Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/2447

2025 12 5

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/2447

2025 m. gruodžio 4 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2018/1727 taikymo taisyklės dėl decentralizuotos IT sistemos, skirtos informacijai saugiai tvarkyti ir perduoti, techninių specifikacijų, priemonių ir kitų reikalavimų dėl jos sukūrimo bei naudojimo

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2018 m. lapkričio 14 d. Europos Parlamento ir Tarybos reglamentą (ES) 2018/1727 dėl Europos Sąjungos bendradarbiavimo baudžiamosios teisenos srityje agentūros (Eurojusto) ir kuriuo pakeičiamas ir panaikinamas Tarybos sprendimas 2002/187/TVR ([1]), ypač į jo 22a straipsnio 3 dalį ir 22b straipsnio 1 dalies a, b, c ir d punktus,

kadangi:

(1) Reglamentu (ES) 2018/1727 nustatytas naujos Eurojusto skaitmeninės vidaus infrastruktūros pagrindas ir decentralizuotos saugios valstybių narių kompetentingų nacionalinių institucijų ir Eurojusto skaitmeninės komunikacijos sistemos sukūrimas;

(2) saugi skaitmeninė komunikacija turi vykti per decentralizuotą IT sistemą. Siekiant sukurti decentralizuotą IT sistemą būtina nustatyti technines specifikacijas, kuriomis būtų apibrėžti komunikacijos metodai ir komunikacijos protokolai, techninės priemonės, kuriomis užtikrinami minimalieji informacijos saugumo standartai ir saugumas, ir šios sistemos diegimo bei minimaliojo prieinamumo tikslai;

(3) pagal Reglamento (ES) 2018/1727 22a straipsnio 1 dalį, decentralizuota IT sistema turi būti sudaryta iš valstybių narių ir Eurojusto IT sistemų, taip pat sąveikių e. CODEX prieigos taškų, per kuriuos tos IT sistemos yra sujungtos. Šiame reglamente nustatomose decentralizuotos IT sistemos techninėse specifikacijose ir kituose reikalavimuose turėtų būti atsižvelgiama į tą pamatinę struktūrą;

(4) decentralizuotos IT sistemos prieigos taškai turėtų būti nustatyti patvirtintų e. CODEX prieigos taškų, apibrėžtų Europos Parlamento ir Tarybos reglamento (ES) 2022/850 ([2]) 3 straipsnio 3 punkte, pagrindu;

(5) decentralizuota IT sistema diegiama didesnėje e. CODEX grindžiamoje decentralizuotoje IT sistemoje, vadinamoje skaitmeninio keitimosi teisingumo duomenimis sistema (JUDEX). Todėl būtina užtikrinti veiksmingą keitimąsi informacija apie horizontaliąją raidą;

(6) pagal Reglamento (ES) 2018/1727 22a straipsnio 4 dalį, valstybės narės ir Eurojustas gali nuspręsti vietoj nacionalinės IT sistemos naudoti Komisijos sukurtą bazinio sistemos modelio programinę įrangą kaip savo galinę sistemą. Siekiant užtikrinti sąveikumą, nacionalinėms IT sistemoms ir bazinio sistemos modelio programinei įrangai turėtų būti taikomos tos pačios techninės specifikacijos ir reikalavimai;

(7) su teroristiniais nusikaltimais ir sunkių formų organizuotu nusikalstamumu susijusių duomenų perdavimas turėtų būti struktūrizuotas, kad būtų pagerinta informacijos kokybė ir aktualumas, taip pat užtikrinta, kad informaciją būtų galima efektyviau integruoti į Eurojusto bylų valdymo sistemą ir geriau sutikrinti su joje jau saugoma informacija. turėtų būti nustatytas pirštų atspaudų duomenų ir nuotraukų, kurie gali būti perduodami Eurojustui asmenų, dėl kurių vyksta su teroristiniais nusikaltimais susijęs baudžiamasis procesas, tapatybei nustatyti, perdavimo formatas ir techniniai standartai;

([1]) OL L 295, 2018 11 21, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

([2]) 2022 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/850 dėl tarpvalstybinio elektroninio keitimosi duomenimis teisminio bendradarbiavimo civilinėse ir baudžiamosiose bylose srityje kompiuterinės sistemos (sistemos e. CODEX), kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1726, (OL L 150, 2022 6 1, p. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojustas tarpininkauja ir teikia pagalbą išduodant ir vykdant teisminio bendradarbiavimo prašymus, įskaitant prašymus ir sprendimus dėl priemonių, kuriomis įgyvendinamas tarpusavio pripažinimo principas. Nacionalinės kompetentingos institucijos turėtų turėti galimybę prašyti Eurojusto pagalbos ir koordinavimo per decentralizuotą IT sistemą;

(9) siekiant užtikrinti efektyvumą ir nuoseklumą, svarbu, kad techninės specifikacijos, kurios turi būti nustatytos pagal Reglamentą (ES) 2018/1727, būtų suderinamos su techninėmis specifikacijomis, nustatytomis pagal Europos Parlamento ir Tarybos reglamentus (ES) 2023/2844 ([3]), (ES) 2023/1543 ([4]) ir (ES) 2024/3011 ([5]), taip pat su būsimomis skaitmenizacijos priemonėmis, susijusiomis su Eurojusto įgaliojimais teikti paramą nacionalinėms kompetentingoms institucijoms;

(10) per decentralizuotą IT sistemą taip pat turėtų galėti vykti bet kokia kita Eurojusto ir kompetentingų nacionalinių institucijų komunikacija, kaip antai informacijos apie informacijos tvarkymo rezultatus perdavimas, įskaitant informaciją apie tai, ar esama sąsajų su bylų valdymo sistemoje jau saugomomis bylomis, pagal Reglamento (ES) 2018/1727 22 straipsnį, kai Eurojustas veikia savo iniciatyva, arba informaciją, perduodamą Eurojustui tam, kad būtų išsaugoti, analizuojami ir laikomi su genocidu, nusikaltimais žmoniškumui, karo nusikaltimais ir susijusiomis nusikalstamomis veikomis susiję įrodymai, pagal to reglamento 4 straipsnio 1 dalies j punktą;

(11) siekiant užtikrinti, kad šiame reglamente būtų atsižvelgiama į Eurojusto veiklos poreikius, pagal Reglamento (ES) 2018/1727 22a straipsnio 3 dalį konsultuotasi su Eurojustu;

(12) pagal prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo pridėto Protokolo Nr. 21 dėl Jungtinės Karalystės ir Airijos pozicijos dėl laisvės, saugumo ir teisingumo erdvės 4 straipsnį Airija 2019 m. rugsėjo 9 d. raštu pranešė ketinanti pripažinti Reglamentą (ES) 2018/1727 ir jo laikytis. Komisijos sprendimu (ES) 2019/2006 ([6]) patvirtinamas Airijos dalyvavimas. Europos Parlamento ir Tarybos reglamentu (ES) 2023/2131 ([7]) iš dalies pakeistas Reglamentas (ES) 2018/1727, kad būtų galima sukurti saugios skaitmeninės komunikacijos kanalus tarp Eurojusto ir kompetentingų nacionalinių institucijų, ir suteiktas teisinis pagrindas šiam reglamentui. Tokiomis aplinkybėmis, kai Airija nepranešė apie savo pageidavimą dalyvauti priimant ir taikant Reglamentą (ES) 2023/2131 ir nepranešė apie ketinimą pripažinti tą reglamentą ir jo laikytis, Airijai pagal Protokolo Nr. 21 1, 2 straipsnius ir 4a straipsnio 1 dalį Reglamentas (ES) 2023/2131 nėra privalomas ar taikomas. Todėl Airija nedalyvauja priimant šį reglamentą;

(13) pagal prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo pridėto Protokolo Nr. 22 dėl Danijos pozicijos 1 ir 2 straipsnius Danija nedalyvavo priimant Reglamentą (ES) 2018/1727. Todėl Danijai šis reglamentas nėra privalomas ar taikomas;

