EIROPAS KOMISIJA

Briselē, 13.7.2011
COM(2011) 429 galīgā redakcija

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Eiropas Teroristu finansēšanas izsekošanas sistēma: pieejamie risinājumi

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Eiropas Teroristu finansēšanas izsekošanas sistēma: pieejamie risinājumi

1. IEVADS

Kad Padome piekrita tam, ka tiek noslēgts Nolīgums starp Eiropas Savienību un Amerikas Savienotajām Valstīm par tādu finanšu ziņojumapmaiņas datu apstrādi un nodošanu, kurus Eiropas Savienība dara pieejamus ASV, lai īstenotu Teroristu finansēšanas izsekošanas programmu (ES un ASV *TFTP* nolīgums)[1], tā arī aicināja Komisiju viena gada laikā no nolīguma spēkā stāšanās dienas (2010. gada 1. augusta) iesniegt Eiropas Parlamentam un Padomei priekšlikumu par "juridisku un tehnisku sistēmu datu ieguvei ES teritorijā"[2]. Eiropas Parlaments ir arī pastāvīgi norādījis, ka ilgākā termiņā ir nepieciešams rast noturīgu un juridiski pārdomātu Eiropas risinājumu pieprasīto datu iegūšanai Eiropas teritorijā[3]. Arī Paziņojumā "ES iekšējās drošības stratēģija darbībā – pieci soļi pretim drošākai Eiropai" jau tika noteikts, ka Komisija 2011. gadā izstrādās politiku, kā ES iegūt un analizēt finanšu ziņojumapmaiņas datus, kas tiek glabāti tās teritorijā[4]. Tā kā jau ir pierādījusies ASV *TFTP* efektivitāte, paredzams, ka Eiropas sistēma sniegtu būtisku ieguldījumu pasākumos, kuru mērķis ir liegt teroristiem piekļuvi finansējumam un materiāliem un izsekot viņu darījumus. Var minēt arī ES un ASV *TFTP* nolīguma 11. pantu, kurā noteikts, ka nolīguma darbības laikā Eiropas Komisija veiks pētījumu par iespēju ieviest līdzvērtīgu ES sistēmu, kas ļautu datus pārsūtīt tiešāk. Šis paziņojums ir pirmais solis Komisijas atbildē uz minēto pantu un Padomes aicinājumu. Tajā ir izklāstīti dažādie pasākumi, ko Komisija veikusi virzībā uz šādas "juridiskas un tehniskas sistēmas" izveidi, un raksturoti dažādie risinājumi, kas tiek apsvērti šā mērķa sasniegšanai. Pašreizējā posmā šajā paziņojumā netiek norādīts viens vēlamais risinājums, tomēr tajā ir minēti būtiskie aspekti, kas jāņem vērā attiecībā uz apsvērtajiem risinājumiem. Ņemot vērā jautājuma politisko nozīmību un tā juridisko un tehnisko sarežģītību, Komisija vēlas informēt Padomi un Eiropas Parlamentu par pašreizējo situāciju un aizsākt debates. Komisija uzskata, ka ir lietderīgi veikt šādas turpmākas debates, pirms tiek iesniegti konkrēti priekšlikumi, pamatojoties uz ietekmes novērtējumu.

Šajā saistībā būtu jāuzsver, ka šis paziņojums nekādā veidā iepriekšēji neietekmē priekšlikumu, ko Komisija izvirzīs. Jebkurā priekšlikumā, ko nākotnē pieņems, tiks ņemtas vērā minētās apspriedes un ietekmes novērtējums, kas būs balstīts uz pētījumu, kura veikšanu Komisija ir uzticējusi līgumdarba veicējam, noslēdzot līgumu 2010. gada otrajā pusē. Ņemot vērā to, kāda ietekme tiesību akta priekšlikumam būtu uz pamattiesībām un jo īpaši uz datu aizsardzību, ietekmes novērtējumā īpaša uzmanība tiks pievērsta tam, cik nepieciešami un samērīgi ir pasākumi, ko Komisija varētu ierosināt. Šajā nolūkā Komisija ievēros norādes, kādas sniegtas tās paziņojumā par Pamattiesību hartas īstenošanas stratēģiju[5].

