmaiņas protokols, kurš izstrādāts saskaņā ar *OASIS* sistēmu un nodrošina elektronisko uzņēmējdarbības dokumentu drošu, uzticamu un sadarbspējīgu apmaiņu, izmantojot *SOAP*, un atbalsta uzņēmumu savstarpējo integrāciju dažādās sistēmās;

2.15. "*AS4*" ir paziņojums par piemērojamību Nr. 4, *OASIS* standarts, kas apraksta *ebMS* 3.0; tas vienkāršo drošu un sadarbspējīgu ziņojumapmaiņu starp uzņēmumiem, izmantojot atvērtus standartus, piemēram, *SOAP* un *WS-Security*;

2.16. "atjaunošanas laika mērķis" ir maksimālais pieņemamais laiks pakalpojuma atjaunošanai pēc incidenta;

2.17. "atjaunošanas punkta mērķis" ir datu zaudējuma maksimālais pieļaujamais apjoms atteices gadījumā.

3. **Saziņas metodes ar elektronisko līdzekļu starpniecību**

3.1. Rakstiskas saziņas nolūkā starp dalībvalstu kompetentajām iestādēm, starp kompetentajām iestādēm un pakalpojumu sniedzēju izraudzītajiem iedibinājumiem vai pakalpojumu sniedzēju juridiskajiem pārstāvjiem, kā arī starp kompetentajām iestādēm un Savienības aģentūrām vai struktūrām decentralizētā IT sistēma datu apmaiņas nolūkos izmanto uz pakalpojumiem balstītas saziņas metodes, piemēram, tīmekļa pakalpojumus vai citus atkalizmantojamus komponentus un programmatūras risinājumus. Konkrētāk, tas ietver saziņu, izmantojot *e-CODEX* piekļuves punktus, kā noteikts Regulas (ES) 2022/850 5. panta 2. punktā. Tādēļ, lai nodrošinātu efektīvu un sadarbspējīgu pārrobežu datu apmaiņu, decentralizētā IT sistēma atbalsta saziņu, izmantojot *e-CODEX* sistēmu.

3.2. Ņemot vērā to paredzamo lielo e-pierādījumu apjomu, kas pēc Eiropas e-pierādījumu sniegšanas rīkojuma nosūtāmi, izmantojot decentralizēto IT sistēmu, – kā izklāstīts Regulas (ES) 2023/1543 19. panta 1. un 4. punktā, – kā rezultātā var rasties tehnisko spēju ierobežojumi, kuri varētu negatīvi ietekmēt decentralizēto IT sistēmu, e-pierādījumus nosūta, izmantojot šo sistēmu, ciktāl tie nepārsniedz 25 megabaitu (25 600 kilobaitu) robežvērtību. To e-pierādījumu nosūtīšanu, kas pārsniedz minēto robežvērtību, veic saskaņā ar minētās regulas 19. panta 5. punktu.

3.3. Ņemot vērā Regulas (ES) 2023/1543 19. panta 6. punktu, ja nosūtīšanu veic, izmantojot minētajā punktā paredzētos alternatīvos līdzekļus, jo nav iespējams izmantot decentralizēto IT sistēmu kāda no minētās regulas 19. panta 5. punktā izklāstītajiem iemesliem dēļ:

3.3.1. Ja nosūtīšana attiecas uz rakstisku saziņu, tostarp veidlapu apmaiņu, starp kompetentajām iestādēm un pakalpojumu sniedzējiem Regulas (ES) 2023/1543 19. panta 1. punkta nozīmē, nosūtīšanas iniciators reģistrē nosūtīšanu savā valsts IT sistēmā, kas ir decentralizētās IT sistēmas daļa. Reģistrētā informācija ietver vismaz lietas vai datnes atsauces numuru, tās datumu un laiku, sūtītāju un saņēmēju, datnes nosaukumu un tās lielumu.

3.3.2. Ja nosūtīšana attiecas uz rakstisku saziņu, tostarp veidlapu apmaiņu, starp kompetentajām iestādēm, kā arī rakstisku saziņu ar kompetentajām Savienības aģentūrām vai struktūrām Regulas (ES) 2023/1543 19. panta 4. punkta nozīmē, nosūtīšanas iniciators reģistrē nosūtīšanu decentralizētajā IT sistēmā, jo īpaši savā valsts IT sistēmā vai attiecīgā gadījumā IT sistēmās, ko pārvalda kompetentā Savienības aģentūra vai struktūra. Reģistrētā informācija ietver vismaz lietas vai datnes atsauces numuru, nosūtīšanas datumu un laiku, sūtītāju un saņēmēju, datnes nosaukumu un tās lielumu.