([3]) 2023 m. gruodžio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/2844 dėl teisminio bendradarbiavimo ir teisės kreiptis į teismą tarpvalstybinėse civilinėse, komercinėse ir baudžiamosiose bylose skaitmenizacijos, kuriuo iš dalies keičiami tam tikri teisminio bendradarbiavimo srities aktai, (OL L, 2023/2844, 2023 12 27, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) 2023 m. liepos 12 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/1543 dėl Europos įrodymų pateikimo orderių ir Europos įrodymų saugojimo orderių elektroniniams įrodymams baudžiamajame procese ir laisvės atėmimo bausmių vykdymui pasibaigus baudžiamajam procesui (OL L 191, 2023 7 28, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) 2024 m. lapkričio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/3011, dėl baudžiamojo proceso perdavimo (OL L, 2024/3011, 2024 12 18, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) 2019 m. lapkričio 29 d. Komisijos sprendimas (ES) 2019/2006 dėl Airijos dalyvavimo įgyvendinant Europos Parlamento ir Tarybos reglamentą (ES) 2018/1727 dėl Europos Sąjungos bendradarbiavimo baudžiamosios teisenos srityje agentūros (Eurojusto) (OL L 310, 2019 12 2, p. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) 2023 m. spalio 4 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/2131, kuriuo iš dalies keičiami Europos Parlamento ir Tarybos reglamentas (ES) 2018/1727 ir Tarybos sprendimas 2005/671/TVR, kiek tai susiję su skaitmeniniu keitimusi informacija terorizmo bylose, (OL L, 2023/2131, 2023 10 11, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([8]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis 2025 m. spalio 21 d. pateikė nuomonę;

(15) šiame reglamente numatytos priemonės atitinka pagal Reglamento (ES) 2018/1727 22c straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Decentralizuotos IT sistemos techninės specifikacijos

Decentralizuotos IT sistemos techninės specifikacijos, priemonės ir tikslai, nurodyti Reglamento (ES) 2018/1727 22b straipsnio 1 dalies a, b, c ir d punktuose, yra nustatomi šio reglamento I priede.

2 straipsnis

Skaitmeniniai procedūrų standartai

Reglamento (ES) 2018/1727 22a straipsnio 3 dalyje nurodyti skaitmeniniai procedūrų standartai, taikytini elektroninei komunikacijai per decentralizuotą IT sistemą, yra nustatomi šio reglamento II priede.

3 straipsnis

Pirštų atspaudų ir nuotraukų perdavimo techninės specifikacijos

Pirštų atspaudų ir nuotraukų perdavimo techninės specifikacijos ir formatas, nurodyti Reglamento (ES) 2018/1727 22a straipsnio 3 dalyje, yra nustatomi šio reglamento III priede.

4 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas pagal Sutartis privalomas visas ir tiesiogiai taikomas valstybėse narėse.

Priimta Briuselyje 2025 m. gruodžio 4 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

([8]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB, (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

I PRIEDAS

DECENTRALIZUOTOS IT SISTEMOS TECHNINĖS SPECIFIKACIJOS, PRIEMONĖS IR TIKSLAI

1. **Įvadas ir taikymo sritis**

Šiame priede nustatomos decentralizuotos IT sistemos, skirtos keistis informacija pagal Reglamentą (ES) 2018/1727, techninės specifikacijos, priemonės ir tikslai.

Dėl decentralizuoto šios IT sistemos pobūdžio galima tiesiogiai ir saugiai keistis duomenimis tarp kompetentingų nacionalinių institucijų ir Eurojusto.

2. **Terminų apibrėžtys**

Šiame priede vartojamų terminų apibrėžtys:

2.1. saugusis hipertekstų persiuntimo protokolas (angl. *Hypertext Transport Protocol Secure*) arba HTTPS – šifruotos komunikacijos ir saugaus ryšio kanalai;

2.2. kilmės neginčijamumas – savybė, reiškianti, kad duomenų vientisumas ir kilmė įrodomi tokiomis priemonėmis kaip skaitmeninis sertifikavimas, viešojo rakto infrastruktūra, elektroniniai parašai ir elektroniniai spaudai;

2.3. gavimo neginčijamumas – savybė, reiškianti, kad duomenų, siuntėjo siųstų numatytajam gavėjui, gavimas įrodomas tokiomis priemonėmis kaip skaitmeninis sertifikavimas, viešojo rakto infrastruktūra, elektroniniai parašai ir elektroniniai spaudai;

2.4. SOAP protokolas (angl. *Simple Object Access Protocol*) – kaip nustatyta Žiniatinklio konsorciumo standartuose, pranešimų siuntimo protokolo specifikacija, kuria nustatomi keitimosi struktūrizuota informacija, diegiant saityno paslaugas kompiuteriniuose tinkluose, reikalavimai;

2.5. REST (angl. *Representational State Transfer* – reprezentacinės būsenos perdavimas) – architektūrinis stilius, skirtas tinklinėms taikomosioms programoms kurti, grindžiamas bebūsenės kliento ir serverio komunikacijos modeliu, naudojant standartinius metodus operacijoms dėl išteklių, kurie įprastai perteikiami struktūrizuotais formatais, atlikti;

2.6. saityno paslauga – programinės įrangos sistema, sukurta sąveikiųjų įrenginių tarpusavio ryšiams tinkle palaikyti ir turinti sąsają, aprašytą kompiuterio apdorojamu formatu;

2.7. keitimasis duomenimis – keitimasis pranešimais ir dokumentais naudojantis decentralizuota IT sistema;

2.8. e. CODEX – Reglamento (ES) 2022/850 3 straipsnio 1 punkte apibrėžta sistema e. CODEX;

2.9. ES e. teisingumo baziniai žodynai – Reglamento (ES) 2022/850 priedo 4 punkte apibrėžti ES e. teisingumo baziniai žodynai;

2.10. „ebMS“ – „ebXML“ pranešimų paslauga – pranešimų siuntimo protokolas, sukurtas pagal OASIS sistemą, kuriuo sudaromos sąlygos saugiai, patikimai ir sąveikiai keistis elektroniniais verslo dokumentais naudojant SOAP protokolą. Taip remiama įmonių tarpusavio integracija įvairiose sistemose;

2.11. AS4–4-asis taikomumo pareiškimas (angl. *Applicability Statement* 4), OASIS standartas, kuriuo apibūdinamas „ebMS 3.0“; juo supaprastinamas saugus ir sąveikus įmonių tarpusavio pranešimų siuntimas, taikant atviruosius standartus, pvz., SOAP ir „WS-Security“;

2.12. atkūrimo laiko tikslas – ilgiausias priimtinas paslaugos atkūrimo po incidento laikas;

2.13. atkūrimo taško tikslas – didžiausias priimtinas sutrikus veikimui prarastų duomenų kiekis.

3. **Komunikacijos elektroninėmis priemonėmis metodai**

3.1. Decentralizuotoje IT sistemoje naudojami paslaugomis grindžiami komunikacijos metodai, kaip antai saityno paslaugos ar kiti daugkartinio naudojimo komponentai ir programinės įrangos sprendimai, skirti keistis pranešimais ir dokumentais.

3.2. Konkrečiai, decentralizuota IT sistema apima komunikaciją per e. CODEX prieigos taškus, kaip nustatyta Reglamento (ES) 2022/850 5 straipsnio 2 dalyje. Todėl, siekiant užtikrinti veiksmingą ir sąveikų tarpvalstybinį keitimąsi duomenimis, decentralizuota IT sistema palaiko ryšį per sistemą e. CODEX.

4. **Komunikacijos protokolai**

4.1. Decentralizuotoje IT sistemoje naudojami saugūs interneto protokolai, skirti:

a) komunikacijai decentralizuotoje IT sistemoje tarp kompetentingų institucijų ir Eurojusto;

b) komunikacijai su kompetentingų institucijų / teismų duomenų baze, kaip nurodyta 7.1 punkte.

4.2. Struktūrizuotų duomenų ir metaduomenų apibrėžimo ir perdavimo tikslais decentralizuotos IT sistemos komponentai grindžiami išsamiais ir visuotinai pripažintais pramonės standartais ir protokolais, kaip antai SOAP ir REST.