---

1 OV L 195, 27.7.2010., 5. lpp.
2 Padomes 2010. gada 13. jūlija lēmums, OV L 195, 27.7.2010., 3. lpp.
3 Skat., piemēram, Rezolūciju P7_TA(2010)0143 un Paskaidrojuma rakstu Ieteikumam A7-0224/2010.
4 COM (2010) 673, galīgā redakcija, 22.11.2010. Skat. 2. mērķa 2. darbību, 8. lpp.
5 COM (2010) 573, galīgā redakcija, 19.10.2010.

Turklāt ietekmes novērtējumā būs iekļauts vajadzīgais tehniskais pamatmateriāls, kā arī visu pieejamo risinājumu sīks izvērtējums. Šie jautājumi jau ir pārrunāti ar vairākām šajā jomā ieinteresētajām personām, tostarp dalībvalstu iestādēm, datu aizsardzības iestādēm, Eiropolu un izraudzīto pakalpojumu sniedzēju. Minētā pētījuma galīgie rezultāti būs pieejami tikai šā gada beigās. Lai pamatotu ietekmes novērtējuma sagatavošanu, Eiropas Komisija ir sarīkojusi trīs ekspertu sanāksmes ar minētajām ieinteresētajām personām, kā arī *TFTP* darbības nodrošināšanā iesaistītajām ASV iestādēm. Šajā paziņojumā aplūkotie risinājumi ir pamatoti ar pētījuma provizoriskajiem rezultātiem un minētajās ekspertu sanāksmēs notikušajām apspriedēm.

2. ES TERORISTU FINANSĒŠANAS IZSEKOŠANAS SISTĒMAS IZVEIDES MĒRĶI

ES Teroristu finansēšanas izsekošanas sistēmas *(TFTS)* izveidei ir divi galvenie iemesli:

- sistēmai ir jāsniedz efektīvs ieguldījums cīņā pret terorismu un tā finansēšanu Eiropas Savienībā;

- sistēmai ir jāsniedz ieguldījums uz trešām valstīm pārsūtīto personas datu apjoma ierobežošanā. Sistēmai būtu jānodrošina datu apstrāde, kas vajadzīga, lai programmu varētu īstenot ES teritorijā, ievērojot ES principus un tiesību aktus datu aizsardzības jomā.

Ir pierādījies, ka Amerikas Savienotajās Valstīs Teroristu finansēšanas izsekošanas programmai *(TFTP)* ir ievērojama pievienotā vērtība terorisma un tā finansēšanas apkarošanā, kas nāk par labu ne vien ASV iestādēm, bet arī Eiropas Savienības dalībvalstu un trešo valstu iestādēm. Nesenajā ES un ASV *TFTP* nolīguma pārskatā[6] tika apstiprināts, ka kopš *TFTP* izveides ASV ir veikta vairāk nekā 2500 ziņojumu apmaiņa ar trešo valstu iestādēm, no kuriem liels vairākums (1700) ir koplietoti ar Eiropas Savienību. ASV programmas efektivitāte un tās vērtība terorisma un tā finansēšanas apkarošanā ir apstiprināta arī abos ziņojumus, ko sniedzis tiesnesis *Bruguière*, kuru Eiropas Komisija 2008. gadā iecēla programmas pārskatīšanai. No *TFTP* iegūtajā informācijā, kas tika sniegta ES iestādēm, bija būtiskas norādes uz vairākiem lieliem teroristu uzbrukumiem (to mēģinājumiem), piemēram, uzbrukumiem Madridē un Londonā, 2006. gada plānu uzspridzināt transatlantiskos lidojumus, izmantojot šķidrās sprāgstvielas, un mēģinājumu uzbrukt ASV interesēm Vācijā 2007. gadā. Arī ES Pārskata grupa secināja, ka tai ir iesniegtas "pārliecinošas norādes uz *TFTP* pievienoto vērtību terorisma un tā finansēšanas apkarošanā". Ņemot vērā šo pieredzi, ir pārliecinošs pamats uzskatīt, ka ES *TFTS* nodrošinās arī ievērojamu pievienoto vērtību ES un dalībvalstu centieniem apkarot terorismu un tā finansēšanu.

