2025/2447

5.12.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/2447,

4. detsember 2025,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1727 rakenduseeskirjad teabe turvalise töötlemise ja edastamise detsentraliseeritud IT-süsteemi loomise ja kasutamise tehniliste kirjelduste, meetmete ja muude nõuete osas

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

Võttes arvesse Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määrust (EL) 2018/1727 ([1]) Euroopa Liidu Kriminaalõigusalase Koostöö Ameti (Eurojust) kohta ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsus 2002/187/JSK, eriti selle artikli 22a lõiget 3 ning artikli 22b lõike 1 punkte a, b, c ja d,

ning arvestades järgmist:

(1) Määruses (EL) 2018/1727 on sätestatud Eurojusti uue digitaalse sisetaristu raamistik ja nähtud ette liikmesriikide pädevate asutuste ja Eurojusti vahelise detsentraliseeritud turvalise digitaalse sidesüsteemi loomine.

(2) Turvalist digitaalset sidet peetakse detsentraliseeritud IT-süsteemi kaudu. Selleks et luua detsentraliseeritud IT-süsteem, tuleb kehtestada tehnilised kirjeldused, milles määratakse kindlaks sidemeetodid ja sideprotokollid, tehnilised meetmed, millega tagatakse infoturbe miinimumstandardid ja turvalisus ning kõnealuse süsteemi käideldavuse miinimumeesmärgid.

(3) Vastavalt määrusele (EL) 2018/1727 artikli 22a lõikele 1 peaks detsentraliseeritud IT-süsteem koosnema liikmesriikide ja Eurojusti IT-süsteemidest ja neid omavahel siduvatest koostalitlevatest e-CODEXi pääsupunktidest. Detsentraliseeritud IT-süsteemi tehnilised kirjeldused ja muud nõuded, mis sätestatakse käesolevas määruses, peaksid seda raamistikku arvesse võtma.

(4) Detsentraliseeritud IT-süsteemi pääsupunktid peaksid põhinema Euroopa Parlamendi ja nõukogu määruse (EL) 2022/850 ([2]) artikli 3 punktis 3 määratletud volitatud e-CODEXi pääsupunktidel.

(5) Detsentraliseeritud IT-süsteemi rakendatakse suuremas e-CODEXil põhinevas detsentraliseeritud IT-süsteemis, mida nimetatakse õigusvaldkonna digitaalseks andmevahetussüsteemiks (JUDEX). Seepärast tuleb tagada tulemuslik teabevahetus horisontaalsete arengute kohta.

(6) Liikmesriigid ja Eurojust võivad vastavalt määruse (EL) 2018/1727 artikli 22a lõikele 4 otsustada riikliku süsteemi asemel kasutada oma tagasüsteemina komisjoni arendatud etalonteostuse tarkvara. Koostalitlusvõime tagamiseks peaksid nii riiklikud IT-süsteemid kui ka etalonteostuse tarkvara vastama samadele tehnilistele kirjeldustele ja nõuetele.

(7) Terroriaktide ja raskete organiseeritud kuritegude andmeid tuleks edastada struktureeritud viisil, et parandada teabe kvaliteeti ja asjakohasust ning tagada, et teavet saab tõhusamalt integreerida Eurojusti kohtuasjade haldamise süsteemi ja paremini kontrollida, võrreldes seda kõnealuses süsteemis juba säilitatava teabega. Tuleks määrata kindlaks selliste sõrmejäljeandmete ja fotode edastamise vorming ja tehnilised kirjeldused, mis võidakse edastada Eurojustile selleks, et tuvastada isikud, kelle suhtes on algatatud terroriaktiga seotud kriminaalmenetlus.

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

([2]) Euroopa Parlamendi ja nõukogu 30. mai 2022. aasta määrus (EL) 2022/850, milles käsitletakse arvutipõhist süsteemi piiriüleseks elektrooniliseks andmevahetuseks tsiviil- ja kriminaalasjades tehtava õigusalase koostöö valdkonnas (e-CODEXi süsteem) ning millega muudetakse määrust (EL) 2018/1726 (ELT L 150, 1.6.2022, lk 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust hõlbustab õigusalase koostöö taotluste, sealhulgas vastastikuse tunnustamise põhimõtet rakendavate õigusaktide alusel tehtud taotluste või otsuste väljaandmist ja täitmist ning aitab sellele kaasa. Liikmesriikide pädevad asutused peaksid saama detsentraliseeritud IT-süsteemi kaudu küsida Eurojustilt abi ja paluda tal tegevust koordineerida.

(9) Selleks et tagada tulemuslikkus ja kooskõla, on oluline, et määruse (EL) 2018/1727 alusel kehtestatavad tehnilised kirjeldused vastavad Euroopa Parlamendi ja nõukogu määruste (EL) 2023/2844, ([3]) (EL) 2023/1543 ([4]) ja (EL) 2024/3011 ([5]) alusel kehtestatud tehnilistele kirjeldustele ning tulevastele digitaliseerimismeetmele, mis on olulised seoses Eurojusti ülesandega toetada liikmesriikide pädevaid asutusi.

(10) Detsentraliseeritud IT-süsteemi kaudu tuleks võimaldada Eurojusti ja liikmesriikide pädevate asutuste vahel ka igasugune muu side, nagu teabe edastamine teabe töötlemise tulemuste kohta, sealhulgas seoste kohta kohtuasjade haldamise süsteemis juba säilitatavate kohtuasjadega vastavalt määruse (EL) 2018/1727 artiklile 22, kui Eurojust toimib omal algatusel, või sellise teabe edastamine, mis on Eurojustile edastatud genotsiidi, inimsusvastaste kuritegude, sõjakuritegude ja nendega seotud kuritegude kohta tõendite säilitamiseks, analüüsimiseks ja hoiustamiseks vastavalt kõnealuse määruse artikli 4 lõike 1 punktile j.

(11) Eurojustiga on konsulteeritud määruse (EL) 2018/1727 artikli 22a lõike 3 kohaselt tagamaks, et käesolevas määruses võetakse arvesse Eurojusti operatiivvajadusi.

(12) Euroopa Liidu lepingule ja Euroopa Liidu toimimise lepingule lisatud protokolli nr 21 (Ühendkuningriigi ja Iirimaa seisukoha kohta vabadusel, turvalisusel ja õigusel rajaneva ala suhtes) artikli 4 kohaselt teatas Iirimaa 9. septembri 2019. aasta kirjas soovist nõustuda määrusega (EL) 2018/1727 ja olla sellega seotud. See osalemine kinnitati komisjoni otsusega (EL) 2019/2006 ([6]). Määrust (EL) 2018/1727 on muudetud Euroopa Parlamendi ja nõukogu määrusega (EL) 2023/2131, ([7]) et võimaldada luua Eurojusti ja liikmesriikide pädevate asutuste vahelised turvalised digitaalsed sidekanalid ning nimetatud muutmismäärus on käesoleva määruse õiguslik alus. Kuna Iirimaa ei teatanud oma soovist osaleda määruse (EL) 2023/2131 vastuvõtmisel ja kohaldamisel ega ole teatanud oma soovist kõnealuse määrusega nõustuda ja olla sellega seotud, ei ole protokolli nr 21 artiklite 1 ja 2 ning artikli 4a lõike 1 kohaselt määrus (EL) 2023/2131 Iirimaa suhtes siduv ja seda ei kohaldata Iirimaal. Seetõttu ei osale Iirimaa käesoleva määruse vastuvõtmisel.

(13) Euroopa Liidu lepingule ja Euroopa Liidu toimimise lepingule lisatud protokolli nr 22 (Taani seisukoha kohta) artiklite 1 ja 2 kohaselt ei osalenud Taani määruse (EL) 2018/1727 vastuvõtmisel. Seepärast ei ole käesolev määrus Taani suhtes siduv ega kohaldatav.

