Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/2447

5.12.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/2447

(2025. gada 4. decembris),

ar ko nosaka Eiropas Parlamenta un Padomes Regulas (ES) 2018/1727 piemērošanas noteikumus attiecībā uz tehniskajām specifikācijām, pasākumiem un citām prasībām par decentralizētās IT sistēmas informācijas drošai apstrādei un paziņošanai izveidi un izmantošanu

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (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 ([1]), un jo īpaši tās 22.a panta 3. punktu un 22.b panta 1. punkta a), b), c) un d) apakšpunktu,

tā kā:

(1) Regulā (ES) 2018/1727 ir izklāstīts satvars *Eurojust* jaunajai digitālajai iekšējai infrastruktūrai un decentralizētas drošas digitālās saziņas sistēmas izveidei starp dalībvalstu kompetentajām valsts iestādēm un *Eurojust*.

(2) Droša digitālā saziņa jāveic, izmantojot decentralizēto IT sistēmu. Lai izveidotu decentralizēto IT sistēmu, ir jānosaka tehniskās specifikācijas, ar kurām nosaka saziņas metodes un saziņas protokolus, tehniskos pasākumus, kas nodrošina minimālos informācijas drošības standartus un drošību, kā arī minimālos pieejamības mērķus minētās sistēmas īstenošanai.

(3) Decentralizētajā IT sistēmā saskaņā ar Regulas (ES) 2018/1727 22.a panta 1. punktu ir jāiekļauj dalībvalstu un *Eurojust* IT sistēmas, kā arī sadarbspējīgi *e-CODEX* piekļuves punkti, ar kuru starpniecību šīs IT sistēmas ir savstarpēji savienotas. Minētajā regulā noteiktajās decentralizētās IT sistēmas tehniskajās specifikācijās un citās prasībās būtu jāņem vērā minētais satvars.

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

(5) Minētā decentralizētā IT sistēma tiek īstenota plašākā, uz *e-CODEX* balstītā decentralizētā IT sistēmā, ko dēvē par Tiesiskuma digitālās apmaiņas sistēmu (*JUDEX*). Tādēļ ir jānodrošina efektīva informācijas apmaiņa par horizontālajām norisēm.

(6) Saskaņā ar Regulas (ES) 2018/1727 22.a panta 4. punktu dalībvalstis un *Eurojust* var izvēlēties valsts IT sistēmas vietā izmantot Komisijas izstrādāto references īstenošanas programmatūru kā savu aizmugursistēmu. Lai nodrošinātu sadarbspēju, gan uz valsts IT sistēmām, gan references īstenošanas programmatūru būtu jāattiecina vienas un tās pašas tehniskās specifikācijas un prasības.

(7) Dati par teroristu nodarījumiem un smagu organizēto noziedzību būtu jānosūta strukturētā veidā, lai uzlabotu informācijas kvalitāti un atbilstību, kā arī lai nodrošinātu, ka informāciju var efektīvāk integrēt *Eurojust* lietu pārvaldības sistēmā un labāk salīdzināt ar informāciju, kas jau tiek glabāta minētajā sistēmā. Attiecībā uz daktiloskopiskajiem datiem un fotogrāfijām, ko var nosūtīt *Eurojust*, lai identificētu personas, uz kurām attiecas kriminālprocess saistībā ar terorisma nodarījumiem, būtu jānosaka pārsūtīšanas formāts un tehniskie standarti.

([1]) OV L 295, 21.11.2018., 138. lpp., ELI: http://data.europa.eu/eli/reg/2018/1727/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).

(8) *Eurojust* veicina un atbalsta tiesiskās sadarbības lūgumu izdošanu un izpildi, tostarp tādu lūgumu un lēmumu izpildi, kas balstīti uz instrumentiem, ar kuriem īsteno savstarpējas atzīšanas principu. Valstu kompetentajām iestādēm vajadzētu būt iespējai lūgt *Eurojust* palīdzību un koordināciju, izmantojot decentralizēto IT sistēmu.

(9) Lai nodrošinātu efektivitāti un konsekvenci, ir svarīgi, lai tehniskās specifikācijas, kas jānosaka saskaņā ar Regulu (ES) 2018/1727, būtu saderīgas ar tehniskajām specifikācijām, kuras noteiktas ar Eiropas Parlamenta un Padomes Regulām (ES) 2023/2844 ([3]), (ES) 2023/1543 ([4]) un (ES) 2024/3011 ([5]), kā arī ar turpmākiem digitalizācijas pasākumiem, kas attiecas uz *Eurojust* pilnvarām atbalstīt valstu kompetentās iestādes.

(10) Izmantojot decentralizēto IT sistēmu, būtu jānodrošina arī jebkāda cita saziņa starp *Eurojust* un kompetentajām valsts iestādēm, piemēram, informācijas paziņošana par informācijas apstrādes rezultātiem, tostarp saikne ar lietām, kas jau tiek glabātas lietu pārvaldības sistēmā saskaņā ar Regulas (ES) 2018/1727 22. pantu, ja *Eurojust* rīkojas pēc savas iniciatīvas, vai informācija, kas nosūtīta *Eurojust*, lai saglabātu, analizētu un glabātu pierādījumus, kas saistīti ar genocīdu, noziegumiem pret cilvēci, kara noziegumiem un saistītiem noziedzīgiem nodarījumiem saskaņā ar minētās regulas 4. panta 1. punkta j) apakšpunktu.

(11) Lai nodrošinātu, ka minētajā regulā ir ņemtas vērā *Eurojust* operatīvās vajadzības, ir notikusi apspriešanās ar *Eurojust* saskaņā ar Regulas (ES) 2018/1727 22.a panta 3. punktu.

(12) Saskaņā ar 4. pantu Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, Īrija 2019. gada 9. septembra vēstulē ir paziņojusi, ka vēlas piedalīties Regulas (ES) 2018/1727 pieņemšanā un piemērošanā. Komisijas Lēmums (ES) 2019/2006 ([6]) apstiprināja šādu dalību. Ar Eiropas Parlamenta un Padomes Regulu (ES) 2023/2131 ([7]) tika grozīta Regula (ES) 2018/1727, lai varētu izveidot drošus digitālās saziņas kanālus starp *Eurojust* un kompetentajām valstu iestādēm, un tas ir šīs regulas juridiskais pamats. Apstākļos, kad Īrija nav paziņojusi, ka vēlas piedalīties Regulas (ES) 2023/2131 pieņemšanā un piemērošanā, un nav paziņojusi, ka vēlas uzņemties saistības, kas izriet no minētās regulas, Īrijai saskaņā ar Protokola Nr. 21 1. un 2. pantu un 4.a panta 1. punktu Regula (ES) 2023/2131 nav saistoša un nav jāpiemēro. Līdz ar to Īrija nepiedalās šīs regulas pieņemšanā.