Kaut arī ASV *TFTP* efektivitāte terorisma un tā finansēšanas apkarošanā netiek apšaubīta, ir paustas nopietnas bažas par tās ietekmi uz pilsoņu pamattiesībām. Šīs bažas tiek saistītas galvenokārt ar faktu, ka ES un ASV *TFTP* nolīguma īstenošana ietver liela personas datu apjoma ("masveida datu") sniegšanu ASV iestādēm — lielākais vairums šo datu attiecas uz pilsoņiem, kuriem nav nekādas saistības ar terorismu vai tā finansēšanu. Šādi dati tiek sniegti masveidā (pamatojoties uz attiecīgām datu kategorijām), nevis individuāli (atbildot uz pieprasījumu par vienu vai vairākiem indivīdiem), jo šo datu sniedzējam nav tehnisku iespēju sniegt datus individualizēti. Turklāt, lai datu sniedzējs tos varētu sniegt individuāli, tam būtu jāizveido īpaša meklēšanas un analīzes funkcija, kas nav nepieciešama tā pamatdarbības

[6] SEC (2011) 438, galīgā redakcija, 30.3.2011.

procesos, un šim nolūkam būtu vajadzīgi ievērojami resursi. Datu pieprasīšana individuālā kārtā nozīmētu arī to, ka datu sniedzējs faktiski uzzinātu, kuri indivīdi tiek izvērtēti saistībā ar terorisma izmeklēšanu un kādas ir to finansiālās attiecības. Tas varētu ietekmēt šādas izmeklēšanas efektivitāti.

Lai kompensētu masveida datu sniegšanu, ir ieviesti būtiski aizsardzības pasākumi nolūkā nodrošināt, ka nenotiek datu ļaunprātīga izmantošana un ka meklējumi sniegtajos datos un šo datu izmantošana notiek vienīgi terorisma un tā finansēšanas apkarošanas mērķiem. Nesenajā ES un ASV *TFTP* nolīguma pārskatā ir apstiprināts, ka šie aizsardzības pasākumi patiešām tiek īstenoti saskaņā ar nolīguma noteikumiem.

Tomēr ir izvirzīti argumenti, ka šādu apjomīgu personas datu sniegšana trešām valstīm ir nepamatots šo valstu pilsoņu pamattiesību pārkāpums, ņemot vērā šāda pārkāpuma nepieciešamību un samērīgumu. Tāpēc Padome aicināja Komisiju iesniegt priekšlikumus par "sistēmas izveidi datu ieguvei ES teritorijā" — vispārējais mērķis ir nodrošināt, lai šādu datu apstrāde notiktu saskaņā ar ES tiesību aktiem un principiem datu aizsardzības jomā un atbilstoši ES Pamattiesību hartai. Šajā saistībā jānorāda, ka finanšu datu vākšana un apstrāde, ko veic publiskas iestādes, ietekmē tiesības uz personas datu aizsardzību, kas noteiktas LESD 16. pantā un Hartas 8. pantā.

Saskaņā ar Hartas 52. panta 1. punktu visiem šo pamattiesību ierobežojumiem ir jābūt noteiktiem tiesību aktos ar nepieciešamo precizitāti un kvalitāti, lai nodrošinātu paredzamību, un tajos jārespektē šīs tiesības. Ierobežojumus drīkst uzlikt vienīgi tad, ja tie ir nepieciešami un samērīgi, lai atbilstu likumīgiem mērķiem, ko atzinusi Savienība. Tāpēc šie principi ir jāņem vērā ne vien tad, kad tiek pieņemts lēmums par to, vai ir jāizveido ES *TFTS*, bet arī izvērtējot sistēmas īstenošanas dažādus pieejamos risinājumus. Līdz ar to šie principi vienlīdz ietekmē izvēles, kas izdarāmas attiecībā uz tādiem jautājumiem kā sistēmas darbības joma, piemērojamie glabāšanas periodi, indivīdu tiesības uz piekļuvi un dzēšanu utt. Šie jautājumi nav sīki iztirzāti šajā paziņojumā. Tos būs vispusīgi jāanalizē ietekmes novērtējumā.

Protams, iespējamā sistēmas izveide datu ieguvei ES teritorijā ietekmētu spēkā esošo ES un ASV *TFTP* nolīgumu, kā atzīts nolīguma 11. panta 3. punktā, kurā noteikts, ka, tā kā ES sistēmas izveide varētu būtiski mainīt šā nolīguma kontekstu, ja Eiropas Savienība nolemj izveidot šādu sistēmu, Pusēm būtu jāapspriežas, lai izlemtu, vai šo nolīgumu būtu nepieciešams attiecīgi pielāgot. Tāpēc visi risinājumi ietekmētu arī spēkā esošā ES un ASV *TFTP* nolīguma turpmāko īstenošanu un no tās izrietošo pielāgošanu.