([3]) Euroopa Parlamendi ja nõukogu 13. detsembri 2023. aasta määrus (EL) 2023/2844, mis käsitleb digipööret õigusalase koostöö ning piiriüleste tsiviil-, kaubandus- ja kriminaalasjadega seotud õiguskaitse kättesaadavuse vallas ning millega muudetakse teatavaid õigusalast koostööd käsitlevaid õigusakte (ELT L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Euroopa Parlamendi ja nõukogu määrus (EL) 2023/1543, 12. juuli 2023, mis käsitleb Euroopa andmeesitamismäärust ja Euroopa andmesäilitamismäärust elektrooniliste tõendite hankimiseks kriminaalmenetluses ja kriminaalmenetluse järgsete vabadusekaotuslike karistuste täitmisele pööramiseks (ELT L 191, 28.7.2023, lk 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Euroopa Parlamendi ja nõukogu 27. november 2024. aasta määrus (EL) 2024/3011, mis käsitleb kriminaalmenetluse üleandmist (ELT L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Komisjoni 29. novembri 2019. aasta otsus (EL) 2019/2006, mis käsitleb Iirimaa osalemist Euroopa Parlamendi ja nõukogu määruses (EL) 2018/1727 Euroopa Liidu Kriminaalõigusalase Koostöö Ameti (Eurojust) kohta (ELT L 310, 2.12.2019, lk 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Euroopa Parlamendi ja nõukogu 4. oktoobri 2023. aasta määrus (EL) 2023/2131, millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) 2018/1727 ning nõukogu otsust 2005/671/JSK terrorismijuhtumeid käsitleva digitaalse teabevahetuse osas (ELT L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([8]) artikli 42 lõikele 1 konsulteeriti Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 21. oktoobril 2025.

(15) Käesoleva määrusega ettenähtud meetmed on kooskõlas määruse (EL) 2018/1727 artikli 22c kohaselt asutatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Detsentraliseeritud IT-süsteemi tehnilised kirjeldused

Määruse (EL) 2018/1727 artikli 22b lõike 1 punktides a, b, c ja d osutatud detsentraliseeritud IT-süsteemi tehnilised kirjeldused, meetmed ja eesmärgid sätestatakse käesoleva määruse I lisas.

Artikkel 2

Digitaalsed protsessistandardid

Digitaalsed protsessistandardid, mida kohaldatakse määruse (EL) 2018/1727 artikli 22a lõikes 3 osutatud elektroonilise side korral, sätestatakse käesoleva määruse II lisas.

Artikkel 3

Sõrmejälgede ja fotode edastamise tehnilised kirjeldused

Sõrmejälgede ja fotode edastamise tehnilised kirjeldused ja vorming, millele on osutatud määruse (EL) 2018/1727 artikli 22a lõikes 3, sätestatakse käesoleva määruse III lisas.

Artikkel 4

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja liikmesriikides vahetult kohaldatav kooskõlas aluslepingutega.

Brüssel, 4. detsember 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

([8]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

I LISA

DETSENTRALISEERITUD IT-SÜSTEEMI TEHNILISED KIRJELDUSED, MEETMED JA EESMÄRGID

1. **Sissejuhatus ja kohaldamisala**

Käesolevas lisas sätestatakse määruses (EL) 2018/1727 osutatud teabevahetuseks kasutatava detsentraliseeritud IT-süsteemi tehnilised kirjeldused, meetmed ja eesmärgid.

IT-süsteemi detsentraliseeritud olemus võimaldab liikmesriikide pädevate asutuste ja Eurojusti vahel otse ja turvaliselt andmeid vahetada.

2. **Mõisted**

Käesolevas lisas kasutatakse järgmisi mõisteid:

2.1. „HTTPS“ (Hypertext Transfer Protocol Secure) ehk turvaline hüperteksti edastuse protokoll – krüpteeritud side ja turvalised sidekanalid;

2.2. „päritolu salgamise vääramine“ – meetmed, mille abil tõendatakse andmete terviklust ja päritolu, kasutades selliseid meetodeid nagu digitaalne sertifitseerimine, avaliku võtme taristu ning e-allkirjad ja e-templid;

2.3. „kättesaamise salgamise vääramine“ – meetmed, mille abil andmete lähetajale tõendatakse andmete kättesaamist andmete kavandatud saaja poolt, kasutades selliseid meetodeid nagu digitaalne sertifitseerimine, avaliku võtme taristu, e-allkirjad ja e-templid;

2.4. „SOAP“ (Simple Object Access Protocol) ehk lihtne objektipöörduse protokoll – arvutivõrkudes veebiteenuste rakendamisel struktureeritud teabe vahetamiseks kasutatav veebikonsortsiumi standardite kohane sõnumivahetus-protokoll;

2.5. „REST“ (Representational State Transfer) ehk esitusoleku siire – veebirakenduste kavandamise arhitektuuristiil, mis põhineb olekukontrollita kliendi-serveri sidemudelil ja mille puhul kasutatakse standardmeetodeid toimingute tegemiseks ressurssidega, mis on tavaliselt struktureeritud vormingus;

2.6. „veebiteenus“ – tarkvarasüsteem, mis on loodud masinatevahelise koostalitlusvõimelise võrgupõhise suhtluse toetamiseks ja millel on masintöödeldavas vormingus kirjeldatud liides;

2.7. „andmevahetus“ – sõnumite ja dokumentide vahetamine detsentraliseeritud IT-süsteemi kaudu;

2.8. „e-CODEX“ – määruse (EL) 2022/850 artikli 3 punktis 1 määratletud e-CODEXi süsteem;

2.9. „ELi e-õiguskeskkonna põhisõnastik“ – määruse (EL) 2022/850 lisa punktis 4 määratletud ELi e-õiguskeskkonna põhisõnastik;

2.10. „ebMS“ (ebXML Message Service) – OASISe raames välja töötatud sõnumivahetusprotokoll, mis võimaldab e-äri dokumentide turvalist, usaldusväärset ja koostalitlusvõimelist vahetamist SOAPi abil; toetab ettevõtjatevahelist integreerimist eri süsteemide vahel;

2.11. „AS4“ (Applicability Statement 4) – OASISe standard, mis kirjeldab ebMS 3.0 ning lihtsustab turvalist ja koostalitlusvõimelist ettevõtjatevahelist sõnumivahetust, kasutades avatud standardeid, nagu SOAP ja WS-Security;

2.12. „taaste sihtkestus“ – maksimaalne aktsepteeritav aeg, mis võib intsidendi järel teenuse taastamiseks kuluda;

2.13. „taaste sihtseis“ – maksimaalne aktsepteeritav andmekadu tõrke korral.

3. **Elektroonilise teabevahetuse meetodid**

3.1. Detsentraliseeritud IT-süsteem kasutab sõnumite ja dokumentide vahetamiseks teenusepõhiseid teabevahetusmeetodeid, näiteks veebiteenuseid või muid taaskasutatavaid komponente ja tarkvaralahendusi.

3.2. Täpsemalt hõlmab detsentraliseeritud IT-süsteem teabevahetust e-CODEXi süsteemi pääsupunktide kaudu, nagu on sätestatud määruse (EL) 2022/850 artikli 5 lõikes 2. Seega peab detsentraliseeritud IT-süsteem toimiva ja koostalitlusvõimelise piiriülese andmevahetuse tagamiseks toetama teabevahetust e-CODEXi süsteemi kaudu.

4. **Andmevahetusprotokollid**

4.1. Detsentraliseeritud IT-süsteemis kasutatakse turvalisi internetiprotokolle:

a) pädevate asutuste ja Eurojusti vaheliseks teabevahetuseks detsentraliseeritud IT-süsteemis,

b) pädevate asutuste / kohtute andmebaasi vaheliseks teabevahetuseks vastavalt punktile 7.1.