4.3. Perdavimo ir pranešimų siuntimo protokolų atžvilgiu decentralizuota IT sistema grindžiama standartais pagrįstais saugiais protokolais, tokiais kaip:

a) AS4 profilis, skirtas tarpvalstybiniam keitimuisi duomenimis, užtikrinant saugų ir patikimą pranešimų siuntimą taikant šifravimą ir užtikrinant neginčijamumą;

b) HTTPS/RESTful taikomųjų programų sąsajos, skirtos komunikacijai, kuriomis palaikomi JSON ir XML formatai;

c) SOAP protokolas, skirtas didelio patikimumo ryšiams, su integruotu „WS-Security“ tapatumo nustatymo ir šifravimo tikslais.

4.4. Sklandaus ir sąveikaus keitimosi duomenimis tikslu decentralizuotoje IT sistemoje naudojami komunikacijos protokolai atitinka aktualius sąveikumo standartus.

4.5. XML schemose naudojami (kai taikytina) aktualūs standartai ar žodynai, kurie yra reikalingi schemoje apibrėžtiems elementams ir tipams tinkamai patvirtinti. Tie standartai arba žodynai gali apimti:

a) ES e. teisingumo bazinį žodyną;

b) nesisteminius duomenų tipus (angl. *Unqualified Data Types*);

c) Europos Sąjungos kalbų kodų sąrašą.

4.6. Saugumo ir tapatumo patvirtinimo protokolų atžvilgiu decentralizuota IT sistema grindžiama standartais pagrįstais protokolais, tokiais kaip:

a) TLS (angl. *Transport Layer Security* – transporto lygmens saugumo) protokolas šifruotiems ir patvirtinto tapatumo ryšiams tinkluose, palaikant abipusį tapatumo nustatymą X.509 skaitmeniniais sertifikatais;

b) „Oauth / OpenID Connect“ (OIDC) saugiam tapatumo nustatymui ir leidimų suteikimui;

c) VRI (viešojo rakto infrastruktūra) ir skaitmeniniai parašai, skirti šifravimo raktui saugiai perduoti pranešimų vientisumui tikrinti, naudojant patikimų sertifikavimo institucijų išduotus skaitmeninius sertifikatus (X.509).

5. **Informacijos saugumo tikslai ir atitinkamos techninės priemonės**

5.1. Keičiantis informacija per decentralizuotą IT sistemą, techninės priemonės, kuriomis užtikrinami minimalieji informacinių technologijų saugumo standartai, apima:

a) priemones, kuriomis užtikrinamas informacijos konfidencialumas, be kita ko, naudojant saugius komunikacijos kanalus;

b) priemones, kuriomis užtikrinamas laikomų ir perduodamų duomenų vientisumas;

c) priemones, kuriomis užtikrinamas informacijos siuntėjo decentralizuotoje IT sistemoje kilmės neginčijamumas ir informacijos gavimo neginčijamumas;

d) priemones, kuriomis užtikrinamas saugumo įvykių registravimas laikantis pripažintų tarptautinių rekomendacijų dėl informacinių technologijų saugumo standartų ([1]);

e) priemones, kuriomis užtikrinamas naudotojo tapatumo patvirtinimas ir leidimo naudotojui suteikimas, ir priemones, kuriomis tikrinamas prie decentralizuotos IT sistemos prijungiamų sistemų tapatumas.

5.2. Decentralizuotos IT sistemos komponentais užtikrinama saugi komunikacija ir duomenų perdavimas naudojant šifravimą, viešojo rakto infrastruktūrą su skaitmeniniais sertifikatais, skirtais tapatumui nustatyti ir šifravimo raktui saugiai perduoti, saugius pranešimų siuntimo protokolus, kaip antai AS4 („ebMS“), „RESTful“ programų sąsajas ir SOAP protokolą, pranešimų konfidencialumui ir saugumui užtikrinti.

5.3. Kai decentralizuotoje IT sistemoje naudojamas TLS protokolas, naudojama naujausia stabili šio protokolo versija arba, jei tai neįmanoma, versija be žinomų saugumo spragų. Leidžiamas tik toks šifravimo rakto ilgis, kuriuo užtikrinamas pakankamas kriptografinio saugumo lygis, ir nenaudojami šifravimo algoritmų rinkiniai, kurie, kaip žinoma, yra nesaugūs arba pasenę.

5.4. Decentralizuotos IT sistemos veikimo tikslais naudojami VRI skaitmeniniai sertifikatai yra, kiek tik įmanoma, išduodami sertifikavimo institucijų, pripažintų kvalifikuotais patikimumo užtikrinimo paslaugų teikėjais pagal Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 ([2]). Įgyvendinamos priemonės, skirtos užtikrinti, kad tokie sertifikatai būtų naudojami tik pagal numatytąją paskirtį, užtikrinant reikiamo lygio patikimumą ir laikantis taikytinų Reglamento (ES) Nr. 910/2014 reikalavimų.

5.5. Decentralizuotos IT sistemos komponentai kuriami laikantis pritaikytosios ir standartizuotosios duomenų apsaugos principo ir įgyvendinamos tinkamos administracinės, organizacinės ir techninės priemonės aukštam kibernetinio saugumo lygiui užtikrinti.

5.6. Komisija kuria, plėtoja ir prižiūri bazinio sistemos modelio programinę įrangą laikydamasi Reglamente (ES) 2018/1725 nustatytų duomenų apsaugos reikalavimų ir principų. Komisijos teikiama bazinio sistemos modelio programine įranga sudaromos sąlygos valstybėms narėms atlikti savo pareigas atitinkamai pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 ([3]) ir Direktyvą (ES) 2016/680.

([1]) Nedarant poveikio registravimui saugumo tikslais, decentralizuotos IT sistemos komponentuose naudojamais registravimo mechanizmais atitinkamai galima užtikrinti atitiktį Reglamento (ES) 2018/1725 88 straipsnyje ir, kai taikytina, 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR, (OL L 119, 2016 5 4, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj) 25 straipsnyje nustatytiems reikalavimams.

([2]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB, (OL L 257, 2014 8 28, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Valstybės narės, naudojančios nacionalinę galinę sistemą, kuri nėra bazinio sistemos modelio programinė įranga, įgyvendina priemones, reikalingas užtikrinti, kad jų nacionalinės galinės sistemos atitiktų atitinkamai Reglamento (ES) 2016/679 ir Direktyvos (ES) 2016/680 reikalavimus.

5.8. Eurojustas įgyvendina priemones, reikalingas užtikrinti, kad jo galinė sistema arba jo įdiegtas bazinio sistemos modelio programinės įrangos plėtinys atitiktų reglamentų (ES) 2018/1725 ir (ES) 2018/1727 reikalavimus.

5.9. Valstybės narės ir Eurojustas, laikydamiesi atitinkamos savo politikos, nustato patikimus grėsmių aptikimo ir reagavimo į incidentus mechanizmus, skirtus decentralizuotai IT sistemai priklausančioms IT sistemoms, už kurias jie atsakingi, kad būtų užtikrintas savalaikis saugumo incidentų nustatymas, jų padarinių sušvelninimas ir atkūrimas po jų.

6. **Minimaliojo prieinamumo tikslai**

6.1. Eurojustas ir valstybės narės užtikrina, kad decentralizuotos IT sistemos komponentai, už kuriuos jie atsakingi, būtų prieinami visą parą ir visomis savaitės dienomis, o siektina techninio prieinamumo norma yra bent 98 % per metus, neskaitant planinės techninės priežiūros.

6.2. Komisija užtikrina, kad teismų duomenų bazė būtų prieinama visą parą ir visomis savaitės dienomis, o siektina techninio prieinamumo norma yra didesnė nei 99 % per metus, neskaitant planinės techninės priežiūros.

6.3. Darbo dienomis techninės priežiūros darbus, kiek tik įmanoma, planuojama atlikti nuo 20.00 iki 7.00 val. Vidurio Europos laiku (CET).