(13) Saskaņā ar 1. un 2. pantu Protokolā Nr. 22 par Dānijas nostāju, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, Dānija nepiedalījās Regulas (ES) 2018/1727 pieņemšanā. Tādēļ Dānijai šī regula nav saistoša un nav jāpiemēro.

([3]) Eiropas Parlamenta un Padomes Regula (ES) 2023/2844 (2023. gada 13. decembris) par tiesu iestāžu sadarbības un tiesu iestāžu pieejamības digitalizāciju pārrobežu civillietās, komerclietās un krimināllietās un ar ko groza dažus tiesību aktus tiesu iestāžu sadarbības jomā (OV L, 2023/2844, 27.12.2023., ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Eiropas Parlamenta un Padomes Regula (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 (OV L 191, 28.7.2023., 118. lpp., ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Eiropas Parlamenta un Padomes Regula (ES) 2024/3011 (2024. gada 27. novembris) par tiesvedības nodošanu krimināllietās (OV L, 2024/3011, 18.12.2024., ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Komisijas Lēmums (ES) 2019/2006 (2019. gada 29. novembris) par Īrijas dalību Eiropas Parlamenta un Padomes Regulas (ES) 2018/1727 par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (*Eurojust*) īstenošanā (OV L 310, 2.12.2019., 59. lpp., ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Eiropas Parlamenta un Padomes Regula (ES) 2023/2131 (2023. gada 4. oktobris), ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) 2018/1727 un Padomes Lēmumu 2005/671/TI attiecībā uz digitālu informācijas apmaiņu terorisma lietās (OV L, 2023/2131, 11.10.2023., ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([8]) 42. panta 1. punktu notika apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kurš 2025. gada 21. oktobrī ir sniedzis atzinumu.

(15) Šajā regulā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi ar Regulas (ES) 2018/1727 22.c pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Decentralizētās IT sistēmas tehniskās specifikācijas

Regulas (ES) 2018/1727 22.b panta 1. punkta a), b), c) un d) apakšpunktā minētās decentralizētās IT sistēmas tehniskās specifikācijas, pasākumi un mērķi ir noteikti šīs regulas I pielikumā.

2. pants

Digitālie procesuālie standarti

Digitālie procesuālie standarti, kas piemērojami elektroniskajai saziņai, izmantojot Regulas (ES) 2018/1727 22.a panta 3. punktā minēto decentralizēto IT sistēmu, ir noteikti šīs regulas II pielikumā.

3. pants

Pirkstu nospiedumu un fotogrāfiju pārsūtīšanas tehniskās specifikācijas

Pirkstu nospiedumu un fotogrāfiju pārsūtīšanas tehniskās specifikācijas un formāts, kas minēts Regulas (ES) 2018/1727 22.a panta 3. punktā, ir noteikts šīs regulas III pielikumā.

4. 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 4. decembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

([8]) 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).

I PIELIKUMS

DECENTRALIZĒTĀS IT SISTĒMAS TEHNISKĀS SPECIFIKĀCIJAS, PASĀKUMI UN MĒRĶI

1. **Ievads un darbības joma**

Šajā pielikumā ir noteiktas decentralizētās IT sistēmas tehniskās specifikācijas, pasākumi un mērķi attiecībā uz informācijas apmaiņu saskaņā ar Regulu (ES) 2018/1727.

IT sistēmas decentralizētais raksturs ļauj tieši un droši apmainīties ar datiem starp kompetentajām valsts iestādēm un *Eurojust*.

2. **Definīcijas**

Šajā pielikumā izmanto šādas 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. "vienkāršais objektpiekļuves protokols" (*Simple Object Access Protocol* jeb "*SOAP*") saskaņā ar Globālā tīmekļa konsorcija standartiem ir ziņojumapmaiņas protokola specifikācija apmaiņai ar strukturētu informāciju tīmekļa pakalpojumu ieviešanā datortīklos;

2.5. "REST" (esošā stāvokļa pārnese) 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 un dokumentu apmaiņa decentralizētajā IT sistēmā;

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

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

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

2.11. "*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*;

2.12. “atjaunošanas laika mērķis” ir maksimālais pieņemamais laiks pakalpojuma atjaunošanai pēc incidenta;

2.13. “atjaunošanas punkta mērķis” ir datu zaudējuma maksimālais pieļaujamais apjoms atteices gadījumā.

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

3.1. Decentralizētajā IT sistēmā būtu jāizmanto uz pakalpojumiem balstītas komunikācijas metodes, piemēram, tīmekļa pakalpojumi vai citi atkalizmantojami komponenti un programmatūras risinājumi ziņojumu un dokumentu apmaiņai.

3.2. Konkrētāk, decentralizētā IT sistēma ietver saziņu, izmantojot *e-CODEX* piekļuves punktus, kā noteikts Regulas (ES) 2022/850 5. panta 2. punktā. Tāpēc, lai nodrošinātu efektīvu un sadarbspējīgu pārrobežu datu apmaiņu, decentralizētā IT sistēma atbalsta saziņu, izmantojot *e-CODEX* sistēmu.

4. **Saziņas protokoli**

4.1. Decentralizētā IT sistēma izmanto drošus interneta protokolus:

a) saziņai decentralizētajā IT sistēmā starp kompetentajām iestādēm un *Eurojust*;

b) saziņai ar kompetento iestādi / tiesu datubāzi, kā minēts 7.1. punktā.

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*.

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 *XML* shēmās izmanto attiecīgus standartus vai leksikas, kas vajadzīgi, lai pienācīgi validētu šajā shēmā definētos elementus un veidus. Minētie standarti vai leksikas var ietvert:

a) ES e-tiesiskuma pamatleksiku;

b) nekvalificētus datu veidus;

c) kodu sarakstus Eiropas Savienības valodu kodiem.

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

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, 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 drošības notikumu reģistrēšanu saskaņā ar atzītiem starptautiskiem ieteikumiem par informācijas tehnoloģijas drošības standartiem ([1]);

e) 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. Ja *TLS* izmanto decentralizētās IT sistēmas kontekstā, tad ir jāizmanto protokola jaunākā stabilā versija vai, ja tādas nav, versija bez zināmām drošības ievainojamībām. Ir atļauti tikai kodu atslēgu garumi, kas nodrošina pienācīgu kriptogrāfiskās drošības līmeni, un netiek izmantoti šifra komplekti, par kuriem zināms, ka tie ir nedroši vai novecojuši.

5.4. Ciktāl iespējams, *PKI* digitālos sertifikātus, ko izmanto decentralizētās IT sistēmas darbības vajadzībām, izdod sertifikācijas iestādes, kas atzītas par kvalificētiem uzticamības pakalpojumu sniedzējiem saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 ([2]). Tiek īstenoti pasākumi, lai nodrošinātu, ka šādus sertifikātus izmanto tikai tiem paredzētajiem mērķiem, vajadzīgajā uzticamības līmenī un saskaņā ar piemērojamajām Regulas (ES) Nr. 910/2014 prasībām.