4.2. Struktureeritud andmete ja metaandmete määratlemiseks ja edastamiseks kasutatavad detsentraliseeritud IT-süsteemi komponendid põhinevad põhjalikel ja üldtunnustatud valdkondlikel standarditel ja protokollidel, nagu SOAP ja REST.

4.3. Transpordi- ja sõnumivahetusprotokollide osas põhineb detsentraliseeritud IT-süsteem turvalistel standardipõhistel protokollidel, näiteks:

a) piiriüleseks andmevahetuseks AS4 Profile, mis tagab turvalise ja usaldusväärse sõnumivahetuse krüpteerimise ja salgamise vääramise abil;

b) JSON- ja XML-vorminguid toetavaks teabevahetuseks HTTPS/RESTful rakendusliidesed;

c) väga usaldusväärseks teabevahetuseks SOAP, mis hõlmab autentimiseks ja krüpteerimiseks protokolli WS-Security.

4.4. Sujuva ja koostalitlusvõimelise andmevahetuse tagamiseks vastavad detsentraliseeritud IT-süsteemi kasutatavad andmevahetusprotokollid asjakohastele koostalitlusvõime standarditele.

4.5. Vajaduse korral kasutatakse XML-skeemides asjakohaseid standardeid või sõnastikke, et võimaldada skeemis määratletud elementide ja tüüpide nõuetekohast valideerimist. Nende standardite või sõnastike hulka võivad kuuluda:

a) ELi e-õiguskeskkonna põhisõnastik;

b) kvalifitseerimata andmetüübid;

c) Euroopa Liidu keelekoodide loend.

4.6. Turbe- ja autentimisprotokollide osas põhineb detsentraliseeritud IT-süsteem standardipõhistel protokollidel, näiteks:

a) TLS (transpordikihi turve), mis võimaldab võrkudes krüpteeritud ja autenditud teabevahetust, toetades vastastikust autentimist X.509 digisertifikaatide kaudu;

b) OAuth/OpenID Connect (OIDC) turvaliseks autentimiseks ja volitamiseks;

c) PKI (avaliku võtme taristu) ja digiallkirjad, mis võimaldavad turvalist võtmekehtestust ja sõnumite tervikluse kontrollimist, kasutades usaldusväärsete sertifitseerimisasutuste väljastatud digisertifikaate (X.509).

5. **Infoturbe eesmärgid ja sellega seotud tehnilised meetmed**

5.1. Tehnilised meetmed, millega tagatakse detsentraliseeritud IT-süsteemi kaudu teabe vahetamisel infotehnoloogilise turvalisuse miinimumstandardid, hõlmavad järgmist:

a) meetmed, millega tagatakse teabe konfidentsiaalsus, muu hulgas turvaliste sidekanalite kasutamise kaudu;

b) meetmed, millega tagatakse andmete terviklus nii jõudeoleku kui ka edastamise ajal;

c) meetmed, millega tagatakse detsentraliseeritud IT-süsteemis teabe saatja päritolu salgamise vääramine ja teabe kättesaamise salgamise vääramine;

d) meetmed, millega tagatakse turvasündmuste logimine vastavalt tunnustatud rahvusvahelistele soovitustele infotehnoloogia turvastandardite kohta; ([1])

e) meetmed, millega tagatakse kasutajate autentimine ja volitamine, ning meetmed, millega kontrollitakse detsentraliseeritud IT-süsteemiga ühendatud süsteemide identiteeti.

5.2. Detsentraliseeritud IT-süsteemi komponentidega tagatakse turvaline side ja andmeedastus, kasutades krüpteerimist, avaliku võtme taristut koos digisertifikaatidega autentimiseks ja turvaliseks võtmekehtestuseks ning turvalisi sõnumivahetusprotokolle nagu AS4 (ebMS), RESTful rakendusliidesed ja SOAP, et säilitada sõnumite konfidentsiaalsus ja terviklus.

5.3. Kui detsentraliseeritud IT-süsteemis kasutatakse TLS-i, tuleb kasutada protokolli uusimat stabiilset versiooni või kui see ei ole võimalik, siis sellist versiooni, millel ei ole teadaolevaid turvanõrkusi. Lubatud on ainult võtmepikkused, mis tagavad krüptoturvalisuse piisava taseme, ja teadaolevalt ebaturvalisi või taunitavaid šifrikomplekte ei tohi kasutada.

5.4. PKI digisertifikaadid, mida kasutatakse detsentraliseeritud IT-süsteemi käituseks, peaks võimaluse korral väljastama sertifitseerimisasutus, mis on Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 ([2]) kohaselt tunnustatud kvalifitseeritud usaldusteenuse osutaja. Tuleb rakendada meetmeid, millega tagatakse, et kõnealuseid sertifikaate kasutatakse ainult ettenähtud eesmärkidel, nõuetekohasel usalduse tasemel ja kooskõlas määruses (EL) nr 910/2014 sätestatud nõuetega.

5.5. Detsentraliseeritud IT-süsteemi komponendid töötatakse välja lõimitud ja vaikimisi andmekaitse põhimõtte kohaselt ning küberturvalisuse kõrge taseme tagamiseks rakendatakse asjakohaseid haldus-, korralduslikke ja tehnilisi meetmeid.

5.6. Komisjon kavandab, arendab ja hooldab etalonteostuse tarkvara kooskõlas määruses (EL) 2018/1725 sätestatud andmekaitsenõuete ja -põhimõtetega. Komisjoni pakutav etalonteostuse tarkvara võimaldab liikmesriikidel täita Euroopa Parlamendi ja nõukogu määrusest (EL) 2016/679 ([3]) ja direktiivist (EL) 2016/680 tulenevaid kohustusi (vastavalt kohaldatavusele).

([1]) Ilma et see piiraks turvaotstarbelist logimist, võimaldavad detsentraliseeritud IT-süsteemi komponentide kasutatavad logimismehhanismid asjakohasel juhul tagada vastavuse määruse (EL) 2018/1725 artiklis 88 ja vajaduse korral Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiivi (EL) 2016/680 (mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT L 119, 4.5.2016, lk 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj)) artiklis 25 sätestatud nõuetele.

([2]) Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Liikmesriigid, kes kasutavad etalonteostuse tarkvarast erinevat riiklikku tagasüsteemi, rakendavad vajalikke meetmeid, et tagada selle süsteemi vastavus määruse (EL) 2016/679 ja direktiivi (EL) 2016/680 nõuetele (vastavalt kohaldatavusele).

5.8. Eurojust rakendab vajalikke meetmeid tagamaks, et tema tagasüsteem või tema kasutatav etalonteostuse tarkvara eksemplar vastab määruste (EL) 2018/1725 ja (EL) 2018/1727 nõuetele.

5.9. Liikmesriigid ja Eurojust loovad oma vastutusalasse kuuluvate ja detsentraliseeritud IT-süsteemi osaks olevate IT-süsteemide jaoks tugevad ohtude avastamise ja intsidentidele reageerimise mehhanismid, et tagada turvaintsidentide õigeaegne tuvastamine ja leevendamine ning neist taastumine vastavalt ettenähtud korrale.

6. **Käideldavuse miinimumeesmärgid**

6.1. Eurojust ja liikmesriigid tagavad oma vastutusalasse kuuluvate detsentraliseeritud IT-süsteemi komponentide alalise ööpäevaringse käideldavuse, kusjuures tehnilise käideldavuse iga-aastane sihtmäär on vähemalt 98 %, välja arvatud korraline hooldus.

6.2. Komisjon tagab kohtute andmebaasi alalise ööpäevaringse käideldavuse, kusjuures tehnilise käideldavuse iga-aastane sihtmäär on vähemalt 99 %, välja arvatud korraline hooldus.