6.4. Valstybės narės praneša Komisijai, Eurojustui ir kitoms valstybėms narėms apie techninės priežiūros darbus tokia tvarka:

a) apie techninės priežiūros darbus, dėl kurių neprieinamumas gali būti iki 4 valandų, – prieš 5 darbo dienas;

b) apie techninės priežiūros darbus, dėl kurių neprieinamumas gali būti 4–12 valandų – prieš 10 darbo dienų;

c) apie techninės priežiūros darbus, dėl kurių neprieinamumas gali būti ilgiau kaip 12 valandų – prieš 30 darbo dienų.

6.5. Jei valstybės narės yra nustačiusios konkrečius reguliarios techninės priežiūros laikotarpius, jos informuoja Komisiją ir Eurojustą bei kitas valstybes nares apie laiką ir dieną (-as), kada planuojami tokie konkretūs reguliariosios techninės priežiūros laikotarpiai. Nukrypstant nuo 1 sakinyje nustatytų pareigų, jei decentralizuotos IT sistemos komponentai, už kuriuos valstybės narės yra atsakingos, taptų neprieinami tokiu konkrečiu reguliariosios techninės priežiūros laikotarpiu, jos galėtų nuspręsti nepranešti Komisijai apie kiekvieną tokį atvejį.

6.6. Įvykus netikėtam decentralizuotos IT sistemos komponentų, už kuriuos atsakingos valstybės narės, techniniam gedimui valstybės narės nedelsdamos informuoja Komisiją ir kitas valstybes nares apie šį gedimą ir, jei žinoma, apie numatomą atkūrimo laikotarpį.

6.7. Eurojustas praneša Komisijai ir valstybėms narėms apie techninės priežiūros darbus tokia tvarka:

a) apie techninės priežiūros darbus, dėl kurių neprieinamumas gali būti iki 4 valandų, – prieš 5 darbo dienas;

b) apie techninės priežiūros darbus, dėl kurių neprieinamumas gali būti 4–12 valandų – prieš 10 darbo dienų;

c) apie techninės priežiūros darbus, dėl kurių neprieinamumas gali būti ilgiau kaip 12 valandų – prieš 30 darbo dienų.

6.8. Jeigu Eurojustas yra nustatęs konkrečius reguliarios techninės priežiūros laikotarpius, jis informuoja Komisiją ir valstybes nares apie laiką ir dieną (-as), kada planuojami tokie konkretūs reguliariosios techninės priežiūros laikotarpiai. Nukrypstant nuo 1 sakinyje nustatytų pareigų, jei decentralizuotos IT sistemos komponentai, už kuriuos Eurojustas yra atsakingas, taptų neprieinami tokiu konkrečiu reguliariosios techninės priežiūros laikotarpiu, Eurojustas galėtų nuspręsti nepranešti Komisijai apie kiekvieną tokį atvejį.

6.9. Įvykus netikėtam decentralizuotos IT sistemos komponentų, už kuriuos atsakingas Eurojustas, techniniam gedimui, Eurojustas nedelsdamas informuoja Komisiją ir valstybes nares apie šį gedimą ir, jei žinoma, apie numatomą atkūrimo laikotarpį.

6.10. Įvykus netikėtam kompetentingų institucijų / teismų duomenų bazės techniniam gedimui, Komisija nedelsdama informuoja Eurojustą ir valstybes nares apie duomenų bazės neprieinamumą ir, jei žinoma, apie numatomą atkūrimo laikotarpį.

6.11. Sutrikus paslaugų teikimui valstybės narės ir Eurojustas užtikrina, kad paslauga būtų greitai atkurta, o duomenų praradimas minimalus, laikantis atkūrimo laiko tikslo ir atkūrimo taško tikslo.

6.12. Valstybės narės ir Eurojustas įgyvendina tinkamas priemones pirmiau nurodytiems prieinamumo tikslams pasiekti ir nustato veiksmingo reagavimo į incidentus procedūras.

7. **Kompetentingų institucijų / teismų duomenų bazė (CDB)**

7.1. Pagal Reglamento (ES) 2018/1727 22a straipsnį, decentralizuotoje IT sistemoje sudaromos sąlygos elektroninei komunikacijai tarp kompetentingų nacionalinių institucijų ir Eurojusto. Atsižvelgiant į kompetentingų nacionalinių institucijų ir Eurojusto pareigas keistis informacija pagal 21, 21a ir 22 straipsnius, taip pat į Eurojusto vaidmenį palengvinant ir remiant bet kokio savitarpio teisinės pagalbos ar tarpusavio pripažinimo prašymo pateikimą ir vykdymą pagal Reglamento (ES) 2018/1727 8 straipsnio 1 dalį, naudojantis decentralizuota IT sistema turi būti galima aiškiai nustatyti dalyvaujančių kompetentingų institucijų tapatybę. Todėl itin svarbu sukurti patikimą duomenų bazę kurioje informacija apie tas institucijas būtų saugoma decentralizuotos IT sistemos reikmėms.

7.2. Toje duomenų bazėje (CDB) struktūrizuotu formatu pateikiama ši informacija:

a) Reglamento (ES) 2018/1727 8 straipsnio 1, 3 ir 4 dalių, 21, 21a ir 22 straipsnių tikslais – informacija apie kompetentingas nacionalines institucijas, įskaitant nacionalinius korespondentus, kaip nustatyta to reglamento 20 straipsnyje, ir nacionalinius narius pagal to reglamento 7 straipsnį ([4]);

b) kai aktualu, informacija, reikalinga geografinėms ar esminėms kompetentingų institucijų kompetencijos sritims nustatyti, ar kiti aktualūs kriterijai, reikalingi jų kompetencijai nustatyti;

c) informacija, reikalinga tinkamam techninių pranešimų maršruto parinkimui decentralizuotoje IT sistemoje užtikrinti.

7.3. Komisija yra atsakinga už CDB sukūrimą, priežiūrą, veikimą ir veikimo palaikymą;

7.4. CDB sudaromos sąlygos valstybėms narėms ir Eurojustui atnaujinti šioje duomenų bazėje pateiktą informaciją, o decentralizuotoje IT sistemoje dalyvaujančioms kompetentingoms nacionalinėms institucijoms ir nacionaliniams nariams suteikiama galimybė programiškai susipažinti su informacija ir ją gauti;

7.5. prieiga prie CDB yra galima pagal bendrą komunikacijos protokolą, nepriklausomai nuo to, ar prie decentralizuotos IT sistemos prisijungusios kompetentingos institucijos naudoja nacionalinę galinę sistemą, ar bazinio sistemos modelio programinės įrangos diegtį;

7.6. valstybės narės užtikrina, kad į CDB įtraukta informacija apie jų kompetentingas institucijas, nurodyta 7.2 punkte, būtų išsami, tiksli ir atnaujinama.

([4]) Tai nedaro poveikio nacionalinio nario įgaliojimų delegavimui jo pavaduotojui, kitiems nacionalinio biuro darbuotojams ar įgaliotiems Eurojusto darbuotojams.

II PRIEDAS

SKAITMENINIAI PROCEDŪRŲ STANDARTAI

Reglamento (ES) 2022/850 3 straipsnio 9 punkte skaitmeniniai procedūrų standartai apibrėžti kaip veiklos procesų modelių ir duomenų schemų techninės specifikacijos, kuriomis nustatoma elektroninė duomenų, kuriais keičiamasi per sistemą e. CODEX, struktūra.

Šiame priede nustatomos veiklos procesų modelių techninės specifikacijos ir duomenų schemų techninės specifikacijos.

1. **Veiklos procesų modelių pagal Reglamentą (ES) 2018/1727 techninės specifikacijos**

Veiklos procesų modelių techninės specifikacijos nustatytos 1.1–1.5 punktuose. Jose apibrėžiami pagrindiniai aspektai, reikalingi elektroninei komunikacijai Reglamento (ES) 2018/1727 tikslais per decentralizuotą IT sistemą.

Decentralizuotoje IT sistemoje galima keistis informacija tik tarp valstybės narės kompetentingų nacionalinių institucijų ir tos valstybės narės nacionalinio nario.

1.1. *Keitimasis su Europos teisminiu kovos su terorizmu registru (CTR) susijusia informacija – Reglamento (ES) 2018/1727 21a straipsnis*

1.1.1. CTR duomenų perdavimo modelis

Kompetentinga nacionalinė institucija nacionaliniam nariui perduoda CTR skirtus duomenis apie su terorizmu susijusius procesus.