5.5. 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.

5.6. 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 ([3]) un Direktīvu (ES) 2016/680.

([1]) Neskarot reģistrēšanu drošības nolūkos, reģistrēšanas mehānismi, ko izmanto decentralizētās IT sistēmas komponenti, attiecīgā gadījumā ļauj nodrošināt atbilstību prasībām, kas noteiktas Regulas (ES) 2018/1725 88. pantā un attiecīgā gadījumā 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., ELI: http://data.europa.eu/eli/dir/2016/680/oj), 25. pantā.

([2]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp. ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([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).

5.7. Dalībvalstis, kuras izmanto valsts aizmugursistēmu, kas nav references īstenošanas programmatūra, īsteno vajadzīgos pasākumus, lai nodrošinātu, ka tās valsts aizmugursistēma atbilst Regulas (ES) 2016/679 un Direktīvas (ES) 2016/680 prasībām.

5.8. *Eurojust* īsteno vajadzīgos pasākumus, lai nodrošinātu, ka tās aizmugursistēma vai tās ieviestā references īstenošanas programmatūra atbilst Regulas (ES) 2018/1725 un (ES) 2018/1727 prasībām.

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

6. **Minimālie pieejamības mērķi**

6.1. *Eurojust* un dalībvalstis 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.

6.2. 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.

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

6.4. Dalībvalstis paziņo Komisijai, *Eurojust* un pārējām dalībvalstīm par uzturēšanas darbībām šādos termiņos:

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

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

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

6.5. Ja dalībvalstis ir noteikušas regulārus uzturēšanas periodus, tās informē Komisiju, *Eurojust* un pārējās dalībvalstis par laiku un dienu(-ām), kad šādi noteiktie regulārie periodi ir plānoti. Atkāpjoties no pirmajā teikumā izklāstītajiem pienākumiem – ja dalībvalstu atbildībā esošās decentralizētās IT sistēmas komponenti kļūst nepieejami šādā regulārā perioda laikā, dalībvalstis var izvēlēties neziņot Komisijai par katru reizi.

6.6. Dalībvalstu atbildībā esošas decentralizētas IT sistēmas komponenta neparedzētas tehniskas atteices gadījumā dalībvalstis nekavējoties informē Komisiju un pārējās dalībvalstis par atteici un, ja zināms, par plānoto atjaunošanas termiņu.

6.7. *Eurojust* paziņo Komisijai un dalībvalstīm par uzturēšanas darbībām šādos termiņos:

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

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

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

6.8. Ja *Eurojust* ir fiksēti regulārie uzturēšanas periodi, *Eurojust* informē Komisiju un dalībvalstis par laiku un dienu(-ām), kad šādi fiksēti regulārie intervāli ir plānoti. Atkāpjoties no pirmajā teikumā izklāstītajiem pienākumiem – ja decentralizētās IT sistēmas komponenti, par ko ir atbildīgs *Eurojust*, kļūst nepieejami šāda noteiktā regulārā perioda laikā, *Eurojust* var par to katru reizi nepaziņot Komisijai.

6.9. *Eurojust* atbildībā esošas decentralizētas IT sistēmas komponenta neparedzētas tehniskas kļūmes gadījumā *Eurojust* nekavējoties informē Komisiju un dalībvalstis par atteici un, ja tas ir zināms, par paredzamo atgūšanas termiņu.

6.10. Kompetento iestāžu / Tiesu datubāzes negaidītas tehniskas atteices gadījumā Komisija nekavējoties informē *Eurojust* un dalībvalstis par datubāzes nepieejamību un, ja tas ir zināms, par prognozējamo atjaunošanas termiņu.

6.11. Pakalpojuma traucējumu gadījumā dalībvalstis un *Eurojust* nodrošina, ka pakalpojums tiek ātri atjaunots un datu zudums ir minimāls saskaņā ar atveseļošanas laika mērķi un atveseļošanas punkta mērķi.

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

7. **Kompetentās iestādes / Tiesas datubāze (*CDB*)**

7.1. Saskaņā ar Regulas (ES) 2018/1727 22.a pantu decentralizētā IT sistēma nodrošina elektronisko saziņu starp kompetentajām valstu iestādēm un *Eurojust*. Ņemot vērā pienākumus apmainīties ar informāciju starp kompetentajām valsts iestādēm un *Eurojust* atbilstoši 21., 21.a un 22. pantam, kā arī *Eurojust* lomu veicināt un atbalstīt jebkura savstarpējas tiesiskās palīdzības vai savstarpējas atzīšanas lūguma izdošanu un izpildi saskaņā ar Regulas (ES) 2018/1727 8. panta 1. punktu, iesaistītajām kompetentajām iestādēm ir jābūt skaidri identificējamām, kad tās izmanto decentralizēto IT sistēmu. Tādēļ ir būtiski izveidot autoritatīvu šo iestāžu informācijas datubāzi decentralizētās IT sistēmas vajadzībām.

7.2. *CDB* strukturētā formātā iekļauj šādu informāciju:

a) Regulas (ES) 2018/1727 8. panta 1. punkta, 8. panta 3. punkta, 8. panta 4. punkta, 21. panta, 21.a panta un 22. panta vajadzībām informācija par kompetentajām valsts iestādēm, tostarp valsts korespondentiem, kā noteikts minētās regulas 20. pantā, kā arī par valsts pārstāvjiem saskaņā ar minētās regulas 7. pantu ([4]);

b) attiecīgā gadījumā informācija, kas vajadzīga, lai noteiktu iestāžu kompetences ģeogrāfiskās vai būtiskās jomas, vai citus attiecīgus kritērijus, kas vajadzīgi to kompetences noteikšanai;

c) informācija, kas vajadzīga pareizai tehniskai ziņojumu maršrutēšanai decentralizētajā IT sistēmā.

7.3. Komisija ir atbildīga par *CDB* izstrādi, uzturēšanu, darbību un atbalstu.

7.4. *CDB* ļauj dalībvalstīm un *Eurojust* atjaunināt tajā ietverto informāciju un kompetentajām valsts iestādēm un valstu pārstāvjiem, kas piedalās decentralizētajā IT sistēmā, programmatiski piekļūt informācijai un izgūt to.

7.5. Piekļuve *CDB* ir iespējama, izmantojot kopīgu saziņas protokolu, neatkarīgi no tā, vai kompetentās iestādes, kas savienotas ar decentralizēto IT sistēmu, izmanto valsts aizmugursistēmu vai references īstenošanas programmatūras izveidi.