3. ES TERORISTU FINANSĒŠANAS IZSEKOŠANAS SISTĒMAS GALVENĀS FUNKCIJAS

Viens no pirmajiem jautājumiem, kas tika aktualizēts minētajās apspriedēs ar ieinteresētajām personām, ir tāds, ka lielākais vairums ieinteresēto personu uzskata, ka gadījumā, ja tiek izveidota ES Teroristu finansēšanas izsekošanas sistēma (ES *TFTS*), tam būtu jānotiek ES pilsoņu drošības interesēs. Sistēmu nedrīkstētu izveidot vienkārši tādēļ, lai sniegtu attiecīgu informāciju ASV iestādēm, — arī dalībvalstu iestādes ir patiesi ieinteresētas šādas sistēmas rezultātos. Šī pieeja nozīmē arī to, ka Eiropas līdzvērtīgajai sistēmai nevajadzētu katrā ziņā kopēt visus ASV *TFTP* elementus, lai gan ASV *TFTP* noteikti varētu kalpot kā piemērs tam, kā šādu sistēmu var izveidot. Tāpat ES sistēma būtu jāizveido, ņemot vērā ES tiesiskā un administratīvā regulējuma īpašo raksturu, kā arī ievērojot minētās piemērojamās pamattiesības.

Tomēr jebkurā sistēmā, kuras mērķis ir teroristu finansēšanas izsekošana saskaņā ar iepriekš izklāstītajiem pamatmērķiem, būtu jāparedz šādu pamatfunkciju īstenošana:

- (likumīgi derīgu) pieprasījumu sagatavošana un iesniegšana izraudzītajam(-iem) ziņojumapmaiņas pakalpojumu sniedzējam(-iem) par "izejas" datiem, kas sniedzami pilnvarotam saņēmējam vai saņēmējiem. Minētais ietver pieprasāmo ziņojumu kategoriju noteikšanu, šādu ziņojumu nosūtīšanas biežuma noteikšanu un saziņas uzturēšanu ar pakalpojumu sniedzējiem par šiem jautājumiem;

- pasākumi, lai uzraudzītu un atļautu šādu "izejas" datu pieprasījumus izraudzītajam(-iem) pakalpojumu sniedzējam(-iem). Minētais ietver pārbaudes, lai noskaidrotu, vai "izejas" datu pieprasījums ir sagatavots saskaņā ar piemērojamiem ierobežojumiem;

- "izejas" datu saņemšana no izraudzītā(-ajiem) pakalpojumu sniedzēja(-iem) un uzglabāšana (apstrāde), tostarp atbilstošas fizisko un elektronisko datu drošības sistēmas īstenošana;

- faktiskā meklējumu veikšana sniegtajos datos saskaņā ar piemērojamo tiesisko regulējumu, pamatojoties uz dalībvalstu, ASV vai citu trešo valstu iestāžu lūgumiem veikt šādu meklēšanu, balstoties uz skaidri noteiktiem nosacījumiem un aizsardzības pasākumiem, vai pēc iestādes (vai iestāžu), kam uzticēta datu apstrāde, pašas (pašu) ierosmes;

- sniegtajos datos veikto meklējumu uzraudzība un meklējumu pilnvarošana;

- meklējumu rezultātu analizēšana, apvienojot šos rezultātus ar citu pieejamo informāciju vai izlūkdatiem;

- meklējumu rezultātu (bez turpmākas analīzes) vai analīzes rezultātu izplatīšana pilnvarotajiem saņēmējiem;

- atbilstoša datu aizsardzības režīma, tostarp piemērojamo saglabāšanas periodu, īstenošana, reģistrēšanas pienākumi, piekļuves, labojumu un dzēšanas pieprasījumu apstrāde utt.

Šīs pamatfunkcijas būtu jānosaka atbilstošos juridiskos instrumentos ES līmenī, valstu līmenī vai abos līmeņos atkarībā no izvēlētā risinājuma.

4. PAMATPRINCIPI, KAS JĀŅEM VĒRĀ, APSVEROT PIEEJAMOS RISINĀJUMUS

Papildus apsvērumiem, kas saistīti ar izklāstītajām pamatfunkcijām, izvēle starp pieejamiem risinājumiem lielā mērā būs atkarīga no tā, kā tie ietekmēs vairākus būtiskus aspektus, kas pašlaik tiek izvērtēti ietekmes novērtējumā un tiek iztirzāti turpmāk.