6.3. Võimaluse korral kavandatakse hooldustööd tööpäevadel ajavahemikku 20.00–7.00 Kesk-Euroopa aja järgi.

6.4. Liikmesriigid teavitavad komisjoni, Eurojusti ja teisi liikmesriike hooldustöödest järgmiselt:

a) 5 tööpäeva ette, kui hooldustööd võivad põhjustada kuni 4-tunnise katkestuse;

b) 10 tööpäeva ette, kui hooldustööd võivad põhjustada 4–12-tunnise katkestuse;

c) 30 tööpäeva ette, kui hooldustööd võivad põhjustada kuni enam kui 12-tunnise katkestuse.

6.5. Kui liikmesriigid on kehtestanud korralise hoolduse perioodid, teavitavad nad komisjoni, Eurojusti ja teisi liikmesriike sellise kindlaksmääratud korralise hoolduse kavandatud päeva(de)st ja kellaajast. Erandina esimeses lauses sätestatud kohustustest võivad liikmesriigid otsustada, et ei teavita komisjoni iga kord, kui nende vastutusalasse kuuluvad detsentraliseeritud IT-süsteemi komponendid muutuvad sellise kindlaksmääratud korralise hoolduse perioodil käideldamatuks.

6.6. Liikmesriigi vastutusalasse kuuluva detsentraliseeritud IT-süsteemi komponendi ootamatu tehnilise tõrke korral teavitab liikmesriik komisjoni ja teisi liikmesriike viivitamata nii tõrkest kui ka eeldatavast taaste ajakavast, kui see on teada.

6.7. Eurojust teavitab komisjoni ja liikmesriike hooldustöödest järgmiselt:

a) 5 tööpäeva ette, kui hooldustööd võivad põhjustada kuni 4-tunnise katkestuse;

b) 10 tööpäeva ette, kui hooldustööd võivad põhjustada 4–12-tunnise katkestuse;

c) 30 tööpäeva ette, kui hooldustööd võivad põhjustada kuni enam kui 12-tunnise katkestuse.

6.8. Kui Eurojust on kehtestanud korralise hoolduse perioodid, teavitab ta komisjoni ja liikmesriike sellise kindlaksmääratud korralise hoolduse kavandatud päeva(de)st ja kellaajast. Erandina esimeses lauses sätestatud kohustustest võib Eurojust otsustada, et ei teavita komisjoni iga kord, kui tema vastutusalasse kuuluvad detsentraliseeritud IT-süsteemi komponendid muutuvad kindlaksmääratud korralise hoolduse perioodil käideldamatuks.

6.9. Eurojusti vastutusalasse kuuluva detsentraliseeritud IT-süsteemi komponendi ootamatu tehnilise tõrke korral teavitab Eurojust komisjoni ja liikmesriike viivitamata nii tõrkest kui ka eeldatavast taaste ajakavast, kui see on teada.

6.10. Pädevate asutuste / kohtute andmebaasi ootamatu tehnilise tõrke korral teavitab komisjon viivitamata Eurojusti ja liikmesriike andmebaasi tõrkest ja eeldatavast taaste ajakavast, kui see on teada.

6.11. Teenuse katkemise korral tagavad liikmesriigid ja Eurojust, et vastavalt taaste sihtkestusele ja taaste sihtseisule taastatakse teenus kiiresti ja andmekadu on minimaalne.

6.12. Liikmesriigid ja Eurojust rakendavad eespool kirjeldatud käideldavuse eesmärkide saavutamiseks asjakohaseid meetmeid ja kehtestavad menetlused intsidentidele tulemuslikuks reageerimiseks.

7. **Pädevate asutuste / kohtute andmebaas**

7.1. Määruse (EL) 2018/1727 artikli 22a kohaselt peab detsentraliseeritud IT-süsteem võimaldama elektroonilist sidet liikmesriikide pädevate asutuste ja Eurojusti vahel. Pidades silmas artiklite 21, 21a ja 22 kohast liikmesriikide pädevate asutuste ja Eurojusti vahelise teabevahetuse kohustust, aga ka määruse (EL) 2018/1727 artikli 8 lõike 1 kohast Eurojusti rolli hõlbustada vastastikuse õigusabi taotluste ja vastastikuse tunnustamise taotluste väljaandmist ja täitmist ning aidata sellele kaasa, peavad pädevad asutused olema selgelt identifitseeritavad, kui nad kasutavad detsentraliseeritud IT-süsteemi. Seepärast on oluline luua detsentraliseeritud IT-süsteemi jaoks usaldusväärne andmebaas, mis sisaldab teavet nende asutuste kohta.

7.2. Pädevate asutuste / kohtute andmebaas sisaldab struktureeritud kujul järgmist teavet:

a) määruse (EL) 2018/1727 artikli 8 lõigete 1, 3 ja 4, artikli 21, artikli 21a ja artikli 22 kohaldamiseks teave liikmesriigi pädevate asutuste, sealhulgas kõnealuse määruse artikliga 20 ette nähtud riigisiseste kontaktisikute ja kõnealuse määruse artikliga 7 ette nähtud liikmesriigi liikmete ([4]) kohta;

b) asjakohasel juhul teave, mis on vajalik et teha kindlaks pädevate asutuste pädevuse geograafiline või valdkondlik ulatus, või muud asjakohased kriteeriumid, mis on vajalikud, et teha kindlaks asutuste pädevus;

c) teave, mis on vajalik sõnumite nõuetekohaseks tehniliseks marsruutimiseks detsentraliseeritud IT-süsteemi raames.

7.3. Komisjon vastutab pädevate asutuste / kohtute andmebaasi arendamise, hooldamise, käitamise ja toetamise eest;

7.4. pädevate asutuste / kohtute andmebaas võimaldab liikmesriikidel ja Eurojustil seal teavet ajakohastada ning detsentraliseeritud IT-süsteemis osalevatel liikmesriikide pädevatel asutustel ja liikmesriigi liikmetel sellele teabele programmi abil juurde pääseda ja seda välja otsida;

7.5. juurdepääs pädevate asutuste / kohtute andmebaasile peab olema võimalik üldise sideprotokolli kaudu, sõltumata sellest, kas detsentraliseeritud IT-süsteemiga ühendatud pädevad asutused kasutavad riiklikku tagasüsteemi või etalonteostuse tarkvara;

7.6. liikmesriigid tagavad, et punktis 7.2 osutatud teave nende pädevate asutuste kohta on pädevate asutuste / kohtute andmebaasis täielik, täpne ja ajakohastatud.

([4]) See ei piira liikmesriigi liikme volituste delegeerimist tema asetäitjale, teistele riikliku büroo töötajatele või Eurojusti volitatud töötajatele.

II LISA

DIGITAALSED PROTSESSISTANDARDID

Määruse (EL) 2022/850 artikli 3 punktis 9 on digitaalne protsessistandard määratletud kui tehnilised kirjeldused, mis käsitlevad äriprotsessi mudeleid ja andmeskeeme, milles määratakse kindlaks e-CODEXi süsteemi kaudu vahetatavate andmete elektrooniline struktuur.

Käesolevas lisas sätestatakse äriprotsessi mudelite ja andmeskeemide tehnilised kirjeldused.

1. **Äriprotsessi mudelite tehnilised kirjeldused vastavalt määrusele (EL) 2018/1727**

Äriprotsessi mudelite tehnilised kirjeldused on sätestatud punktides 1.1–1.5. Neis määratakse kindlaks peamised aspektid, mis on vajalikud, et võimaldada määruse (EL) 2018/1727 kohaldamiseks vajalikku elektroonilist sidet detsentraliseeritud IT-süsteemi kaudu.

Detsentraliseeritud IT-süsteem peab võimaldama vahetada teavet ainult teatava liikmesriigi pädevate asutuste ja kõnealuse liikmesriigi liikme vahel.