7.6. Dalībvalstis nodrošina, ka informācija par to kompetentajām iestādēm *CDB*, kā noteikts 7.2. punktā, ir pilnīga, precīza un atjaunināta.

([4]) Tas neskar valsts pārstāvja pilnvaru deleģēšanu viņa vietniekam, citiem valsts biroja darbiniekiem vai pilnvarotiem *Eurojust* darbiniekiem.

II PIELIKUMS

DIGITĀLIE PROCESUĀLIE STANDARTI

Regulas (ES) 2022/850 3. panta 9. punktā digitālie procesuālie standarti ir definēti kā tehniskās specifikācijas darbības procesu modeļiem un datu shēmām, kas nosaka elektronisko struktūru datiem, kuru apmaiņu veic, izmantojot *e-CODEX* sistēmu.

Šajā pielikumā ir izklāstītas darbības procesu modeļu tehniskās specifikācijas un datu shēmu tehniskās specifikācijas.

1. **Tehniskās specifikācijas darbības procesu modeļiem saskaņā ar Regulu (ES) 2018/1727**

Darbības procesu modeļu tehniskās specifikācijas ir izklāstītas 1.1.–1.5. punktā. Tajās ir noteikti galvenie aspekti, kas nepieciešami elektroniskās saziņas nodrošināšanai Regulas (ES) 2018/1727 vajadzībām, izmantojot decentralizēto IT sistēmu.

Decentralizētā IT sistēma ļauj apmainīties ar informāciju tikai starp dalībvalsts kompetentajām valsts iestādēm un attiecīgās dalībvalsts valsts pārstāvi.

1.1. *Informācijas apmaiņa saistībā ar Eiropas Tiesu iestāžu pretterorisma reģistru (*CTR*) (Regulas (ES) 2018/1727 21.a pants)*

1.1.1. Modelis – *CTR* datu nosūtīšana

Kompetentā valsts iestāde nosūta ar *CTR* saistītajam valsts pārstāvim datus par terorisma procesiem.

1.1.2. Modelis – *CTR* datu saņemšana

Valsts pārstāvis saņem *CTR* datus.

1.1.3. Modelis – piekrišanas pieprasījums

Valsts pārstāvis lūdz savas kompetentās valsts iestādes piekrišanu.

1.1.4. Modelis – piekrišanas pieprasījuma saņemšana

Kompetentā valsts iestāde saņem piekrišanas pieprasījumu.

1.1.5. Modelis – atbildes uz piekrišanas pieprasījumu nosūtīšana

Kompetentā valsts iestāde nosūta atbildi uz piekrišanas pieprasījumu.

1.1.6. Modelis – atbildes uz piekrišanas pieprasījumu saņemšana

Valsts pārstāvis saņem atbildi uz piekrišanas pieprasījumu.

1.1.7. Modelis – informācija par saikni

Valsts pārstāvis informē kompetento valsts iestādi par saikni ar citu lietu.

1.1.8. Modelis – atjaunināt *CTR* datus

Kompetentā valsts iestāde tās attiecīgajam valsts loceklim nosūta datus, kas jāatjaunina vai jādzēš.

1.1.9. Modelis – saņemt atjauninātus *CTR* datus

Valsts pārstāvis saņem *CTR* datus, kas jāatjaunina vai jādzēš.

1.2. *Informācijas apmaiņa saistībā ar smagiem noziegumiem, Regulas (ES) 2018/1727 21. pants*

1.2.1. Modelis – nosūtīt datus par smagu noziegumu ar pārrobežu dimensiju

Valsts kompetentā iestāde nosūta *Eurojust* datus par smagiem pārrobežu noziegumiem.

1.2.2. Modelis – saņemt datus par smagu noziegumu ar pārrobežu dimensiju

Valsts pārstāvis saņem datus par smagiem pārrobežu noziegumiem.

1.2.3. Modelis – piekrišanas pieprasījums

Valsts pārstāvis lūdz savas valsts kompetentās iestādes piekrišanu.

1.2.4. Modelis – piekrišanas pieprasījuma saņemšana

Kompetentā valsts iestāde saņem piekrišanas pieprasījumu.

1.2.5. Modelis – atbildes uz piekrišanas pieprasījumu nosūtīšana

Kompetentā valsts iestāde nosūta atbildi uz piekrišanas pieprasījumu.

1.2.6. Modelis – atbildes uz piekrišanas pieprasījumu saņemšana

Valsts pārstāvis saņem atbildi uz piekrišanas pieprasījumu.

1.2.7. Modelis – informācija par saikni

Valsts pārstāvis informē kompetento valsts iestādi par saikni ar citu lietu.

1.2.8. Modelis – atjaunināt datus par smagu noziegumu ar pārrobežu dimensiju

Kompetentā valsts iestāde tās attiecīgajam valsts loceklim nosūta datus, kas jāatjaunina vai jādzēš.

1.2.9. Modelis – saņemt atjauninātus datus par smagu noziegumu ar pārrobežu dimensiju

Valsts pārstāvis saņem tādus datus par smagiem pārrobežu noziegumiem, kuri ir jāatjaunina vai jādzēš.

1.3. *Vispārējas informācijas apmaiņa*

1.3.1. Modelis – nosūtīt informāciju

Valsts pārstāvis nosūta informāciju kompetentajai valsts iestādei vai otrādi.

1.3.2. Modelis – saņemt informāciju

Informāciju saņem kompetentā valsts iestāde vai valsts pārstāvis.

1.3.3. Modelis – atbildēt uz informāciju

Kompetentā valsts iestāde atbild uz informāciju, kas saņemta no valsts pārstāvja, vai otrādi.

1.3.4. Modelis – saņemt atbildi

Valsts pārstāvis saņem atbildi no kompetentās valsts iestādes.

1.3.5. Modelis – nosūtīt informāciju

Kompetentā valsts iestāde nosūta informāciju valsts pārstāvim.

1.3.6. Modelis – saņemt informāciju

Valsts pārstāvis saņem informāciju.

1.3.7. Modelis – atbildēt uz informāciju

Valsts pārstāvis atbild uz informāciju, kas saņemta no kompetentās valsts iestādes.

1.3.8. Modelis – saņemt atbildi

Kompetentā valsts iestāde saņem atbildi no valsts pārstāvja.

1.4. *Veicināšanas un atbalsta loma (Regulas (ES) 2018/1727 8. panta 1. punkts)*

Piezīme. Ja 1.5. punktā izklāstītie veicināšanas un atbalsta modeļi ietver apmaiņu tiesību aktos noteiktos veidos, kas izveidoti ar Savienības tiesību aktiem tiesu iestāžu sadarbības krimināllietās jomā, modeļos, ja tādi ir pieejami, izmanto attiecīgos strukturētos datu apliecinājumus un *XML* shēmas, kas izstrādātas minētajiem aktiem, piemēram, tās, kas izveidotas Īstenošanas regulas (ES) 2023/2844 vai citu attiecīgo instrumentu vajadzībām.