3.3.3. Ja e-pierādījumi saskaņā ar Eiropas e-pierādījumu sniegšanas rīkojumu ir nosūtīti, izmantojot alternatīvus saziņas līdzekļus, starp pakalpojumu sniedzējiem un izdevējvalsts kompetentajām iestādēm ([1]), vai ja izpildes iestāde e-pierādījumus, izmantojot alternatīvus līdzekļus, nosūta izdevējvalsts kompetentajām iestādēm saskaņā ar izpildes procedūru, kas paredzēta Regulas (ES) 2023/1543 16. panta 9. punktā, iniciators:

a) reģistrē un nosūta iestādei, kurai e-pierādījumi ir nosūtīti vai darīti pieejami, manifestu, kurā ietver šādu informāciju:

1) informācija par nosūtītāju un saņēmēju;

2) metadati, kas sniegtos e-pierādījumus saista ar konkrētu(-iem) Eiropas e-pierādījumu sniegšanas vai saglabāšanas rīkojumu(-iem);

3) nosūtīšanas datums un laiks vai norāde, kad e-pierādījumi tika darīti pieejami saņēmējam;

4) informācija par nosūtīšanas līdzekļiem (piemēram, ieraksts par drošu saiti, ar kuras starpniecību e-pierādījumi tika darīti pieejami, saņemšanas vai piegādes apliecinājums no pasta operatoriem utt. ([2]));

5) to e-pierādījumu pilns(-i) datnes(-ņu) nosaukums(-i), kas nosūtīti vai citādi darīti pieejami iecerētajam saņēmējam izdevējvalstī;

6) to e-pierādījumu datu apjoms, kas nosūtīti vai citādi darīti pieejami iecerētajam saņēmējam izdevējvalstī;

7) vismaz viens to datu jaucējkods, kas tika nosūtīti vai darīti pieejami, un norāde par izmantoto(-ajiem) jaucējalgoritmu(-iem). Jaucējalgoritms(-i), ko izmanto šā(-o) jaucējkoda(-u) aprēķināšanai, ir kriptogrāfiski spēcīgs(-i) vispārlietojams(-i) algoritms(-i), uz ko neattiecas tādas publiski atklātas nepilnības kā kolīzijas (piemēram, *SHA-512*, *SHA3-512*, *BLAKE2* vai *RIPEMD-160*, bet, iespējams, spēcīgākas, atkarībā no tehnoloģiju attīstības);

b) attiecīgā gadījumā a) apakšpunktā minētajā manifestā norāda datumu un laiku, līdz kuram e-pierādījumi būs pieejami. Šis laikposms izdevējvalsts kompetentajai iestādei nodrošina saprātīgu termiņu e-pierādījumu izgūšanai, kas nav īsāks par 10 kalendārajām dienām un nav garāks par 45 kalendārajām dienām no brīža, kad e-pierādījumi ir darīti pieejami. Pēc izdevējvalsts kompetentās iestādes lūguma iniciatora norādīto termiņu atsevišķos gadījumos var pagarināt;

c) var reģistrēt a) apakšpunktā minētajā manifestā jebkādu papildu informāciju vai piezīmes, kas attiecas uz lietu, un nosūtīt iestādei, kurai e-pierādījumi ir nosūtīti vai darīti pieejami.

3.4. Ņemot vērā Regulas (ES) 2023/1543 28. pantu, references īstenošanas programmatūra programmatiski vāc, nosūta vai citādi nodrošina piekļuvi minētā panta 2. punktā minētajai statistikai gan strukturētos (piemēram, *XML*), gan nestrukturētos (piemēram, *PDF*) datu formātos. Dalībvalstu pārvaldītie valstu portāli ([3]), ja tie ir tehniski tā izstrādāti, saskaņā ar Regulas (ES) 2023/1543 28. panta 3. punktu var arī nosūtīt vai sniegt šos statistikas datus Komisijai automatizētā procesā. Komisija izdod norādījumus par datu struktūru un šīs statistikas vākšanas un paziņošanas metodi.