1.1.2. CTR duomenų gavimo modelis

Nacionalinis narys gauna CTR duomenis.

1.1.3. Sutikimo prašymo modelis

Nacionalinis narys prašo savo kompetentingos nacionalinės institucijos sutikimo.

1.1.4. Sutikimo prašymo gavimo modelis

Kompetentinga nacionalinė institucija gauna sutikimo prašymą.

1.1.5. Atsakymo į sutikimo prašymą siuntimo modelis

Kompetentinga nacionalinė institucija siunčia atsakymą į sutikimo prašymą.

1.1.6. Atsakymo į sutikimo prašymą gavimo modelis

Nacionalinis narys gauna atsakymą į sutikimo prašymą.

1.1.7. Informavimo apie sąsają modelis

Nacionalinis narys informuoja kompetentingą nacionalinę instituciją apie sąsają su kita byla.

1.1.8. CTR duomenų atnaujinimo modelis

Kompetentinga nacionalinė institucija savo atitinkamam nacionaliniam nariui perduoda duomenis, kuriuos reikia atnaujinti arba ištrinti.

1.1.9. Atnaujintų CTR duomenų gavimo modelis

Nacionalinis narys gauna CTR duomenis, kuriuos reikia atnaujinti arba ištrinti.

1.2. *Keitimasis su sunkiais nusikaltimais susijusia informacija – Reglamento (ES) 2018/1727 21 straipsnis*

1.2.1. Sunkių tarpvalstybinių nusikaltimų duomenų perdavimo modelis

Nacionalinė kompetentinga institucija perduoda Eurojustui duomenis apie sunkius tarpvalstybinius nusikaltimus.

1.2.2. Sunkių tarpvalstybinių nusikaltimų duomenų gavimo modelis

Nacionalinis narys gauna sunkių tarpvalstybinių nusikaltimų duomenis.

1.2.3. Sutikimo prašymo modelis

Nacionalinis narys prašo savo nacionalinės kompetentingos institucijos sutikimo.

1.2.4. Sutikimo prašymo gavimo modelis

Kompetentinga nacionalinė institucija gauna sutikimo prašymą.

1.2.5. Atsakymo į sutikimo prašymą siuntimo modelis

Kompetentinga nacionalinė institucija siunčia atsakymą į sutikimo prašymą.

1.2.6. Atsakymo į sutikimo prašymą gavimo modelis

Nacionalinis narys gauna atsakymą į sutikimo prašymą.

1.2.7. Informavimo apie sąsają modelis

Nacionalinis narys informuoja kompetentingą nacionalinę instituciją apie sąsają su kita byla.

1.2.8. Sunkių tarpvalstybinių nusikaltimų duomenų atnaujinimo modelis

Kompetentinga nacionalinė institucija savo atitinkamam nacionaliniam nariui perduoda duomenis, kuriuos reikia atnaujinti arba ištrinti.

1.2.9. Sunkių tarpvalstybinių nusikaltimų atnaujintų duomenų gavimo modelis

Nacionalinis narys gauna sunkių tarpvalstybinių nusikaltimų duomenis, kuriuos reikia atnaujinti arba ištrinti.

1.3. *Keitimasis bendra informacija*

1.3.1. Informacijos siuntimo modelis

Nacionalinis narys siunčia informaciją kompetentingai nacionalinei institucijai ir atvirkščiai.

1.3.2. Informacijos gavimo modelis

Kompetentinga nacionalinė institucija arba nacionalinis narys gauna informaciją.

1.3.3. Atsakymo į informaciją modelis

Kompetentinga nacionalinė institucija atsako į iš nacionalinio nario gautą informaciją arba atvirkščiai.

1.3.4. Atsakymo gavimo modelis

Nacionalinis narys gauna kompetentingos nacionalinės institucijos atsakymą.

1.3.5. Informacijos siuntimo modelis

Kompetentinga nacionalinė institucija siunčia informaciją nacionaliniam nariui.

1.3.6. Informacijos gavimo modelis

Nacionalinis narys gauna informaciją.

1.3.7. Atsakymo į informaciją modelis

Nacionalinis narys atsako į iš kompetentingos nacionalinės institucijos gautą informaciją.

1.3.8. Atsakymo gavimo modelis

Kompetentinga nacionalinė institucija gauna nacionalinio nario atsakymą.

1.4. *Pagalbos ir paramos teikimo vaidmuo – Reglamento (ES) 2018/1727 8 straipsnio 1 dalis*

Pastaba. Kai 1.5 punkte nurodyti pagalbos ir paramos modeliai apima keitimąsi Sąjungos teisės aktų teisminio bendradarbiavimo baudžiamosiose bylose srityje nustatytos formos pranešimais, tuose modeliuose, kai įmanoma, turi būti naudojamos atitinkamos struktūrizuotos duomenų pateiktys ir XML schemos, parengtos pagal tuos aktus, pavyzdžiui, tos, kurios nustatytos Reglamento (ES) 2023/2844 ar kitų atitinkamų aktų įgyvendinimo tikslais.

1.5. *Pagalbos arba paramos prašymo modelis*

1.5.1. Pagalbos arba paramos prašymo perdavimo modelis

Nacionalinė kompetentinga institucija perduoda pagalbos prašymą arba paramos prašymą savo atitinkamam nacionaliniam nariui.

1.5.2. Pagalbos arba paramos prašymo gavimo modelis

Nacionalinis narys gauna pagalbos arba paramos prašymą ir jį persiunčia prašomosios valstybės narės nacionaliniam nariui, nedalyvaujančiam sistemoje JUDEX.

1.5.3. Pagalbos arba paramos prašymo persiuntimo kompetentingai nacionalinei institucijai modelis

Prašomosios valstybės narės nacionalinis narys nusiunčia prašymą savo atitinkamai kompetentingai nacionalinei institucijai.

1.5.4. Pagalbos arba paramos prašymo gavimo modelis

Kompetentinga nacionalinė institucija gauna pagalbos arba paramos prašymą.

1.5.5. Atsakymo į pagalbos arba paramos prašymą siuntimo modelis

Kompetentinga nacionalinė institucija prašomosios valstybės narės nacionaliniam nariui siunčia atsakymą į prašymą arba su tuo prašymu susijusią informaciją.

1.5.6. Atsakymo į pagalbos arba paramos prašymą gavimo modelis

Nacionalinis narys iš kompetentingos nacionalinės institucijos gauna atsakymą į pagalbos ar paramos prašymą arba su tuo prašymu susijusią informaciją ir tuo pasidalija su prašančiosios valstybės narės nacionaliniu nariu, nedalyvaujančiu sistemoje JUDEX.

1.5.7. Atsakymo į pagalbos arba paramos prašymą modelis

Prašančiosios valstybės narės nacionalinis narys atsako į pagalbos arba paramos prašymą, gautą iš kompetentingos nacionalinės institucijos, arba pasidalija su tuo prašymu susijusia informacija.

1.5.8. Atsakymo gavimo modelis

Kompetentinga nacionalinė institucija gauna atsakymą į pagalbos ar paramos prašymą arba su tuo prašymu susijusią informaciją.

2. **Duomenų schemų techninės specifikacijos**

Techninės specifikacijos, kuriomis turės būti remiamasi rengiant XML schemų apibrėžtis (XSD) skaitmenizacijai pagal Reglamentą (ES) 2018/1727, yra nustatytos šio priedo 2.1 ir 2.2 punktuose. Siekiant pateikti išsamų šių schemų rengimo aprašą, šiomis specifikacijomis apibrėžiami pagrindiniai komponentai ir kita aktuali informacija.

Aprašas yra bendro pobūdžio, kad, norint keisti ir plėtoti parengtas XML schemų apibrėžtis, šių specifikacijų nereikėtų iš esmės keisti.

Šios specifikacijos taikomos teisės aktų nustatytai schemų formai, pridėtai prie Reglamento (ES) 2018/1727, bet kokiems iš anksto parengtiems pranešimams arba laisvos formos pranešimams, naudojamiems keičiantis informacija pagal tą reglamentą.