1.1. *Määruse (EL) 2018/1727 artikkel 21a: Euroopa terrorismivastase võitluse registriga (terrorismivastase võitluse register) seotud teabevahetus*

1.1.1. Terrorismivastase võitluse registri andmete edastamise mudel

Liikmesriigi pädev asutus edastab terrorismivastase võitluse registri jaoks ettenähtud andmed terrorismiga seotud menetluse kohta liikmesriigi liikmele.

1.1.2. Terrorismivastase võitluse registri andmete saamise mudel

Liikmesriigi liige saab terrorismivastase võitluse registri andmed.

1.1.3. Nõusoleku taotlemise mudel

Liikmesriigi liige taotleb oma liikmesriigi pädevalt asutuselt nõusolekut.

1.1.4. Nõusolekutaotluse saamise mudel

Liikmesriigi pädev asutus saab nõusolekutaotluse.

1.1.5. Nõusolekutaotlusele vastuse saatmise mudel

Liikmesriigi pädev asutus saadab nõusolekutaotlusele vastuse.

1.1.6. Nõusolekutaotlusele vastuse saamise mudel

Liikmesriigi liige saab nõusolekutaotluse vastuse.

1.1.7. Seosest teavitamise mudel

Liikmesriigi liige teavitab liikmesriigi pädevat asutust seosest teise juhtumiga.

1.1.8. Terrorismivastase võitluse registri andmete ajakohastamise mudel

Liikmesriigi pädev asutus edastab andmed, mida tuleb ajakohastada või mis tuleb kustutada, oma liikmesriigi liikmele.

1.1.9. Terrorismivastase võitluse registri ajakohastatud andmete saamise mudel

Liikmesriigi liige saab terrorismivastase võitluse registri andmed, mida tuleb ajakohastada või mis tuleb kustutada.

1.2. *Määruse (EL) 2018/1727 artikkel 21: raskete kuritegudega seotud teabevahetus*

1.2.1. Piiriülese mõõtmega raske kuriteo andmete edastamise mudel

Liikmesriigi pädev asutus edastab piiriülese mõõtmega raske kuriteo andmed Eurojustile.

1.2.2. Piiriülese mõõtmega raske kuriteo andmete saamise mudel

Liikmesriigi liige saab piiriülese mõõtmega raske kuriteo andmed.

1.2.3. Nõusoleku taotlemise mudel

Liikmesriigi liige taotleb oma liikmesriigi pädevalt asutuselt nõusolekut.

1.2.4. Nõusolekutaotluse saamise mudel

Liikmesriigi pädev asutus saab nõusolekutaotluse.

1.2.5. Nõusolekutaotlusele vastuse saatmise mudel

Liikmesriigi pädev asutus saadab nõusolekutaotlusele vastuse.

1.2.6. Nõusolekutaotlusele vastuse saamise mudel

Liikmesriigi liige saab nõusolekutaotluse vastuse.

1.2.7. Seosest teavitamise mudel

Liikmesriigi liige teavitab liikmesriigi pädevat asutust seosest teise juhtumiga.

1.2.8. Piiriülese mõõtmega raske kuriteo andmete ajakohastamise mudel

Liikmesriigi pädev asutus edastab andmed, mida tuleb ajakohastada või mis tuleb kustutada, oma liikmesriigi liikmele.

1.2.9. Piiriülese mõõtmega raske kuriteo ajakohastatud andmete saamise mudel

Liikmesriigi liige saab piiriülese mõõtmega raske kuriteo andmed, mida tuleb ajakohastada või mis tuleb kustutada.

1.3. *Üldise teabe vahetamine*

1.3.1. Teabe saatmise mudel

Liikmesriigi liige saadab teabe liikmesriigi pädevale asutusele või vastupidi.

1.3.2. Teabe saamise mudel

Liikmesriigi pädev asutus või liikmesriigi liige saab teabe.

1.3.3. Teabele vastamise mudel

Liikmesriigi pädev asutus vastab teabele, mille ta on saanud liikmesriigi liikmelt, või vastupidi.

1.3.4. Vastuse saamise mudel

Liikmesriigi liige saab vastuse liikmesriigi pädevalt asutuselt.

1.3.5. Teabe saatmise mudel

Liikmesriigi pädev asutus saadab teabe liikmesriigi liikmele.

1.3.6. Teabe saamise mudel

Liikmesriigi liige saab teabe.

1.3.7. Teabele vastamise mudel

Liikmesriigi liige vastab liikmesriigi pädevalt asutuselt saadud teabele.

1.3.8. Vastuse saamise mudel

Liikmesriigi pädev asutus saab liikmesriigi liikmelt vastuse.

1.4. *Määruse (EL) 2018/1727 artikli 8 lõige 1: hõlbustamine ja kaasaaitamine*

Märkus. Juhul kui punktis 1.5 kirjeldatud hõlbustamise ja kaasaitamise mudelid hõlmavad kriminaalasjades tehtava õigusalase koostöö valdkonnas liidu õigusaktidega kehtestatud kohustuslike vormide vahetamist, peavad mudelid võimaluse korral kasutama asjakohast struktureeritud andmete esitust ja kõnealuste õigusaktide jaoks väljatöötatud XML-skeeme, näiteks neid, mis on kehtestatud määruse (EL) 2023/2844 või muude asjakohaste õigusaktide rakendamiseks.

1.5. *Hõlbustamise või kaasaaitamise taotluse mudel*

1.5.1. Hõlbustamise või kaasaaitamise taotluse edastamise mudel

Liikmesriigi pädev asutus edastab hõlbustamise või kaasaaitamise taotluse oma liikmesriigi liikmele.

1.5.2. Hõlbustamise või kaasaaitamise taotluse saamise mudel

Liikmesriigi liige saab hõlbustamise või kaasaaitamise taotluse ja saadab selle väljaspool JUDEXit edasi taotluse saanud liikmesriigi liikmele.

1.5.3. Hõlbustamise või kaasaaitamise taotluse liikmesriigi pädevale asutusele edasisaatmise mudel

Taotluse saanud liikmesriigi liige saadab taotluse oma liikmesriigi pädevale asutusele.

1.5.4. Hõlbustamise või kaasaaitamise taotluse saamise mudel

Liikmesriigi pädev asutus saab hõlbustamise või kaasaaitamise taotluse.

1.5.5. Hõlbustamise või kaasaaitamise taotlusele vastuse saatmise mudel

Liikmesriigi pädev asutus saadab vastuse või taotlust puudutava teabe taotluse saanud liikmesriigi liikmele.

1.5.6. Hõlbustamise või kaasaaitamise taotlusele vastuse saamise mudel

Liikmesriigi liige saab liikmesriigi pädevalt asutuselt hõlbustamise või kaasaaitamise taotluse vastuse või taotlust puudutava teabe ja jagab seda väljaspool JUDEXit taotluse esitanud liikmesriigi liikmega.

1.5.7. Hõlbustamise või kaasaaitamise taotlusele vastamise mudel

Taotluse esitanud liikmesriigi liige vastab liikmesriigi pädevalt asutuselt saadud hõlbustamise või kaasaaitamise taotlust puudutavale teabele või jagab seda teavet.

1.5.8. Vastuse saamise mudel

Liikmesriigi pädev asutus saab vastuse või teabe, mis puudutab hõlbustamise või kaasaaitamise taotlust.

2. **Andmeskeemide tehnilised kirjeldused**

Tehnilised kirjeldused, mis tuleb võtta määruse (EL) 2018/1727 digitaliseerimisel XML skeemi definitsioonide väljatöötamise aluseks, on sätestatud käesoleva lisa punktides 2.1 ja 2.2. Tehnilistes kirjeldustes määratakse kindlaks peamised komponendid ja muu teave, milles esitatakse põhjalik kirjeldus kõnealuste skeemide loomiseks.