([1]) Skaidrības labad atsauces uz kompetentajām valsts iestādēm *mutatis mutandis* saprot arī kā atsauces uz *Eurojust* valsts pārstāvjiem, Eiropas prokuroriem un Eiropas deleģētajiem prokuroriem, ciktāl tie ir pilnvaroti veikt tās pašas funkcijas saskaņā ar ES tiesību aktiem un valstu tiesību aktiem.

([2]) Jāņem vērā, ka saskaņā ar 19. panta 5. punktu nosūtīšana, izmantojot šādus alternatīvus saziņas līdzekļus, atbilst ātras, drošas un uzticamas nosūtīšanas prasībām un ļauj saņēmējam noteikt autentiskumu.

([3]) "Valstu portāli" būtu jāsaprot kā valstu "IT sistēmas", kas ir daļa no decentralizētās IT sistēmas, kura definēta Regulas (ES) 2023/1543 3. panta 21. punktā.

4. **Saziņas protokoli**

4.1. Decentralizētā IT sistēma izmanto drošus interneta protokolus:

a) saziņai decentralizētajā IT sistēmā starp kompetentajām iestādēm;

b) saziņai decentralizētajā IT sistēmā starp kompetentajām iestādēm un Savienības aģentūrām un struktūrām;

c) saziņai starp kompetentajām iestādēm un pakalpojumu sniedzējiem, izmantojot *API* un tīmekļa saskarni; un

d) saziņai ar Tiesu datubāzi.

4.2. Attiecībā uz strukturētu datu un metadatu definēšanu un nosūtīšanu decentralizētās IT sistēmas komponentu pamatā ir visaptveroši un plaši atzīti nozares standarti un protokoli, piemēram, *SOAP* un *REST*, jo īpaši tie, uz kuriem atsaucas Eiropas standartizācijas organizācijas, piemēram, ETSI.

4.3. Attiecībā uz transporta un ziņojumapmaiņas protokoliem decentralizētās IT sistēmas pamatā ir droši, standartos balstīti protokoli, piemēram:

a) *AS4* profils datu pārrobežu apmaiņai, nodrošinot drošu un uzticamu ziņojumapmaiņu ar šifrēšanu un nenoliedzamību;

b) saziņai paredzēti *HTTPS*/*RESTful API*, kas atbalsta *JSON* un *XML* formātus;

c) augstas uzticamības mijiedarbībai paredzēti *SOAP*, ietverot *WS-Security* autentifikācijai un šifrēšanai.

4.4. Netraucētas un sadarbspējīgas datu apmaiņas nolūkā decentralizētās IT sistēmas izmantotie saziņas protokoli atbilst attiecīgajiem sadarbspējas standartiem.

4.5. Attiecīgā gadījumā e-pierādījumu *XML* shēmās izmanto attiecīgus standartus vai leksikas, kas vajadzīgi, lai pienācīgi validētu šajā shēmā definētos elementus un veidus. Tie var būt:

a) ES e-tiesiskuma pamatleksika;

b) nekvalificēti datu veidi;

c) kodu saraksts Eiropas Savienības valodu kodiem.

Attiecīgā gadījumā arī *XML* shēmās var iekļaut attiecīgos ETSI standartus, lai izmantotu to definīcijas.

4.6. Komisija nosaka kopējās *API* specifikācijas, ko izpildes valstis dara pieejamas pakalpojumu sniedzējiem kā līdzekli, lai piekļūtu decentralizētajai IT sistēmai. Iespējamā un saprātīgā apmērā šīs *API* pamatā ir ETSI TS 104 144 ("Saskarnes definīcija Regulai (ES) 2023/1543 (E-pierādījumu regula) valstu iestādēm un pakalpojumu sniedzējiem").

4.7. Attiecībā uz drošības un autentifikācijas protokoliem decentralizētās IT sistēmas pamatā ir standartos balstīti protokoli, piemēram:

a) *TLS* (transporta slāņa drošība) šifrētai un autentificētai saziņai tīklos, atbalstot savstarpēju autentifikāciju ar *X.509* digitālajiem sertifikātiem;

b) *OAuth* | *OpenID Connect* (*OIDC*) drošai autentifikācijai un autorizēšanai;

c) Publiskās atslēgas infrastruktūra un digitālie paraksti drošai atslēgu apmaiņas un ziņojumu integritātes verifikācijai, izmantojot digitālos sertifikātus (*X.509*), ko izdevušas uzticamas sertifikācijas iestādes (SI).