1.5. *Veicināšanas vai atbalsta pieprasījuma modelis*

1.5.1. Modelis – pārsūtīt veicināšanas vai atbalsta pieprasījumu

Valsts kompetentā iestāde pārsūta veicināšanas pieprasījumu vai atbalsta pieprasījumu savam attiecīgajam valsts pārstāvim.

1.5.2. Modelis – saņemt veicināšanas vai atbalsta pieprasījumu

Valsts pārstāvis saņem veicināšanas vai atbalsta pieprasījumu un nosūta to pieprasījuma saņēmējas dalībvalsts valsts pārstāvim ārpus *JUDEX*.

1.5.3. Modelis – pārsūtīt veicināšanas vai atbalsta pieprasījumu kompetentajai valsts iestādei

Pieprasījuma saņēmējas dalībvalsts valsts pārstāvis nosūta pieprasījumu savai attiecīgajai kompetentajai valsts iestādei.

1.5.4. Modelis – saņemt veicināšanas vai atbalsta pieprasījumu

Kompetentā valsts iestāde saņem veicināšanas vai atbalsta pieprasījumu.

1.5.5. Modelis – nosūtīt atbildi uz veicināšanas vai atbalsta pieprasījumu

Kompetentā valsts iestāde pieprasījuma saņēmējas dalībvalsts valsts pārstāvim nosūta atbildi vai informāciju par pieprasījumu.

1.5.6. Modelis – saņemt atbildi uz veicināšanas vai atbalsta pieprasījumu

Valsts pārstāvis no kompetentās valsts iestādes saņem atbildi uz veicināšanas vai atbalsta pieprasījumu vai informāciju par to un nosūta to pieprasītājas dalībvalsts valsts pārstāvim ārpus *JUDEX*.

1.5.7. Modelis – atbildēt uz veicināšanas vai atbalsta pieprasījumu

Pieprasījuma iesniedzējas dalībvalsts valsts pārstāvis atbild uz kompetentās valsts iestādes sniegto informāciju par veicināšanas vai atbalsta pieprasījumu vai apmainās ar informāciju par to.

1.5.8. Modelis – saņemt atbildi

Kompetentā valsts iestāde saņem atbildi uz veicināšanas vai atbalsta pieprasījumu vai informāciju par to.

2. **Datu shēmu tehniskās specifikācijas**

Tehniskās specifikācijas, kas jāizmanto par pamatu *XML* shēmu definīciju (*XSD*) izstrādei Regulas (ES) 2018/1727 digitalizācijai, ir izklāstītas šā pielikuma 2.1. un 2.2. punktā. Minētajās specifikācijās ir noteikti galvenie komponenti un cita informācija, kas sniedz visaptverošu aprakstu šo shēmu ražošanai.

Apraksts ar nodomu ir veidots vispārīgs, lai ļautu modificēt un paplašināt ražotos *XSD*, un tam nebūtu vajadzīgas būtiskas izmaiņas šajās specifikācijās.

Šīs specifikācijas attiecas uz to tiesību aktos noteikto shēmu veidiem, kas pievienotas Regulai (ES) 2018/1727, visiem iepriekš noteiktiem ziņojumiem vai visiem brīvā teksta ziņojumiem, ko izmanto apmaiņai saskaņā ar minēto regulu.

2.1. *Vispārīgi apsvērumi*

Attiecībā uz visām shēmām piemēro šādus noteikumus.

2.1.1. Versijpārvaldība

Iekļauj versijas atribūtu, kas atvieglo shēmas versijpārvaldību un ļauj shēmu atjaunināt turpmākajās iterācijās atbilstoši uzņēmējdarbības prasībām. Versijas atribūts norāda, vai jaunā versija ir atpakaļsaderīga gadījumā, ja tiek ieviestas jaunas funkcijas vai papildinājumi.

2.1.2. Shēmas deklarācija un metadati

— Attiecīgā gadījumā shēmā izmanto attiecīgus standartus vai leksiku, kas *e-CODEX* vajadzīga sadarbspējas nodrošināšanai, lai pienācīgi validētu šajā shēmā definētos elementus un veidus. Tas var ietvert:

  — ES e-tiesiskuma pamatleksiku,

  — nekvalificētus datu veidus,

  — kodu sarakstu Eiropas Savienības valodu kodiem.

— Attiecīgā gadījumā shēmā var iekļaut attiecīgos ETSI standartus, lai izmantotu to definīcijas.

2.1.3. Anotācijas un dokumentācija

— **Anotācijas**: katram shēmas elementam parasti pievieno anotācijas. Anotācijas sniedz cilvēklasāmu informāciju par elementu, bieži skaidri un kodolīgi definējot tā nolūku vai lietojumu.

2.1.4. Izmantošana un pielāgojamība

Shēmā ievēro šādus noteikumus, kas izklāstīti a) līdz d) apakšpunktā.

a) **Modulārā struktūra**: katru sadaļu projektē ar īpašu funkcionalitāti, un to var izmantot atkārtoti vai pielāgot atsevišķi. Tas padara shēmu viegli pielāgojamu dažādiem lietošanas gadījumiem.

b) **Paplašināmība**: shēmu izstrādā tā, lai atbalstītu jaunu elementu vai atribūtu iekļaušanu, ja nākotnē būs vajadzīga papildu informācija. To panāk, izmantojot fakultatīvus elementus un sekvences, ko var paplašināt, netraucējot esošās shēmas darbībai.

c) **Pielāgojama struktūra**: shēmu izstrādā tā, lai vajadzības gadījumā varētu pievienot vai mainīt elementus vai datu tipus. Shēmas struktūrā jāspēj veikt izmaiņas prasībās, neveicot būtisku tās pārprojektēšanu.

d) **Fakultatīvi elementi**: shēmas elementus var marķēt kā fakultatīvus, t. i., īpašos apstākļos tos var iekļaut vai izlaist.

Shēmu izstrādā tā, lai ar tās palīdzību varētu vākt strukturētus datus konkrētiem pieprasījumiem.

2.1.5. Izmaiņas

Shēmu raksturo elastīgums, modularitāte un viegla tās pielāgošana. Sarežģīti tipi un fakultatīvi elementi shēmā tiek iestrādāti tā, lai tie būtu pielāgoti dažādiem scenārijiem un viegli pārveidojami un paplašināmi.

2.2. *Strukturētu datu apmaiņa*

Strukturētos datus, kas minēti 2.2.1. un 2.2.2. punktā, sniedz saskaņā ar Regulas (ES) 2018/1727 22.a panta 3. punktu. Shēma ļauj arī norādīt datu kopas, kuras turpmākajos atjauninājumos ir jādzēš.