2.1. *Bendrieji aspektai*

Visoms teiktinoms schemoms taikomos šios nuostatos:

2.1.1. Versijų rengimas

Turi būti įtrauktas versijos atributas, kuris palengvina schemos versijų valdymą ir suteikia galimybę atnaujinti schemą vėlesnėse iteracijose pagal veiklos poreikius. Versijos atributas nurodo, ar, diegiant naujas funkcijas arba patobulinimus, nauja versija yra suderinama atgaline data.

2.1.2. Schemos deklaravimas ir metaduomenys

— XML schemoje naudojami (kai taikytina) aktualūs standartai ar žodynai, reikalingi e. CODEX sąveikumui užtikrinti, kurie yra būtini schemoje apibrėžtiems elementams ir tipams tinkamai patvirtinti. Tai gali apimti:

  — ES e. teisingumo bazinį žodyną;

  — nesisteminius duomenų tipus;

  — Europos Sąjungos kalbų kodų sąrašą.

— Be to, kai taikytina, į schemą gali būti įtraukti atitinkami ETSI standartai, kad būtų galima naudoti juose pateiktas apibrėžtis.

2.1.3. Anotacijos ir dokumentavimas

— **Anotacijos**. Prie kiekvieno schemos elemento paprastai pridedamos anotacijos. Anotacijose pateikiama žmonėms suprantamos informacijos apie elementą, dažnai aiškiai ir glaustai apibrėžiant jo paskirtį arba naudojimą.

2.1.4. Naudojimas ir pritaikomumas

Schema turi atitikti a–d punktuose nustatytas taisykles:

a) **Modulinė struktūra.** Kiekvienas skyrius turi būti parengtas konkrečiai funkcijai atlikti ir jį turi būti galima pakartotinai naudoti arba savarankiškai pritaikyti. Taip schema turi būti lengvai pritaikoma įvairiems naudojimo atvejams.

b) **Išplečiamumas.** Schema parengiama tokia, kad, jei ateityje reikėtų papildomos informacijos, būtų galima įtraukti naujų elementų ar atributų. Tai pasiekiama naudojant pasirenkamuosius elementus ir sekas, kurias galima plėsti nepertraukiant esamų įdiegčių.

c) **Pritaikoma struktūra.** Schema parengiama tokia, kad prireikus būtų galima pridėti ar keisti elementus ar duomenų tipus. Schemos struktūra turi būti tokia, kad, norint pakeisti reikalavimus, nereikėtų esminių pertvarkų.

d) **Pasirenkamieji elementai.** Schemos elementai gali būti pažymėti kaip pasirenkamieji – tai reiškia, kad, priklausomai nuo konkrečių aplinkybių, jie gali būti įtraukiami arba neįtraukiami.

Schema parengiama tokia, kad būtų palaikomas struktūrizuotų duomenų rinkimas pagal konkrečius prašymus.

2.1.5. Pakeitimai

Schemos projektui turi būti būdingas lankstumas, modulinis principas ir lengvas pritaikomumas. Sudėtingi tipai ir pasirenkamieji elementai turi būti įtraukti į projektą taip, kad jis būtų tinkamas įvairiems scenarijams, o kartu jį būtų lengva keisti ir plėtoti.

2.2. *Keitimasis struktūrizuotais duomenimis*

Struktūrizuoti duomenys, nurodyti 2.2.1 ir 2.2.2 punktuose, teikiami pagal Reglamento (ES) 2018/1727 22a straipsnio 3 dalį. Pagal schemą taip pat turi būti galima nurodyti duomenų rinkinius, kurie ateityje atnaujinant duomenis bus ištrinti.

2.2.1. Europos teisminio kovos su terorizmu registro duomenys

Toliau pateiktomis duomenų schemos techninėmis specifikacijomis nustatomas struktūrinis schemos kūrimo XML formatu pagrindas.

a) Aukščiausio lygmens skyrius:

šis aukščiausio lygmens skyrius atitinka Reglamento (ES) 2018/1727 III priede nustatytą informaciją, skirtą Europos teisminiam kovos su terorizmu registrui (CTR).

b) Pranešimo struktūra:

CTR duomenų struktūrą sudaro elementų seka; joje mažų mažiausiai turi būti:

i) informacija, skirta fizinių asmenų tapatybei nustatyti:

— pavardė (-ės);

— vardas (-ai);

— slapyvardžiai;

— gimimo data;

— gimimo vieta (miestas ir valstybė);

— pilietybė ar pilietybės;

— tapatybės nustatymo dokumentas (rūšis ir dokumento numeris);

— lytis;

— gyvenamoji vieta;

ii) informacija, skirta juridinių asmenų tapatybei nustatyti:

— įmonės pavadinimas;

— teisinė forma;

— pagrindinės buveinės vieta;

iii) informacija, skirta tiek fizinių, tiek juridinių asmenų tapatybei nustatyti:

— telefono numeriai;

— e. pašto adresai;

— informacija apie sąskaitas bankuose ar kitose finansų įstaigose;

— statusas procese;

iv) informacija apie nusikaltimą:

— informacija apie juridinius asmenis, dalyvaujančius rengiant ar vykdant teroristinį nusikaltimą;

— teisinė nusikaltimo kvalifikacija pagal nacionalinę teisę;

— taikytina sunkaus nusikaltimo forma pagal I priede nurodytą sąrašą;

— priklausymas teroristinei grupei;

— terorizmo rūšis, pavyzdžiui, džihadistas, separatistas, kairysis ar dešinysis;

— trumpa bylos santrauka;

v) informacija apie nacionalinį procesą:

— tokio proceso statusas;

— atsakinga prokuratūra;

— bylos numeris;

— oficialaus teismo proceso pradžios data;

— sąsajos su kitomis aktualiomis bylomis;

vi) papildomos informacijos laukas (laisvos formos tekstas)

vii) išankstinio leidimo kodas.

2.2.2. Duomenys, perduodami pagal Reglamento (ES) 2018/1727 21 straipsnį

a) Reglamento (ES) 2018/1727 21 straipsnio 4 dalis, jungtinių tyrimų grupių (JTG) sudarymas

i) Aukščiausio lygmens skyrius
Šis aukščiausio lygmens skyrius atitinka Reglamento (ES) Nr. 2018/1727 21 straipsnio 4 dalyje nurodytą informaciją apie jungtinių tyrimų grupių sudarymą.

ii) Pranešimo struktūra
duomenų struktūrą sudaro elementų seka; joje mažų mažiausiai turi būti:

— Už baudžiamąjį procesą atsakinga nacionalinė teisminė institucija

— Nacionalinis baudžiamojo proceso registracijos numeris

— Baudžiamojo proceso statusas

— Tiriamos nusikalstamos veikos

— Kitos byloje dalyvaujančios valstybės

— Ar byla jau remiama Eurojusto?

— Jei taip, nurodyti Eurojusto bylos identifikacinį numerį.

— Jei ne, ar tai yra paramos prašymas?

— Ar byla remiama Europolo?

— Jei taip, ar naudojama operatyvinė darbo grupė (OTF) ir (arba) Saugaus keitimosi informacija tinklo programa (SIENA)?