5. **Informācijas drošības mērķi un attiecīgie tehniskie pasākumi**

5.1. Tehniskajos pasākumos, ar ko nodrošina informācijas tehnoloģijas drošības minimālos standartus informācijas apmaiņai decentralizētajā IT sistēmā, ietilpst:

a) pasākumi, kas nodrošina informācijas konfidencialitāti, ieskaitot drošu saziņas kanālu izmantošanu;

b) pasākumi, kas nodrošina datu (ziņojumu, veidlapu, dokumentu un e-pierādījumu), kas atrodas glabāšanā, un datu, kas tiek pārvietoti, integritāti;

c) pasākumi, kas decentralizētajā IT sistēmā nodrošina informācijas nosūtītāja izcelsmes nenoliedzamību un informācijas saņemšanas nenoliedzamību;

d) pasākumi, kas nodrošina pieejamību, nodrošinot nepārtrauktu piekļuvi pakalpojumiem un datiem un novēršot traucējumus kiberuzbrukumu vai atteices dēļ;

e) pasākumi, kas nodrošina drošības notikumu reģistrēšanu saskaņā ar atzītiem starptautiskiem ieteikumiem par informācijas tehnoloģijas drošības standartiem;

f) pasākumi, kas nodrošina lietotāju autentifikāciju un autorizāciju, un pasākumi, kas nodrošina to sistēmu identitātes pārbaudi, kuras ir savienotas ar decentralizēto IT sistēmu.

5.2. Decentralizētās IT sistēmas komponenti nodrošina drošu saziņu un datu nosūtīšanu, izmantojot šifrēšanu, publiskās atslēgas infrastruktūru ar digitāliem sertifikātiem autentifikācijai un drošai atslēgu apmaiņai, un drošus ziņojumapmaiņas protokolus, piemēram, *AS4* (*ebMS*), *RESTful API* un *SOAP*, lai saglabātu ziņojumu konfidencialitāti un integritāti.

5.3. Decentralizētās IT sistēmas komponentus izstrādā saskaņā ar integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principu, un īsteno atbilstīgus administratīvus, organizatoriskus un tehniskus pasākumus, lai nodrošinātu augstu kiberdrošības līmeni.

5.4. Komisija izstrādā, attīsta un uztur references īstenošanas programmatūru saskaņā ar datu aizsardzības prasībām un principiem, kas noteikti Regulā (ES) 2018/1725. Komisijas nodrošinātā references īstenošanas programmatūra ļauj dalībvalstīm izpildīt savus pienākumus attiecīgi saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([4]) un Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680 ([5]).

5.5. Dalībvalstis, kuras izmanto citu valsts IT sistēmu, kas nav references īstenošanas programmatūra, īsteno vajadzīgos pasākumus, lai nodrošinātu, ka tā atbilst attiecīgi Regulas (ES) 2016/679 un Direktīvas (ES) 2016/680 prasībām.

5.6. *Eurojust* un Eiropas Prokuratūra, ņemot vērā to dalību decentralizētajā IT sistēmā, īsteno vajadzīgos pasākumus, lai nodrošinātu, ka to attiecīgās IT sistēmas atbilst Regulas (ES) 2018/1725 un to dibināšanas aktu prasībām.

5.7. Dalībvalstis, *Eurojust* un Eiropas Prokuratūra izveido stabilus mehānismus draudu atklāšanai un reaģēšanai uz incidentiem, lai nodrošinātu drošības incidentu savlaicīgu identificēšanu, mazināšanu un atkopšanos no tiem saskaņā ar to attiecīgo politiku attiecībā uz to atbildībā esošajām IT sistēmām, kas ir daļa no decentralizētās IT sistēmas.

6. **E-pierādījumu** ([6]) **šifrēšana**

6.1. Neskarot decentralizētās IT sistēmas nodrošinātos drošības pasākumus, kompetentās iestādes, izdodot Eiropas e-pierādījumu sniegšanas rīkojumu, papildus var sniegt īpašu publisku *X.509* sertifikātu e-pierādījumu asimetriskai šifrēšanai.

([4]) 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.).

([5]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89. lpp.).

([6]) Lai novērstu šaubas, termins "e-pierādījumi" attiecas tikai uz definīciju, kas sniegta Regulas (ES) 2023/1543 3. panta 8. punktā.

6.2. Par 6.1. punktā minēto sertifikātu izdošanu, pārvaldību, verifikāciju un visiem saistītajiem aspektiem, kā arī par attiecīgo publiskās atslēgas infrastruktūru ir atbildīga vienīgi izdevējvalsts.