See kirjeldus peab olema üldine ja võimaldama loodud XML skeemi definitsioone muuta ja laiendada, ilma et tehnilisi kirjeldusi tuleks märkimisväärselt muuta.

Tehnilised kirjeldused kehtivad määrusele (EL) 2018/1727 lisatud skeemide kohustusliku vormi, eelnevalt kindlaks määratud sõnumite ja kõnealuse määruse kohases teabevahetuses kasutatud vabas vormis sõnumite korral.

2.1. *Üldised märkused*

Kõigi skeemide suhtes, mis tuleb esitada, kehtivad järgmised sätted.

2.1.1. Versioonid

Lisatakse versiooniatribuut, mis hõlbustab skeemiversioonide haldamist ja võimaldab skeemi tulevastes versioonides ärinõuete kohaselt ajakohastada. Versiooniatribuut näitab, kas uus versioon on pärast uute elementide või täpsustuste lisamist tagasiühilduv.

2.1.2. Skeemi deklaratsioon ja metaandmed

— Vajaduse korral kasutatakse skeemides asjakohaseid standardeid või sõnastikke, mida nõuab e-CODEXi süsteem koostalitlusvõime tagamiseks ja mis on vajalikud kõnealuses skeemis määratletud elementide ja tüüpide nõuetekohaseks valideerimiseks. Nende hulka võivad kuuluda:

  — ELi e-õiguskeskkonna põhisõnastik;

  — kvalifitseerimata andmetüübid;

  — Euroopa Liidu keelekoodide loend.

— Samuti võib skeem vajaduse korral hõlmata asjakohaseid ETSI standardeid, et kasutada neis sisalduvaid määratlusi.

2.1.3. Kommentaarid ja dokumentatsioon

— **Kommentaarid**. Skeemi iga elemendi juurde tuleb üldjuhul lisada kommentaarid. Kommentaarid sisaldavad inimloetavat teavet elemendi kohta ning sageli määratletakse neis selgelt ja kokkuvõtlikult elemendi otstarve või kasutus.

2.1.4. Kasutus ja kohandatavus

Skeem järgib punktides a–d sätestatud reegleid.

a) **Modulaarne struktuur**: igal jaotisel on konkreetne funktsioon ja iga jaotist saab sõltumatult taaskasutada või kohandada. See võimaldab skeemi erinevate kasutusmallidega hõlpsasti kohandada.

b) **Laiendatavus**: skeem projekteeritakse nii, et see toetab uute elementide või atribuutide kaasamist, kui tulevikus on vaja lisateavet. Selleks kasutatakse valikulisi elemente ja jadasid, mida saab laiendada, ilma olemasolevaid teostusi kahjustamata.

c) **Kohandatav struktuur**: skeem projekteeritakse nii, et see võimaldab vajaduse korral elemente või andmetüüpe lisada või muuta. Skeemi struktuur võimaldab nõudeid muuta, ilma suurte ümberkorraldusteta.

d) **Vabatahtlikud elemendid**: skeemi teatavad elemendid võib tähistada kui vabatahtlikud, st konkreetsetest asjaoludest sõltuvalt võib need kas kaasata või välja jätta.

Skeem projekteeritakse nii, et see toetab konkreetsete taotluste korral struktureeritud andmete kogumist.

2.1.5. Muudatused

Skeem projekteeritakse nii, et seda iseloomustab paindlikkus, modulaarsus ja kohandamise lihtsus. Komplekstüübid ja vabatahtlikud elemendid kaasatakse skeemi viisil, mis võimaldab käsitleda eri stsenaariume, kuid samas teha lihtsalt muudatusi ja laiendusi.

2.2. *Struktureeritud andmete vahetamine*

Punktides 2.2.1 ja 2.2.2 osutatud struktureeritud andmed esitatakse kooskõlas määruse (EL) 2018/1727 artikli 22a lõikega 3. Skeem peab võimaldama märkida ka andmekogumeid, mis hilisemate uuenduste käigus kustutatakse.

2.2.1. Euroopa õigusalase terrorismivastase võitluse registri andmed

Andmeskeemi järgmised tehnilised kirjeldused moodustavad XML-vormingus skeemi loomise struktureeritud raamistiku.

a) Kõrgeima tasandi jaotis

See kõrgeima tasandi jaotis vastab teabele, mis on esitatud määruse (EL) 2018/1727 III lisas (teave Euroopa õigusalase terrorismivastase võitluse registri jaoks).

b) Sõnumi struktuur

Terrorismivastase võitluse registri andmete struktuur koosneb elementide jadast ja sisaldab vähemalt järgmisi andmeid:

i) teave, mida on vaja füüsilise isiku tuvastamiseks:

— perekonnanimi;

— eesnimi (-nimed);

— varjunimed;

— sünniaeg;

— sünnikoht (linn ja riik);

— kodakondsus või kodakondsused;

— isikut tõendav dokument (dokumendi liik ja number);

— sugu;

— elukoht;

ii) teave, mida on vaja juriidilise isiku tuvastamiseks:

— ärinimi;

— õiguslik vorm;

— peakontori asukoht;

iii) teave, mida on vaja nii füüsilise kui ka juriidilise isiku tuvastamiseks:

— telefoninumbrid;

— e-posti aadressid;

— pangakontode või muude finantseerimisasutuste kontode üksikasjad;

— staatus menetluses;

iv) teave süüteo kohta:

— teave juriidiliste isikute kohta, kes on seotud terroriakti ettevalmistamise või toimepanemisega;

— süüteo kvalifikatsioon siseriikliku õiguse kohaselt;

— kohaldatav raske kuriteo liik I lisas esitatud raskete kuritegude loetelust;

— seostatus terrorirühmitusega;

— terroristlik suunitlus, näiteks džihadism, separatism, äärmusvasakpoolsus või äärmusparempoolsus;

— juhtumi lühikokkuvõte;

v) teave riigisisese menetluse kohta:

— sellise menetluse staatus;

— vastutav prokuratuur;

— juhtumi number;

— ametliku kohtumenetluse algatamise kuupäev;

— seosed muude asjakohaste juhtumitega;

vi) lisateabe väli (vabatekst);

vii) eelneva loa kood.

2.2.2. Määruse (EL) 2018/1727 artikli 21 kohaselt edastatud andmed

a) Määruse (EL) 2018/1727 artikli 21 lõige 4, ühiste uurimisrühmade moodustamine

i) Kõrgeima tasandi jaotis
See kõrgeima tasandi jaotis vastab teabele, mis on esitatud määruse (EL) 2018/1727 artikli 21 lõikes 4 (teave ühiste uurimisrühmade moodustamise kohta).

ii) Sõnumi struktuur
Andmete struktuur koosneb elementide jadast ja sisaldab vähemalt järgmisi andmeid:

— Kriminaalmenetlust läbiviiv õigusasutus

— Kriminaalmenetluse riiklik viitenumber

— Kriminaalmenetluse staatus

— Kuriteod, mida uuritakse

— Muud juhtumiga seotud riigid

— Kas Eurojust aitab juba kaasa juhtumi lahendamisele?

— Jaatava vastuse korral Eurojusti juhtumi ID

— Eitava vastuse korral märkige, kas see on kaasaaitamistaotlus

— Kas Europol aitab kaasa juhtumi lahendamisele?