2.2.1. Eiropas Tiesu iestāžu pretterorisma reģistra dati

Turpmāk norādītās datu shēmas tehniskās specifikācijas veido strukturētu satvaru shēmas izveidei *XML* formātā.

a) Augstākā līmeņa iedaļa

Šī augstākā līmeņa iedaļa atbilst Regulas (ES) 2018/1727 III pielikumā izklāstītajai informācijai Eiropas Tiesu iestāžu pretterorisma reģistram (*CTR*).

b) Ziņojuma struktūra

CTR datu struktūra sastāv no elementu secības un ietver vismaz šādus elementus:

i) informācija fizisku personu identificēšanai:

— uzvārds (dzimtais uzvārds),

— vārds(-i),

— visi pseidonīmi,

— dzimšanas datums,

— dzimšanas vieta (pilsēta un valsts),

— valstspiederība vai valstspiederības,

— identifikācijas dokuments (veids un dokumenta numurs),

— dzimums,

— dzīvesvieta;

ii) informācija juridisku personu identificēšanai:

— nosaukums,

— juridiskā forma,

— galvenā biroja atrašanās vieta;

iii) informācija fizisku un juridisku personu identificēšanai:

— tālruņa numuri,

— e-pasta adreses,

— informācija par kontiem bankās vai citās finanšu iestādēs,

— statuss tiesvedībā;

iv) informācija par nodarījumu:

— informācija par juridiskām personām, kas iesaistītas teroristu nodarījuma sagatavošanā vai veikšanā,

— nodarījuma juridiskā kvalifikācija saskaņā ar valsts tiesību aktiem,

— piemērojamais smaga nozieguma veids no I pielikumā izklāstītā saraksta,

— jebkāda saistība ar teroristu grupu,

— terorisma veids, piemēram, džihādisti, separātisti, kreisi noskaņotie vai labēji noskaņotie,

— īss lietas kopsavilkums;

v) informācija par valsts procesu:

— šāda procesa statuss,

— atbildīgā prokuratūra,

— lietas numurs,

— oficiālas tiesvedības sākšanas datums,

— saiknes ar citām attiecīgām lietām;

vi) papildinformācijas lauks (brīvā formā);

vii) iepriekšējas atļaujas kods.

2.2.2. Dati, kas nosūtīti saskaņā ar Regulas (ES) 2018/1727 21. pantu

a) Regulas (ES) 2018/1727, ar ko izveido kopējas izmeklēšanas grupas (“KIG”), 21. panta 4. punkts

i) Augstākā līmeņa iedaļa
Šī augstākā līmeņa iedaļa atbilst Regulas (ES) 2018/1727 21. panta 4. punktā izklāstītajai informācijai par KIG izveidi.

ii) Ziņojuma struktūra
Datu struktūra sastāv no elementu secības un ietver vismaz šādus elementus.

— Par kriminālprocesu atbildīgā valsts tiesu iestāde

— Kriminālprocesa valsts atsauces numurs

— Kriminālprocesa statuss

— Izmeklētie noziedzīgie nodarījumi

— Citas lietā iesaistītās valstis

— Vai tā ir lieta, ko jau atbalsta *Eurojust*?

— Ja atbilde ir “jā” – *Eurojust* lietas ID.

— Ja atbilde ir “nē” – vai tas ir atbalsta pieprasījums?

— Vai tā ir lieta, ko atbalsta Eiropols?

— Ja atbilde ir "jā" – vai operatīvā darba grupa (*OTF*) un/vai drošas informācijas apmaiņas tīkla lietojumprogramma ("*SIENA*")?

— KIG nolīgums:

— Iesaistītās valstis

— KIG puses (par izmeklēšanu atbildīgās valsts iestādes)

— Kriminālprocesa, ar ko nodarbojas KIG, valsts atsauces numurs

— Parakstīšanas datums

— Ilgums

— Izmeklētie noziedzīgie nodarījumi

— Īss lietas kopsavilkums

— Galvenie aizdomās turamie kriminālprocesā, ko izmeklē KIG (vārds, uzvārds, dzimšanas datums un vieta un, iespējams, citas būtiskas un nepieciešamas datu kategorijas atbilstoši II pielikumam)

— KIG darba rezultāti:

— Grūtības/kavēšanās saistībā ar

— KIG izveidi

— pierādījumu pieprasīšanu/koplietošanu KIG ietvaros

— vienošanās panākšanu par kopīgu kriminālvajāšanas stratēģiju/īstenošanu

— KIG pierādījumu pieņemamība/nepieņemamība/izvērtēšana valsts tiesvedībā

— Tiesvedības iznākums (sekmīga/nesekmīga kriminālvajāšana un notiesājošs/attaisnojošs spriedums)

iii) Iepriekšējas atļaujas kods

b) Regulas (ES) 2018/1727 21. panta 5. punkts, nopietnas sarežģītas lietas

i) Augstākā līmeņa iedaļa

Šī augstākā līmeņa iedaļa atbilst *Eurojust* regulas 21. panta 5. punktā izklāstītajai informācijai, proti – nopietnas sarežģītas lietas

ii) Ziņojuma struktūra

Datu struktūra sastāv no elementu secības un ietver vismaz šādus elementus.

— Par kriminālprocesu atbildīgā valsts tiesu iestāde

— Kriminālprocesa valsts atsauces numurs

— Kriminālprocesa statuss

— Izmeklētie noziedzīgie nodarījumi

— Citas lietā iesaistītās valstis

— Vai tā ir lieta, ko jau atbalsta *Eurojust*?

— Ja atbilde ir "jā" – *Eurojust* lietas ID.

— Ja atbilde ir "nē" – vai tas ir atbalsta pieprasījums?

— Vai tā ir lieta, ko atbalsta Eiropols?

— Ja atbilde ir "jā" – vai operatīvā darba grupa un/vai *SIENA*?

— Piemērojamais smagu noziedzīgu nodarījumu veids

— Iesaistīts organizētās noziedzības tīkls

— Mafijas veids

— Transnacionāls organizētās noziedzības tīkls

— Ietekme ES līmenī

— Galvenie kriminālprocesā aizdomās turamie (vārds, uzvārds, dzimšanas datums un vieta un, iespējams, citas būtiskas un nepieciešamas datu kategorijas atbilstoši II pielikumam)

— Īss lietas kopsavilkums

— Citas iesaistītās valstis

— Valstis, ar kurām jau sākta sadarbība

— Kompetentās iestādes, kas iesaistītas citā valstī

— Izmantotie tiesu iestāžu sadarbības rīki

— Nosūtīto/saņemto pieprasījumu skaits

— Saistīto izmeklēšanu esamība

— Valstis, ar kurām var uzsākt sadarbību / kuras varētu būt skartas

— Vajadzīgās sadarbības veids (piemēram, izdošana, pierādījumu vākšana, cita veida sadarbība)

— Saistīto izmeklēšanu esamība

iii) Iepriekšējas atļaujas kods

c) Regulas (ES) 2018/1727 21. panta 6. punkta a) apakšpunkts, jurisdikcijas kolīzijas

i) Augstākā līmeņa iedaļa

Šī augstākā līmeņa iedaļa atbilst Regulas (ES) 2018/1727 21. panta 6. punkta a) apakšpunktā izklāstītajai informācijai, t. i., jurisdikcijas kolīzijas.

ii) Ziņojuma struktūra

Datu struktūra sastāv no elementu secības un ietver vismaz šādus elementus.