6.3. Neskarot turpmāko tehnoloģiju attīstību, publiskie sertifikāti atbalsta nozares standarta šifrēšanas algoritmus, piemēram, *RSA* (*Rivest-Shamir-Adleman*) vai *ECDH* (eliptiskā līkne *Diffie-Hellman*) attiecībā uz *ECC* (eliptiskās līknes kriptogrāfiju).

6.4. Publiskajos sertifikātos iekļauj atbilstīgu "keyUsage" paplašinājumu, piemēram, "keyEncipherment" vai "dataEncipherment" *RSA* sertifikātiem un "keyAgreement" *ECC* sertifikātiem. Sertifikātus dara pieejamus *PEM* ((*Privacy-Enhanced Mail*) uzlabota privātuma e-pasts) vai *DER* ((*Distinguished Encoding Rules*) atšķirīgi kodēšanas noteikumi) formātā.

6.5. Ja izdevējiestāde ir sniegusi publisku *X.509* sertifikātu un ja pakalpojumu sniedzējs nosūta e-pierādījumus saskaņā ar Eiropas e-pierādījumu sniegšanas rīkojumu, pirms minēto datu nosūtīšanas decentralizētajā IT sistēmā pakalpojumu sniedzējs šifrē e-pierādījumus, izmantojot attiecīgo izdevējvalsts sniegto publisko *X.509* sertifikātu.

6.6. Ja izdevējiestāde ir sniegusi publisku *X.509* sertifikātu, bet e-pierādījumu nosūtīšana šifrētā veidā nav iespējama tehnisku vai citu pamatotu iemeslu dēļ un neskarot Regulas (ES) 2023/1543 19. panta 5. punkta noteikumu, pakalpojumu sniedzējs var nosūtīt datus, nešifrējot saturu. Šādos gadījumos pakalpojumu sniedzējs sniedz pamatotu paskaidrojumu izdevējiestādei.

7. **Minimālie pieejamības mērķi**

7.1. Dalībvalstis, *Eurojust* un Eiropas Prokuratūra nodrošina to atbildībā esošās decentralizētās IT sistēmas komponentu pieejamību 24 stundas diennaktī 7 dienas nedēļā ar mērķi gadā nodrošināt tehniskās pieejamības līmeni vismaz 98 % apmērā, izņemot plānoto uzturēšanu.

7.2. Komisija nodrošina Tiesu datubāzes pieejamību 24 stundas diennaktī 7 dienas nedēļā ar mērķi gadā nodrošināt tehniskās pieejamības līmeni vairāk nekā 99 % apmērā, izņemot plānoto uzturēšanu.

7.3. Iespēju robežās uzturēšanas darbības plāno darba dienās laikā no plkst. 20.00 līdz 7.00 pēc Viduseiropas laika.

7.4. Dalībvalstis, *Eurojust* un Eiropas Prokuratūra paziņo Komisijai un pārējām dalībvalstīm par uzturēšanas darbībām šādi:

a) 5 darbdienas pirms uzturēšanas darbībām, kas var izraisīt pakalpojumu nepieejamību līdz 4 stundām;

b) 10 darbdienas pirms uzturēšanas darbībām, kas var izraisīt pakalpojumu nepieejamību 4 līdz 12 stundas;

c) 30 darbdienas pirms uzturēšanas darbībām, kas var izraisīt pakalpojumu nepieejamību vairāk nekā 12 stundas.

7.5. Ja dalībvalstis, *Eurojust* vai Eiropas Prokuratūra ir noteikušas regulārus uzturēšanas periodus, tās informē Komisiju un decentralizētās IT sistēmas dalībniekus par laiku un dienu(-ām), kad šādi noteiktie regulārie periodi ir plānoti. Neatkarīgi no 7.4. punktā izklāstītajiem pienākumiem, ja dalībvalstu, *Eurojust* vai Eiropas Prokuratūras atbildībā esošās decentralizētās IT sistēmas komponenti kļūst nepieejami šāda noteiktā regulārā perioda laikā, tās var izvēlēties par to nepaziņot Komisijai katru reizi.

7.6. Dalībvalstu, *Eurojust* vai Eiropas Prokuratūras atbildībā esošo decentralizētās IT sistēmas komponentu negaidītas tehniskas atteices gadījumā tās nekavējoties informē Komisiju un decentralizētās IT sistēmas dalībniekus par šo atteici un, ja tas ir zināms, par prognozējamo atjaunošanas termiņu.