— Susitarimas dėl jungtinės tyrimų grupės (JTG):

— dalyvaujančios valstybės

— JTG dalyviai (nacionalinės tyrimus vykdančios institucijos)

— Baudžiamojo proceso, dėl kurio dirba JTG, nacionalinis registracijos numeris

— Pasirašymo data

— Trukmė

— Tiriamos nusikalstamos veikos

— Trumpa bylos santrauka

— Pagrindiniai įtariamieji baudžiamajame procese, dėl kurio dirba JTG (vardas, pavardė, gimimo data ir vieta ir galbūt kitų aktualių ir reikalingų kategorijų duomenys pagal II priedą)

— JTG darbo rezultatai:

— Sunkumai ar vėlavimai:

— sudarant JTG

— prašant pateikti įrodymus ar dalijantis jais JTG

— tariantis dėl bendros baudžiamojo persekiojimo strategijos ar ją įgyvendinant

— JTG įrodymų priimtinumas, nepriimtinumas ar vertinimas nacionaliniame procese

— Teismo proceso rezultatas (sėkmingas ar nesėkmingas baudžiamasis persekiojimas ir apkaltinamieji ar išteisinamieji nuosprendžiai)

iii) Išankstinio leidimo kodas

b) Reglamento (ES) 2018/1727 21 straipsnio 5 dalis, sunkios ir sudėtingos bylos

i) Aukščiausio lygmens skyrius

Šis aukščiausio lygmens skyrius atitinka Eurojusto reglamento 21 straipsnio 5 dalyje nurodytą informaciją, t. y. apie sunkias ir sudėtingas bylas.

ii) Pranešimo struktūra

duomenų struktūrą sudaro elementų seka; joje mažų mažiausiai turi būti:

— Už baudžiamąjį procesą atsakinga nacionalinė teisminė institucija

— Nacionalinis baudžiamojo proceso registracijos numeris

— Baudžiamojo proceso statusas

— Tiriamos nusikalstamos veikos

— Kitos byloje dalyvaujančios valstybės

— Ar byla jau remiama Eurojusto?

— Jei taip, nurodyti Eurojusto bylos identifikacinį numerį.

— Jei ne, ar tai yra paramos prašymas?

— Ar byla remiama Europolo?

— Jei taip, ar naudojama operatyvinė darbo grupė ir (arba) programa SIENA?

— Taikytina sunkaus nusikaltimo forma

— Organizuotos nusikalstamos grupės dalyvavimas

— Mafijos tipas

— Tarpvalstybinė organizuota nusikalstama grupė

— Padariniai ES lygmeniu

— Pagrindiniai įtariamieji baudžiamajame procese (vardas, pavardė, gimimo data ir vieta ir galbūt kitų aktualių ir reikalingų kategorijų duomenys pagal II priedą)

— Trumpa bylos santrauka

— Kitos dalyvaujančios valstybės

— Valstybės, su kuriomis bendradarbiavimas jau pradėtas

— Dalyvaujančios kitos valstybės kompetentingos institucijos

— Naudojamos teisminio bendradarbiavimo priemonės

— Išsiųstų / gautų prašymų skaičius

— Susijusių tyrimų buvimas

— Valstybės, su kuriomis numatoma pradėti bendradarbiavimą / valstybės, kurios gali būti paveiktos

— Reikalingo bendradarbiavimo pobūdis (pvz., ekstradicija, įrodymų rinkimas, kitoks bendradarbiavimas)

— Susijusių tyrimų buvimas

iii) Išankstinio leidimo kodas

c) Reglamento (ES) 2018/1727 21 straipsnio 6 dalies a punktas, jurisdikcijos kolizijos

i) Aukščiausio lygmens skyrius

Šis aukščiausio lygmens skyrius atitinka Reglamento (ES) 2018/1727 21 straipsnio 6 dalies a punkte nurodytą informaciją, t. y. jurisdikcijos kolizijas

ii) Pranešimo struktūra

duomenų struktūrą sudaro elementų seka; joje mažų mažiausiai turi būti:

— Už baudžiamąjį procesą atsakinga nacionalinė teisminė institucija

— Nacionalinis baudžiamojo proceso registracijos numeris

— Baudžiamojo proceso statusas (pvz., tyrimas, baudžiamasis persekiojimas, teismo procesas)

— Tiriamos nusikalstamos veikos

— Kitos byloje dalyvaujančios valstybės

— Ar byla jau remiama Eurojusto?

— Jei taip, nurodyti Eurojusto bylos identifikacinį numerį.

— Jei ne, ar tai yra paramos prašymas?

— Ar byla remiama Europolo?

— Jei taip, ar naudojama operatyvinė darbo grupė ir (arba) programa SIENA?

— Kitos dalyvaujančios valstybės

— Kitos valstybės kompetentingos nacionalinės institucijos, jei žinoma

— Baudžiamojo proceso kitoje valstybėje nacionalinis registracijos numeris

— Proceso kitoje valstybėje etapas, jei žinoma

— Pozityvi ar negatyvi kolizija

— Esama ar galima kolizija

— Koordinavimo veikla, kurios jau imtasi (pvz., konsultacijos pagal Tarybos pamatinį sprendimą 2009/948/TVR ([1]))

— Trumpa bylos santrauka

— Pagrindiniai bendri įtariamieji (vardas, pavardė, gimimo data ir vieta ir galbūt kitų aktualių ir reikalingų kategorijų duomenys pagal II priedą)

iii) Išankstinio leidimo kodas

d) 21 straipsnio 6 dalies b punktas, kontroliuojamasis gabenimas

i) Aukščiausio lygmens skyrius
Šis aukščiausio lygmens skyrius atitinka Reglamento (ES) 2018/1727 21 straipsnio 6 dalies b punkte nurodytą informaciją (kontroliuojamasis gabenimas)

ii) Pranešimo struktūra
duomenų struktūrą sudaro elementų seka; joje mažų mažiausiai turi būti:

— Už baudžiamąjį procesą atsakinga nacionalinė teisminė institucija

— Nacionalinis baudžiamojo proceso registracijos numeris

— Baudžiamojo proceso statusas (pvz., tyrimas, baudžiamasis persekiojimas, teismo procesas)

— Tiriamos nusikalstamos veikos

— Kitos byloje dalyvaujančios valstybės

— Ar byla jau remiama Eurojusto?

— Jei taip, nurodyti Eurojusto bylos identifikacinį numerį.

— Jei ne, ar tai yra paramos prašymas?

— Ar byla remiama Europolo?

— Jei taip, ar naudojama operatyvinė darbo grupė ir (arba) programa SIENA?

— Kitos dalyvaujančios valstybės

— Kilmės / tranzito / paskirties valstybė

— Kitų valstybių kompetentingos nacionalinės institucijos

— Susijusių tyrimų kitose valstybėse buvimas

([1]) 2009 m. lapkričio 30 d. Tarybos pamatinis sprendimas 2009/948/TVR dėl jurisdikcijos įgyvendinimo kolizijų baudžiamuosiuose procesuose prevencijos ir sprendimo (OL L 328, 2009 12 15, p. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Pristatomų prekių rūšis (pvz., narkotikai ir jų tipas / pinigai / ginklai / cigaretės / kita)

— Kontroliuojamojo gabenimo būklė (pvz., planuojamas, vykdomas, užbaigtas)

— Kontroliuojamojo gabenimo (jei jis jau įvykdytas) rezultatas

— Naudojama teisminio bendradarbiavimo priemonė

— Pagrindiniai bendri įtariamieji (vardas, pavardė, gimimo data ir vieta ir galbūt kitų aktualių ir reikalingų kategorijų duomenys pagal II priedą)

iii) Išankstinio leidimo kodas

e) Reglamento (ES) 2018/1727 21 straipsnio 6 dalies c punktas, pasikartojančios problemos, susijusios su teisminio bendradarbiavimo priemonėmis

i) Aukščiausio lygmens skyrius
Šis aukščiausio lygmens skyrius atitinka Reglamento (ES) 2018/1727 21 straipsnio 6 dalies c punkte nurodytą informaciją (pasikartojančios problemos, susijusios su teisminio bendradarbiavimo priemonėmis)

ii) Pranešimo struktūra
duomenų struktūrą sudaro elementų seka; joje mažų mažiausiai turi būti:

— Už baudžiamąjį procesą atsakinga nacionalinė teisminė institucija

— Nacionalinis baudžiamojo proceso registracijos numeris

— Baudžiamojo proceso statusas (pvz., tyrimas, baudžiamasis persekiojimas, teismo procesas)

— Tiriamos nusikalstamos veikos

— Kitos byloje dalyvaujančios valstybės

— Ar byla jau remiama Eurojusto?

— Jei taip, nurodyti Eurojusto bylos identifikacinį numerį.

— Jei ne, ar tai yra paramos prašymas?

— Ar byla remiama Europolo?

— Jei taip, ar naudojama operatyvinė darbo grupė ir (arba) programa SIENA?