— Par kriminālprocesu atbildīgā valsts tiesu iestāde

— Kriminālprocesa valsts atsauces numurs

— Kriminālprocesa statuss (piemēram, izmeklēšana, kriminālvajāšana, tiesas process)

— Izmeklētie noziedzīgie nodarījumi

— Citas lietā iesaistītās valstis

— Vai tā ir lieta, ko jau atbalsta *Eurojust*?

— Ja atbilde ir "jā" – *Eurojust* lietas ID.

— Ja atbilde ir "nē" – vai tas ir atbalsta pieprasījums?

— Vai tā ir lieta, ko atbalsta Eiropols?

— Ja atbilde ir "jā" – vai operatīvā darba grupa un/vai *SIENA*?

— Citas iesaistītās valstis

— Kompetentās valsts iestādes citā valstī, ja tās ir zināmas

— Kriminālprocesa valsts atsauces numurs citā valstī

— Tiesvedības posms citā valstī, ja zināms

— Pozitīvs vai negatīvs konflikts

— Faktisks vai potenciāls konflikts

— Jau veiktās koordinācijas darbības (piemēram, konsultācijas saskaņā ar Padomes Pamatlēmumu 2009/948/TI ([1]))

— Īss lietas kopsavilkums

— Galvenie kopīgie aizdomās turamie (vārds, uzvārds, dzimšanas datums un vieta un, iespējams, citas būtiskas un nepieciešamas datu kategorijas saskaņā ar II pielikumu)

iii) Iepriekšējas atļaujas kods

d) 21. panta 6. punkta b) apakšpunkts, kontrolētas piegādes

i) Augstākā līmeņa iedaļa

Šī augstākā līmeņa iedaļa atbilst Regulas (ES) 2018/1727 21. panta 6. punkta b) apakšpunktā izklāstītajai informācijai. kontrolētas piegādes

ii) Ziņojuma struktūra

Datu struktūra sastāv no elementu secības un ietver vismaz šādus elementus.

— Par kriminālprocesu atbildīgā valsts tiesu iestāde

— Kriminālprocesa valsts atsauces numurs

— Kriminālprocesa statuss (piemēram, izmeklēšana, kriminālvajāšana, tiesas process)

— Izmeklētie noziedzīgie nodarījumi

— Citas lietā iesaistītās valstis

— Vai tā ir lieta, ko jau atbalsta *Eurojust*?

— Ja atbilde ir "jā" – *Eurojust* lietas ID.

— Ja atbilde ir "nē" – vai tas ir atbalsta pieprasījums?

— Vai tā ir lieta, ko atbalsta Eiropols?

— Ja atbilde ir "jā" – vai operatīvā darba grupa un/vai *SIENA*?

— Citas iesaistītās valstis

— Izcelsmes/tranzīta/galamērķa valsts

— Citu valstu kompetentās iestādes

— Saistīta izmeklēšana citās valstīs

([1]) Padomes Pamatlēmums 2009/948/TI (2009. gada 30. novembris) par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu krimināprocesā (OV L 328, 15.12.2009., 42. lpp., ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Piegādāto preču veids (piemēram, narkotikas un veids/nauda/ieroči/cigaretes/cits)

— Kontrolētās piegādes statuss (piemēram, plānota, notiekoša, pabeigta)

— Kontrolētās piegādes iznākums, ja tā jau ir veikta

— Izmantotie tiesu iestāžu sadarbības rīki

— Galvenie kopīgie aizdomās turamie (vārds, uzvārds, dzimšanas datums un vieta un, iespējams, citas būtiskas un nepieciešamas datu kategorijas saskaņā ar II pielikumu)

iii) Iepriekšējas atļaujas kods

e) Regulas (ES) 2018/1727 21. panta 6. punkta c) apakšpunkts, atkārtotas problēmas ar tiesu iestāžu sadarbības instrumentiem

i) Augstākā līmeņa iedaļa

Šī augstākā līmeņa iedaļa atbilst Regulas (ES) 2018/1727 21. panta 6. punkta c) apakšpunktā izklāstītajai informācijai. atkārtotas problēmas ar tiesu iestāžu sadarbības instrumentiem

ii) Ziņojuma struktūra

Datu struktūra sastāv no elementu secības un ietver vismaz šādus elementus.

— Par kriminālprocesu atbildīgā valsts tiesu iestāde

— Kriminālprocesa valsts atsauces numurs

— Kriminālprocesa statuss (piemēram, izmeklēšana, kriminālvajāšana, tiesas process)

— Izmeklētie noziedzīgie nodarījumi

— Citas lietā iesaistītās valstis

— Vai tā ir lieta, ko jau atbalsta *Eurojust*?

— Ja atbilde ir "jā" – *Eurojust* lietas ID.

— Ja atbilde ir "nē" – vai tas ir atbalsta pieprasījums?

— Vai tā ir lieta, ko atbalsta Eiropols?

— Ja atbilde ir "jā" – vai operatīvā darba grupa un/vai *SIENA*?

— Citas iesaistītās valstis

— Kompetentās valsts iestādes, ja tās ir zināmas

— Darbojoties kā izdevējiestāde vai izpildiestāde

— Iesaistītais tiesu iestāžu sadarbības instruments (piemēram, Eiropas apcietināšanas orderis, EIR, iesaldēšana un konfiskācija)

— Attiecīgais konkrētais pieprasījums (t. i., kāds izmeklēšanas pasākums, kāda veida iesaldēšana, Eiropas apcietināšanas orderis soda izpildei vai kriminālvajāšanai)

— Atteikums vai atkārtotas grūtības

— Atteikuma gadījumā – kāds ir konkrētais pamatojums?

— Īss problēmas apraksts

— Citas valsts iestādes (ja tādas ir), kuras skar tā pati problēma

iii) Iepriekšējas atļaujas kods

2.3. *Iepriekšējas atļaujas kodi*

Kopīgojot datus ar *Eurojust* ar *JUDEX* starpniecību, kompetentās valsts iestādes, izmantojot iepriekšējas atļaujas kodus, norāda turpmāko datu apstrādi, piekļuvi tiem un to pārsūtīšanu pēc saiknes identificēšanas. Iepriekšējas atļaujas kodos norāda, vai un cik lielā mērā ar saikni saistīto informāciju var kopīgot ar citām kompetentajām valsts iestādēm, citām Savienības aģentūrām un struktūrām, trešām valstīm vai starptautiskām organizācijām.