7.7. Ja decentralizētās IT sistēmas komponentos, par kuriem ir atbildīga dalībvalsts, tiek veiktas uzturēšanas darbības vai rodas negaidīta komponentu tehniska atteice, kas negatīvi ietekmē *API* un/vai tīmekļa saskarnes pieejamību pakalpojumu sniedzējiem, attiecīgā dalībvalsts nekavējoties dara šo informāciju pieejamu tīmekļa vietnē un/vai bez liekas kavēšanās paziņo to pakalpojumu sniedzējiem, kas darbojas tās teritorijā.

7.8. Tiesu datubāzes negaidītas tehniskas atteices gadījumā Komisija nekavējoties informē dalībvalstis, *Eurojust* un Eiropas Prokuratūru par datubāzes nepieejamību un, ja tas ir zināms, par prognozējamo atjaunošanas termiņu.

7.9. Pakalpojumu sniegšanas traucējumu gadījumā dalībvalstis, *Eurojust* un Eiropas Prokuratūra saskaņā ar atjaunošanas laika mērķi un atjaunošanas punkta mērķi nodrošina, lai pakalpojums tiktu ātri atjaunots un datu zaudējums būtu minimāls.

7.10. Dalībvalstis, *Eurojust* un Eiropas Prokuratūra īsteno atbilstīgus pasākumus, lai sasniegtu iepriekš minētos pieejamības mērķus, un izstrādā procedūras efektīvai reaģēšanai uz incidentiem.

8. **Kompetento iestāžu/Tiesu datubāze (*CDB*)**

8.1. Ņemot vērā Regulas (ES) 2023/1543 19. pantu, decentralizētās IT sistēmas darbības nolūkā ir būtiski izveidot uzticamu datubāzi par pakalpojumu sniedzējiem un kompetentajām iestādēm.

8.2. Kompetento iestāžu uzticamajā datubāzē strukturētā formātā iekļauj šādu informāciju:

a) Regulas (ES) 2023/1543 19. panta vajadzībām – informāciju par kompetentajām iestādēm, kas paziņotas saskaņā ar tās 31. panta 1. punkta a)–c) apakšpunktu, tostarp:

1) *Eurojust* valsts pārstāvjiem, kopā ar norādi par to, vai tie saskaņā ar valsts tiesību aktiem ir pilnvaroti izdot Eiropas e-pierādījumu sniegšanas un Eiropas e-pierādījumu saglabāšanas rīkojumus Eiropas Parlamenta un Padomes Regulas (ES) 2018/1727 ([7]) 8. panta 3. un 4. punkta nozīmē;

2) Eiropas deleģētajiem prokuroriem un Eiropas prokuroriem, ja dalībvalstis par tiem paziņojušas saskaņā ar Padomes Regulas (ES) 2017/1939 ([8]) 105. panta 3. punktu kā kompetento izdevējiestādi Regulas (ES) 2023/1543 nozīmē;

b) attiecīgā gadījumā informāciju, kas vajadzīga, lai noteiktu iestāžu kompetences ģeogrāfiskos apgabalus, vai citus attiecīgus kritērijus, kas vajadzīgi to kompetences noteikšanai;

c) informāciju, kas vajadzīga datu apmaiņas pareizai darbībai un tehniskai ziņojumu maršrutēšanai decentralizētajā IT sistēmā.

8.2.1. Informācijā, kas minēta 8.2. punkta c) apakšpunktā, ietilpst:

a) informācija par dalībvalsti, kurā pakalpojumu sniedzēja izraudzītais iedibinājums ir iedibināts vai kurā rezidē tā juridiskais pārstāvis:

1) dalībvalsts;

2) centrālā iestāde;

([7]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1727 (2018. gada 14. novembris) par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (*Eurojust*) un ar ko aizstāj un atceļ Padomes Lēmumu 2002/187/TI (OV L 295, 21.11.2018., 138. lpp.).