— Jaatava vastuse korral märkige, kas operatiivtöökond ja/või turvaline teabevahetusvõrk (SIENA)

— Ühise uurimisrühma kokkulepe:

— Osalevad riigid

— Ühise uurimisrühma liikmed (liikmesriikide ametiasutused, kes juhivad uurimisi)

— Ühise uurimisrühma pädevusse kuuluva kriminaalmenetluse riiklik viitenumber

— Allkirjastamise kuupäev

— Kestus

— Kuriteod, mida uuritakse

— Juhtumi lühikokkuvõte

— Ühise uurimisrühma pädevusse kuuluva kriminaalmenetluse peamised kahtlusalused (nimi, perekonnanimi, sünniaeg ja -koht ning võimaluse korral muud olulised ja vajalikud II lisa kohased andmekategooriad)

— Ühiste uurimisrühmade töö tulemused:

— Raskused/viivitused seoses järgmisega:

— ühise uurimisrühma moodustamine

— tõendite taotlemine/jagamine ühises uurimisrühmas

— ühises süüdistusstrateegias kokkuleppimine / selle strateegia rakendamine

— Ühise uurimisrühma tõendite lubatavus/mittelubatavus/hindamine siseriiklikus menetluses

— Kohtumenetluse tulemus (edukad/ebaõnnestunud süüdistused ning süüdimõistmised/õigeksmõistmised)

iii) Eelneva loa kood

b) Määruse (EL) 2018/1727 artikli 21 lõige 5, rasked ja keerukad juhtumid

i) Kõrgeima tasandi jaotis
See kõrgeima tasandi jaotis vastab teabele, mis on esitatud Eurojusti määruse artikli 21 lõikes 5 (rasked ja keerukad juhtumid).

ii) Sõnumi struktuur
Andmete struktuur koosneb elementide jadast ja sisaldab vähemalt järgmisi andmeid:

— Kriminaalmenetlust läbiviiv õigusasutus

— Kriminaalmenetluse riiklik viitenumber

— Kriminaalmenetluse staatus

— Kuriteod, mida uuritakse

— Muud juhtumiga seotud riigid

— Kas Eurojust aitab juba kaasa juhtumi lahendamisele?

— Jaatava vastuse korral Eurojusti juhtumi ID

— Eitava vastuse korral märkige, kas see on kaasaaitamistaotlus

— Kas Europol aitab kaasa juhtumi lahendamisele?

— Jaatava vastuse korral märkige, kas operatiivtöökond ja/või SIENA

— Raske kuriteo liik

— Organiseeritud kuritegeliku rühmituse kaasatus

— Maffialaadne rühmitus

— Rahvusvaheline organiseeritud kuritegelik rühmitus

— Tagajärjed ELi tasandil

— Kriminaalmenetluse peamised kahtlusalused (nimi, perekonnanimi, sünniaeg ja -koht ning võimaluse korral muud olulised ja vajalikud II lisa kohased andmekategooriad)

— Juhtumi lühikokkuvõte

— Muud kaasatud riigid

— Riigid, kellega on juba alustatud koostööd

— Kaasatud pädevad asutused muus riigis

— Kasutatud õigusalase koostöö vahendid

— Saadetud/saadud taotluste arv

— Seotud uurimiste olemasolu

— Riigid, kellega on kavas koostööd teha / riigid, mida uurimine tõenäoliselt mõjutab

— Vajaliku koostöö liik (nt väljaandmine, tõendite kogumine, muu koostöö)

— Seotud uurimiste olemasolu

iii) Eelneva loa kood

c) Määruse (EL) 2018/1727 artikli 21 lõike 6 punkt a, kohtualluvuskonfliktid

i) Kõrgeima tasandi jaotis

See kõrgeima tasandi jaotis vastab teabele, mis on esitatud määruse (EL) 2018/1727 artikli 21 lõike 6 punktis a (st kohtualluvuskonfliktid).

ii) Sõnumi struktuur

Andmete struktuur koosneb elementide jadast ja sisaldab vähemalt järgmisi andmeid:

— Kriminaalmenetlust läbiviiv õigusasutus

— Kriminaalmenetluse riiklik viitenumber

— Kriminaalmenetluse staatus (nt uurimine, süüdistuse esitamine, kohtumenetlus)

— Kuriteod, mida uuritakse

— Muud juhtumiga seotud riigid

— Kas Eurojust aitab juba kaasa juhtumi lahendamisele?

— Jaatava vastuse korral Eurojusti juhtumi ID

— Eitava vastuse korral märkige, kas see on kaasaaitamistaotlus

— Kas Europol aitab kaasa juhtumi lahendamisele?

— Jaatava vastuse korral märkige, kas operatiivtöökond ja/või SIENA

— Muud kaasatud riigid

— Muu riigi pädevad asutused, kui need on teada

— Muu riigi kriminaalmenetluse riiklik viitenumber

— Muu riigi menetluse etapp, kui see on teada

— Positiivne või negatiivne kohtualluvuskonflikt

— Tegelik või võimalik kohtualluvuskonflikt

— Juba võetud koordineerimismeetmed (nt konsulteerimine vastavalt nõukogu raamotsusele 2009/948/JSK ([1]))

— Juhtumi lühikokkuvõte

— Peamised ühised kahtlusalused (nimi, perekonnanimi, sünniaeg ja -koht ning võimaluse korral muud olulised ja vajalikud II lisa kohased andmekategooriad)

iii) Eelneva loa kood

d) Artikli 21 lõike 6 punkt b, kontrollialused saadetised

i) Kõrgeima tasandi jaotis

See kõrgeima tasandi jaotis vastab teabele, mis on esitatud määruse (EL) 2018/1727 artikli 21 lõike 6 punktis b (kontrollialused saadetised).

ii) Sõnumi struktuur

Andmete struktuur koosneb elementide jadast ja sisaldab vähemalt järgmisi andmeid:

— Kriminaalmenetlust läbiviiv õigusasutus

— Kriminaalmenetluse riiklik viitenumber

— Kriminaalmenetluse staatus (nt uurimine, süüdistuse esitamine, kohtumenetlus)

— Kuriteod, mida uuritakse

— Muud juhtumiga seotud riigid

— Kas Eurojust aitab juba kaasa juhtumi lahendamisele?

— Jaatava vastuse korral Eurojusti juhtumi ID

— Eitava vastuse korral märkige, kas see on kaasaaitamistaotlus

— Kas Europol aitab kaasa juhtumi lahendamisele?

— Jaatava vastuse korral märkige, kas operatiivtöökond ja/või SIENA

— Muud kaasatud riigid

— Päritoluriik/transiidiriik/sihtriik

— Muude riikide pädevad asutused

— Seotud uurimiste olemasolu muudes riikides

([1]) Nõukogu 30. novembri 2009. aasta raamotsus 2009/948/JSK kohtualluvuskonfliktide vältimise ja lahendamise kohta kriminaalmenetluses (ELT L 328, 15.12.2009, lk 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Kättetoimetatud kaubad (nt uimastid ja nende liik, raha, relvad, sigaretid, muu)

— Kontrollialuse saadetise staatus (nt kavas, teel, kohal)

— Kontrollialuse saadetise tulemus, kui see on juba teada

— Kasutatud õigusalase koostöö vahend

— Peamised ühised kahtlusalused (nimi, perekonnanimi, sünniaeg ja -koht ning võimaluse korral muud olulised ja vajalikud II lisa kohased andmekategooriad)

iii) Eelneva loa kood

e) Määruse (EL) 2018/1727 artikli 21 lõike 6 punkt c, korduvad probleemid õigusalase koostöö vahendite kasutamisel

i) Kõrgeima tasandi jaotis

See kõrgeima tasandi jaotis vastab teabele, mis on esitatud määruse (EL) 2018/1727 artikli 21 lõike 6 punktis c (korduvad probleemid õigusalase koostöö vahendite kasutamisel).

ii) Sõnumi struktuur

Andmete struktuur koosneb elementide jadast ja sisaldab vähemalt järgmisi andmeid:

— Kriminaalmenetlust läbiviiv õigusasutus

— Kriminaalmenetluse riiklik viitenumber

— Kriminaalmenetluse staatus (nt uurimine, süüdistuse esitamine, kohtumenetlus)

— Kuriteod, mida uuritakse

— Muud juhtumiga seotud riigid

— Kas Eurojust aitab juba kaasa juhtumi lahendamisele?