2.4. *Iepriekšdefinēti ziņojumi*

Iepriekšdefinēti ziņojumi ir ar Regulu (ES) 2018/1727 izveidotas apmaiņas atveidojumi, attiecībā uz kuriem tiesību aktos nav paredzēta konkrēta forma. To veidus un skaitu nosaka darījumdarbības un tehniskās analīzes ietvaros.

XLM shēmu definīciju (*XSD*) iepriekšdefinētiem ziņojumiem izstrādā tā, lai nodrošinātu konsekvenci, struktūru un atbilstību darījumdarbības vajadzībām.

Uz šīm shēmām attiecas turpmāk minētais:

a) augstākā līmeņa iedaļu šajā shēmā nosauc atbilstoši konkrētajam definējamajam ziņojuma veidam;

b) šajā struktūrā pievieno un definē konkrētajam ziņojuma veidam vajadzīgos laukus, nodrošinot datu elementu pienācīgu atveidojumu.

2.5. *Brīvā teksta ziņojumi*

Brīvā teksta ziņojumi ir informācijas apmaiņa, kas pieļauj nestrukturētu vai daļēji strukturētu saturu, nodrošinot elastību, vienlaikus ievērojot regulatīvās un darījumdarbības prasības. *XSD* brīvā teksta ziņojumiem izstrādā tā, lai nodrošinātu konsekvenci un pareizu formatēšanu.

Attiecībā uz minētajām shēmām piemēro turpmāk minēto:

a) shēmas augstākā līmeņa iedaļu nosauc atbilstoši definētajam konkrētā brīvā teksta ziņojuma veidam;

b) shēmā nosaka nepieciešamo brīvā teksta ziņojuma struktūru, vienlaikus pēc vajadzības ļaujot pienācīgi sakārtot elementus;

c) struktūrā pievieno un definē konkrētajam brīvā teksta ziņojuma veidam vajadzīgos laukus, nodrošinot datu elementu pienācīgu atveidojumu.

III PIELIKUMS

PIRKSTU NOSPIEDUMU UN FOTOGRĀFIJU TEHNISKĀS SPECIFIKĀCIJAS

Ziņojumiem, ar kuriem apmainās, izmantojot decentralizēto IT sistēmu, var pievienot pielikumus, tostarp Nacionālā standartu un tehnoloģiju institūta (*NIST*) datnes, kurās ir pirkstu nospiedumi un fotogrāfijas, saskaņā ar 1. un 2. punktā noteiktajām tehniskajām specifikācijām.

1. **Pirkstu nospiedumi**

Pirkstu nospiedumi, kurus var nodot *Eurojust*, lai ticami identificētu personas, uz kurām attiecas kriminālprocess saistībā ar terorisma nodarījumiem, atbilst šādiem nosacījumiem:

a) pirkstu nospiedumus sniedz vienā datnē, kurā ir pirkstu nospiedumu digitālie attēli (pirkstu nospiedumu *NIST* datne), un tos iesniedz saskaņā ar *ANSI/NIST-ITL 1-2011* atjaunināto 2015. gada standartu (vai jaunāku versiju);

b) pirkstu nospiedumu *NIST* datni veido ne vairāk kā desmit atsevišķi pirkstu nospiedumi, kas ir pārvelti, uzspiesti vai abējādi iegūti;

c) visi pirkstu nospiedumi ir marķēti;

d) pirkstu nospiedumus iegūst, izmantojot tiešās skenēšanas ierīces vai tinti uz papīra, ja pirkstu nospiedumi, kas iegūti ar tinti uz papīra, ir skenēti vajadzīgajā izšķirtspējā un tādā pašā kvalitātē;

e) pirkstu nospiedumu *NIST* datne ļauj iekļaut papildu informāciju, piemēram, pirkstu nospiedumu reģistrācijas nosacījumus un metodi, ko izmanto atsevišķu pirkstu nospiedumu attēlu iegūšanai;

f) pirkstu nospiedumu nominālā izšķirtspēja ir vai nu 500 ppi, vai 1 000 ppi [1] (ar pieņemamu novirzi +/– 10 ppi) ar 256 pelēkās krāsas toņiem;

g) Izmantojamajā pirkstu nospiedumu saspiešanas algoritmā jāievēro Nacionālā Standartu un tehnoloģiju institūta (*NIST*) ieteikumi. Pirkstu nospiedumu datus ar 500 ppi izšķirtspēju saspiež, izmantojot *WSQ* algoritmu (ISO/IEC 19794-5:2005). Pirkstu nospiedumu datus ar 1 000 ppi izšķirtspēju saspiež, izmantojot *JPEG* 2000 attēlu saspiešanas standartu (ISO/IEC 15444-1) un kodēšanas sistēmu. Mērķa saspiešanas pakāpe ir 15:1.

2. **Fotoattēli**

Fotoattēli, ko var kopīgot ar *Eurojust*, lai ticami identificētu personas, uz kurām attiecas kriminālprocess saistībā ar terorisma nodarījumiem, atbilst šādiem nosacījumiem:

a) ir sniegts tikai viens sejas attēls fotoattēla veidā (*NIST* fotoattēla datnē), kas iesniegts saskaņā ar *ANSI/NIST-ITL 1-2011* atjaunināto 2015. gada standartu (vai jaunāku pieejamo versiju);

b) fotoattēli ir pelēktoņu, krāsaini vai tuvā infrasarkanā starojuma attēli;

c) fotoattēlu kvalitāte atbilst standarta ISO/IEC 19794-5:2011 (vai jaunākas versijas) frontālā attēla tipa attēla prasībām;

d) fotoattēla *NIST* datnē ir iespējams iekļaut papildu informāciju, ieskaitot attēla uzņemšanas datumu;

[1] Pikseļi collā.

e) fotoattēlu, kas uzņemtas portretorientācijā, izšķirtspēja ir vismaz 600 pikseļu reiz 800 pikseļu, bet ne vairāk kā 1 200 pikseļu reiz 1 600 pikseļu;

f) sejas uzņēmums aizņem tik daudz vietas fotoattēlā, lai nodrošinātu, ka starp acu centriem ir vismaz 120 pikseļu;

g) izmantotais fotoattēlu saspiešanas algoritms ievēro Nacionālā Standartu un tehnoloģiju institūta (*NIST*) ieteikumus. Fotoattēlus saspiež tikai vienu reizi ar *JPG* (ISO/IEC 10918) vai *JPEG* 2000 (ISO/IEC 15444) attēla saspiešanas standartu un kodēšanas sistēmu ar maksimālo pieļaujamo attēla kompresijas attiecību 20:1.