([8]) Padomes Regula (ES) 2017/1939 (2017. gada 12. oktobris), ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (*EPPO*) izveidei (OV L 283, 31.10.2017., 1. lpp.).

b) informācija par pakalpojumu sniedzēju:

1) nosaukums;

2) adrese/juridiskā adrese;

3) reģistrācijas numurs;

4) tiesiskā forma;

5) tālruņa numurs;

6) e-pasts;

c) informācija par izraudzīto iedibinājumu / juridisko pārstāvi:

1) tiesību subjekta veids (izraudzītais iedibinājums / juridiskais pārstāvis);

2) nosaukums;

3) adrese/juridiskā adrese;

4) tālruņa numurs;

5) e-pasts;

6) galvenā kontaktpersona/struktūra;

7) oficiālā(-ās) valoda(-as), ko akceptējis pakalpojumu sniedzējs / izraudzītais iedibinājums / juridiskais pārstāvis;

8) pakalpojumi, kas minēti Eiropas Parlamenta un Padomes Direktīvas (ES) 2023/1544 ([9]) 2. panta 1) punktā un tiek piedāvāti Savienībā;

9) to ES juridisko instrumentu veids, attiecībā uz kuriem ir izraudzīts izraudzītais iedibinājums / juridiskais pārstāvis (gadījumos, kad dalībvalstis nepiedalās visos attiecīgajos ES juridiskajos instrumentos);

10) izraudzīšanās/iecelšanas teritoriālā darbības joma;

d) informācijas autentifikācija:

1) pilnvarotā pārstāvja vārds/uzvārds;

2) amata nosaukums;

3) adrese;

4) tālruņa numurs;

5) e-pasts;

6) datums.

8.2.2. Ja pieejama, 8.2. punkta c) apakšpunktā minētajā informācijā var ietilpt:

a) informācija par pakalpojumu sniedzēju:

1) kontaktpersona jautājumiem par paziņojumiem (ja tā nav parakstītājs);

2) tīmekļa vietne;

b) pieejamo datu veidi:

1) par katru attiecīgo pakalpojumu:

— pieejamo datu veidi,

— datu kategorija,

— identifikatori,

— datu pieejamības periods;

([9]) Eiropas Parlamenta un Padomes Direktīva (ES) 2023/1544 (2023. gada 12. jūlijs), ar ko paredz saskaņotus noteikumus par izraudzīto iedibinājumu izraudzīšanos un juridisko pārstāvju iecelšanu elektronisko pierādījumu vākšanai kriminālprocesā (OV L 191, 28.7.2023., 181. lpp., ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) papildu informācija par datiem;

3) papildu informācija par pakalpojumu (piemēram, apakšuzņēmēju līgumattiecības);

c) informācija par izraudzīto iedibinājumu / juridisko pārstāvi:

1) citi pakalpojumu sniedzēji, kuriem izraudzītais iedibinājums vai juridiskais pārstāvis ir izraudzīts;

2) tehniskās palīdzības kontaktinformācija;

3) kontaktpersona ārkārtas situācijās;

d) tehniskā informācija:

1) tehniskā kontaktpunkta kontaktpersonas vārds, uzvārds / nosaukums;

2) tehniskā kontaktpunkta tālruņa numurs;

3) tehniskā kontaktpunkta e-pasts;

4) *API URL* dinamiskai informācijas izgūšanai par datu veidiem;

5) savienojuma veids ar valsts IT sistēmu:

— tīmekļa saskarne,

— API,

— *Push API URL*.

8.3. Ņemot vērā decentralizētās IT sistēmas operatīvās vajadzības:

a) Komisija ir atbildīga par uzticamās datubāzes izstrādi, uzturēšanu, darbību un atbalstu;

b) Komisija piekļuvi uzticamajai datubāzei dara iespējamu, izmantojot *API*, kas darīta pieejama kompetentajām iestādēm, *Eurojust* un Eiropas Prokuratūrai, lai tās varētu piedalīties decentralizētajā IT sistēmā;

c) dalībvalstis nodrošina, ka 8.2. punkta a) un b) apakšpunktā paredzētā informācija par to kompetentajām iestādēm uzticamajā datubāzē ir pilnīga, precīza un atjaunināta;

d) uzticamā datubāze ļauj dalībvalstīm sniegt un atjaunināt informāciju par saviem pakalpojumu sniedzējiem tajā un iestādēm, kas piedalās decentralizētajā IT sistēmā, programmatiski piekļūt minētajai informācijai un to izgūt;

e) dalībvalstis un pakalpojumu sniedzēji nodrošina, ka 8.2. punkta c) apakšpunktā paredzētā informācija uzticamajā datubāzē ir pilnīga, precīza un atjaunināta.