— Jaatava vastuse korral Eurojusti juhtumi ID

— Eitava vastuse korral märkige, kas see on kaasaaitamistaotlus

— Kas Europol aitab kaasa juhtumi lahendamisele?

— Jaatava vastuse korral märkige, kas operatiivtöökond ja/või SIENA

— Muud kaasatud riigid

— Liikmesriikide pädevad asutused, kui need on teada

— Väljaandva või täitva asutusena tegutsev asutus

— Õigusalase koostöö vahend (nt Euroopa vahistamismäärus, Euroopa uurimismäärus, vara arestimine ja konfiskeerimine)

— Konkreetne taotlus (st milline uurimismeede, mis liiki vara arestimine, kas Euroopa vahistamismäärus karistuse täitmisele pööramiseks või süüdistuse esitamiseks)

— Keeldumine või korduv raskus

— Milline on keeldumise korral konkreetne põhjus?

— Probleemi lühikirjeldus

— Muud riiklikud asutused, keda probleem puudutab, kui neid on

iii) Eelneva loa kood

2.3. *Eelnevate lubade koodid*

Kui liikmesriikide pädevad asutused jagavad Eurojustiga JUDEXi kaudu andmeid, teatavad nad pärast seose kindlakstegemist eelnevate lubade koodide kaudu andmete edasisest käsitlemisest, neile juurdepääsust ja nende edastamisest. Eelnevate lubade koodid näitavad, kas ja millisel määral võib teavet seose kohta jagada teiste liikmesriikide pädevate asutuste, muude liidu asutuste ja organite, kolmandate riikide või rahvusvaheliste organisatsioonidega.

2.4. *Eelnevalt kindlaks määratud sõnumid*

Eelnevalt kindlaks määratud sõnumid on määrusega (EL) 2018/1727 kehtestatud teabevahetuse esitused, kuid sellise teabevahetuse jaoks ei ole kõnealuses õigusaktis ette nähtud konkreetset vormi. Nende liik ja arv määratakse kindlaks tehnilise ja ärianalüüsi käigus.

Eelnevalt kindlaks määratud sõnumite XML skeemi definitsioonid projekteeritakse nii, et need tagavad kooskõla, struktuuri ja vastavuse ärivajadustele.

Kõnealuste skeemide korral kehtib järgmine:

a) skeemi kõrgeima tasandi jaotis nimetatakse defineeritava sõnumiliigi järgi;

b) selles struktuuris lisatakse ja defineeritakse vajalikud väljad, mis on nõutavad konkreetse sõnumiliigi jaoks, tagades andmeelementide nõuetekohase esituse.

2.5. *Vabas vormis sõnumid*

Vabas vormis sõnumid on teabevahetuse esitused, mis võimaldavad esitada struktureerimata või osaliselt struktureeritud sisu ning pakuvad paindlikkust, pidades samal ajal kinni regulatiivsetest ja ärinõuetest. Vabas vormis sõnumite XML skeemi definitsioon koostatakse nii, et see tagab kooskõla ja nõuetekohase vormindamise.

Kõnealuste skeemide korral kehtib järgmine:

a) skeemi kõrgeima tasandi jaotis nimetatakse defineeritava vabas vormis sõnumi liigi järgi;

b) skeemis defineeritakse vabas vormis sõnumi struktuur, võimaldades elemente vajaduse korral nõuetekohaselt järjestada;

c) selles struktuuris lisatakse ja defineeritakse vajalikud väljad, mis on nõutavad konkreetse vabas vormis sõnumi liigi jaoks, tagades andmeelementide nõuetekohase esituse.

III LISA

SÕRMEJÄLGEDE JA FOTODE TEHNILISED KIRJELDUSED

Detsentraliseeritud IT-süsteemi kaudu vahetatavatele sõnumitele võib kooskõlas punktides 1 ja 2 sätestatud tehniliste kirjeldustega lisada manuseid, sealhulgas riikliku standardite ja tehnoloogia instituudi (edaspidi „NIST“) faile, mis sisaldavad sõrmejälgi ja fotosid.

1. **Sõrmejäljed**

Sõrmejäljed, mida võib Eurojustiga jagada selleks, et usaldusväärselt tuvastada isikud, kelle suhtes on algatatud terroriaktiga seotud kriminaalmenetlus, peavad vastama järgmistele nõuetele:

a) sõrmejäljed esitatakse ühes failis, mis sisaldab sõrmejälgede digitaalseid kujutisi (sõrmejälgede NIST-fail), ja need edastatakse vastavalt standardi ANSI/NIST-ITL 1–2011 2015. aastal ajakohastatud (või uuemale) versioonile;

b) sõrmejälgede NIST-fail koosneb kuni kümnest individuaalsest sõrmejäljest: pööratud, vajutatud või mõlemad jäljendid;

c) kõik sõrmejäljed on märgistatud;

d) sõrmejäljed skaneeritakse otse või kantakse tinti kasutades paberile, tingimusel et tindiga paberile kantud sõrmejäljed skaneeritakse nõutava lahutusvõimega ja samasuguse kvaliteediga;

e) sõrmejälgede NIST-fail võimaldab kaasata lisateavet, nagu sõrmejälgede registreerimise tingimused ja üksikute sõrmejäljekujutiste saamise meetod;

f) sõrmejälgede nominaalne lahutusvõime on 500 või 1 000 ppi ([1]) (lubatud hälbega +/– 10 ppi) ja kasutatakse 256 halltooni;

g) sõrmejälgede pakkimiseks kasutatava algoritmi puhul järgitakse USA riikliku standardite ja tehnoloogia instituudi soovitusi. Sõrmejäljeandmed lahutusvõimega 500 ppi pakitakse kokku WSQ algoritmi (ISO/IEC 19794-5:2005) abil. Sõrmejäljeandmed lahutusvõimega 1 000 ppi pakitakse kokku JPEG 2000 kujutiste tihendamise standardi (ISO/IEC 15444-1) ja kodeerimissüsteemi abil. Eesmärgiks on tihendussuhe 15:1.

2. **Fotod**

Fotod, mida võib Eurojustiga jagada selleks, et usaldusväärselt tuvastada isikud, kelle suhtes on algatatud terroriaktiga seotud kriminaalmenetlus, peavad vastama järgmistele nõuetele:

a) fotofailis esitatakse ainult üks näokujutis (foto NIST-fail) ja see edastatakse vastavalt standardi ANSI/NIST-ITL 1–2011 2015. aastal ajakohastatud (või uuemale) versioonile;

b) foto peab olema hallskaalal, värviline või lähiinfrapuna;

c) foto kvaliteet peab vastama standardi ISO/IEC 19794-5:2011 (eestvaates näokujutis) või uuema versiooni nõuetele;

d) foto NIST-fail võimaldab kaasata lisateavet, sealhulgas näokujutise tegemise kuupäev;

([1]) Pikslit tolli kohta.

e) portreevaates fotode eraldusvõime on vähemalt 600 korda 800 pikslit ja maksimaalselt 1 200 korda 1 600 pikslit;

f) nägu katab fotost nii palju, et kummagi silma keskpunkti vahele jääb vähemalt 120 pikslit;

g) foto pakkimiseks kasutatava algoritmi puhul järgitakse NIST-soovitusi. Foto pakitakse kokku vaid korra JPG kujutiste tihendamise standardi (ISO/IEC 10918) või JPEG 2000 kujutiste tihendamise standardi (ISO/IEC 15444) ja kodeerimissüsteemi abil; kujutise maksimaalne lubatud tihendussuhe on 20:1.