— Kitos dalyvaujančios valstybės

— Kompetentingos nacionalinės institucijos, jei žinoma

— Ar institucija veikia kaip išduodančioji, ar kaip vykdančioji institucija

— Susijusi teisminio bendradarbiavimo priemonė (pvz., Europos arešto orderis, Europos tyrimo orderis, turto įšaldymas ir konfiskavimas)

— Atitinkamas konkretus prašymas (t. y. kokia tyrimo priemonė, kokio pobūdžio įšaldymas, ar Europos arešto orderis skirtas teismo nuosprendžiui, ar baudžiamajam persekiojimui vykdyti)

— Atsisakymas arba pasikartojantys sunkumai

— Jeigu atsisakoma bendradarbiauti – kokiu konkrečiu pagrindu remiamasi?

— Trumpas problemos aprašymas

— Kitos nacionalinės institucijos, kurias paveikė ta pati problema, jei yra

iii) Išankstinio leidimo kodas

2.3. *Išankstinio leidimo kodai*

Dalydamosi duomenimis su Eurojustu per sistemą JUDEX, kompetentingos nacionalinės institucijos, naudodamos išankstinio leidimo kodus, nurodo tolesnį duomenų tvarkymą, prieigą ir perdavimą, nustačius sąsają. Išankstinio leidimo kodais nurodoma, ar (ir kokiu mastu) su nustatyta sąsaja susijusia informacija gali būti dalijamasi su kitomis kompetentingomis nacionalinėmis institucijomis, kitomis Sąjungos agentūromis ir įstaigomis, trečiosiomis valstybėmis ar tarptautinėmis organizacijomis.

2.4. *Iš anksto nustatyti pranešimai*

Iš anksto nustatyti pranešimai – tai Reglamente (ES) 2018/1727 nustatyto keitimosi informacija, kurio konkrečios formos tame teisės akte nenumatyta, išraiška. Tokių pranešimų tipai ir skaičius nustatomi atliekant veiklos ir techninę analizę.

XLM schemų apibrėžtys (XSD), skirtos iš anksto nustatytiems pranešimams, suformuluojamos taip, kad būtų užtikrintas nuoseklumas, struktūra ir atitiktis veiklos poreikiams.

Toms schemoms taikomos šios nuostatos:

a) šios schemos aukščiausio lygmens skyrius pavadinamas pagal apibrėžiamą konkretų pranešimo tipą;

b) šioje struktūroje papildomai pridedami ir apibrėžiami konkretaus tipo pranešimui reikalingi laukai, užtikrinant tinkamą duomenų elementų pateiktį.

2.5. *Laisvos formos pranešimai*

Laisvos formos pranešimai – tai keitimosi informacija išraiška, teikianti galimybę pateikti nestruktūruotą ar iš dalies struktūruotą turinį; tai teikia lankstumo, o kartu atitinka reguliavimo reikalavimus ir veiklos poreikius. Laisvos formos pranešimų XLM schemos apibrėžtis (XSD) turi būti suformuluota taip, kad būtų užtikrintas nuoseklumas ir tinkamas formatavimas.

Toms schemoms taikomos šios nuostatos:

a) schemos aukščiausio lygmens skyrius pavadinamas pagal apibrėžiamą konkretų laisvos formos pranešimo tipą;

b) toje schemoje apibrėžiama reikiama laisvos formos pranešimo struktūra, o kartu paliekama galimybė prireikus išdėstyti elementus tinkama tvarka;

c) šioje struktūroje papildomai pridedami ir apibrėžiami konkretaus tipo laisvos formos pranešimui reikalingi laukai, užtikrinant tinkamą duomenų elemento pateiktį.

III PRIEDAS

PIRŠTŲ ATSPAUDŲ IR NUOTRAUKŲ TECHNINĖS SPECIFIKACIJOS

Prie pranešimų, kuriais keičiamasi per decentralizuotą IT sistemą, gali būti pridedami priedai, įskaitant Nacionalinio standartų ir technologijų instituto (NIST) rinkmenas su pirštų atspaudais ir nuotraukomis, laikantis 1 ir 2 punktuose nustatytų techninių specifikacijų.

1. **Pirštų atspaudai**

Pirštų atspaudai, kuriais gali būti pasidalijama su Eurojustu tam, kad būtų patikimai nustatyta asmenų, dėl kurių vyksta su teroristiniais nusikaltimais susijęs baudžiamasis procesas, tapatybė, turi atitikti šias sąlygas:

a) pirštų atspaudai pateikiami vienoje rinkmenoje, kurioje yra pirštų atspaudų skaitmeniniai atvaizdai (pirštų atspaudų NIST rinkmena), ir teikiami laikantis 2015 m. atnaujinto standarto ANSI/NIST-ITL 1-2011 (arba naujesnės jo redakcijos);

b) pirštų atspaudų NIST rinkmeną sudaro iki dešimties atskirų pirštų atspaudų: ritintų, plokščiųjų arba abiejų rūšių;

c) visi pirštų atspaudai yra paženklinti;

d) pirštų atspaudai imami skenuojant vietoje arba naudojant rašalą ir popierių, jei rašalu nudažyti pirštų atspaudai popieriuje buvo nuskenuoti išlaikant reikiamą skiriamąją gebą ir tokią pat kokybę;

e) pirštų atspaudų NIST rinkmenoje galima įtraukti papildomos informacijos, pavyzdžiui, pirštų atspaudų registravimo sąlygas ir asmens pirštų atspaudų atvaizdų gavimo metodą;

f) pirštų atspaudų duomenų nominalioji skiriamoji geba yra 500 arba 1 000 ppi ([1]) (priimtinas nuokrypis +/– 10 ppi) su 256 pilkais pustoniais;

g) Naudotinas pirštų atspaudų glaudinimo algoritmas atitinka Nacionalinio standartų ir technologijų instituto (NIST) rekomendacijas. 500 ppi skiriamosios gebos pirštų atspaudų duomenys glaudinami taikant WSQ algoritmą (ISO/IEC 19794-5:2005). 1 000 ppi skiriamosios gebos pirštų atspaudų duomenys glaudinami taikant JPEG 2000 atvaizdų glaudinimo standartą (ISO/IEC 15444-1) ir kodavimo sistemą. Tikslinis glaudinimo santykis yra 15:1.

2. **Nuotraukos**

Nuotraukos, kuriomis gali būti pasidalijama su Eurojustu tam, kad būtų patikimai nustatyta asmenų, dėl kurių vyksta su teroristiniais nusikaltimais susijęs baudžiamasis procesas, tapatybė, turi atitikti šias sąlygas:

a) fotografinėje rinkmenoje (nuotraukos NIST rinkmenoje) pateikiamas tik vienas veido atvaizdas; jis teikiamas laikantis standarto ANSI/NIST-ITL 1-2011, atnaujinto 2015 m., ar bet kurios prieinamos naujesnės šio standarto redakcijos;

b) nuotraukos yra pilkumo tonų, spalvotos arba artimosios infraraudonosios spektro srities;

c) nuotraukų kokybė atitinka ISO/IEC 19794-5:2011 priekinio veido atvaizdo tipo (angl. *frontal image type*) arba bet kokios naujesnės versijos vaizdo reikalavimus;

d) nuotraukos NIST rinkmenoje galima įtraukti papildomos informacijos, įskaitant datą, kada padarytas atvaizdas;

([1]) Pikselių skaičius colyje.

e) portreto orientacijos nuotraukos yra ne mažesnės kaip 600 x 800 pikselių ir ne didesnės kaip 1 200 x 1 600 pikselių raiškos;

f) veidas nuotraukoje užima tokią kadro dalį, kad tarp akių centrų būtų ne mažiau kaip 120 pikselių;

g) naudojamas nuotraukų glaudinimo algoritmas atitinka Nacionalinio standartų ir technologijų instituto (NIST) rekomendacijas. Nuotraukos glaudinamos tik vieną kartą, naudojant JPG (ISO/IEC 10918) arba JPEG 2000 (ISO/IEC 15444) vaizdų glaudinimo standartą ir kodavimo sistemą, taikant didesnį kaip 20:1 leidžiamą vaizdo glaudinimo santykį.