4.1. Efektivitāte

Būtisks faktors ir dažādo risinājumu paredzamā efektivitāte pamatmērķa, proti, terorisma un tā finansēšanas apkarošanas, sasniegšanā. Šajā ziņā priekšroka būtu jādod risinājumiem, kas palielina izredzes datu apmaiņai un analīzei starptautiskā mērogā, jo šāda datu apmaiņa un analīze palielinās efektivitāti un radīs lielāku pievienoto vērtību. Jo īpaši tās organizācijas vai to organizāciju izvēlei, kurām tiks uzticēta datu analīze, kā arī analīzes rezultātu sniegšana attiecīgajām iestādēm, būs būtiska ietekme uz sistēmas vispārējo efektivitāti, kā arī uz datu

apjomu, kas tiks pārsūtīti. Un pat tad — saskaņā ar pašreizējo praksi — dalībvalstīm arī turpmāk būtu jābūt iespējai pilnībā kontrolēt, vai var veikt to informācijas vai izlūkdatu apmaiņu ar citām iestādēm.

4.2. Datu aizsardzība

Informācijas un izlūkdatu apmaiņa un analīze starptautiskā mērogā var notikt tikai tad, ja ir ieviests stabils un pārdomāti izstrādāts datu aizsardzības regulējums. Šāda regulējuma efektivitāte ir atkarīga ne vien no piemērojamām tiesību normām, kas ļauj datu subjektiem īstenot savas tiesības, piemēram, uz tiesību aizsardzību tiesā, bet arī no pieredzējuša personāla, piemēram, neatkarīga datu aizsardzības inspektora un neatkarīgas un pieredzējušas datu aizsardzības kontroles iestādes, pieejamības. Dažās organizācijās, ko varētu iesaistīt ES *TFTS* iespējamā izveidē, šādas struktūrvienības jau darbojas, savukārt citās tās būtu jāizveido. Tāpēc katra risinājuma ietekme uz datu aizsardzību ir rūpīgi jāizvērtē saskaņā ar pamatprincipiem, kas attiecas uz šā paziņojuma 2. sadaļā minēto pamattiesību ievērošanu.

4.3. Datu drošība

Stingrus datu aizsardzības noteikumus nepieciešams papildināt ar mūsdienīgu datu drošības infrastruktūru un tehnoloģiju. Datu drošības apsvērumi liecina par labu to vietu ierobežošanai, kurās var apstrādāt sniegtos datus, kā arī jebkāda veida ārējās piekļuves datiem ierobežošanai. Visdrošākais risinājums būtu datu uzglabāšana vienuviet bez ārējas piekļuves. Lielākā daļa organizāciju, ko varētu iesaistīt *TFTS* darbības nodrošināšanā, jau ir ieviesušas drošas datu apstrādes tehnoloģijas, bet ne visas pašlaik spēj apstrādāt datus, kuru klasifikācijas līmenis ir augstāks par *EU Restricted*.

4.4. Datu uzglabāšana

Datu uzglabāšanu varētu īstenot vai nu valstu, vai ES līmenī. ES līmenī no izraudzītā(-ajiem) pakalpojumu sniedzēja(-iem) saņemtos datus varētu uzglabāt Eiropols vai cita ES iestāde, piemēram, Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (IT aģentūra)[7], kas pašlaik tiek veidota. Tā kā datu uzglabāšana ir nenodalāmi saistīta ar datu aizsardzības un datu drošības jautājumiem, arī par datu uzglabāšanu atbildīgās iestādes izvēle būtu cieši jāsaista ar datu aizsardzības un datu drošības režīmu, ko šādas organizācijas var piedāvāt.

4.5. Esošo struktūru un instrumentu izmantošana

Visos risinājumos būtu jāparedz esošo struktūru izmantošana, ciktāl tas iespējams. Tādējādi tiks ietaupītas izmaksas un būs iespējams likt lietā gūto pieredzi, kā arī izmantot esošo infrastruktūru. Lai varētu izmantot šādus esošos instrumentus, ir jānodrošina, lai esošai organizācijai uzticētie jaunie pienākumi atbilstu attiecīgās organizācijas pašreizējām pilnvarām. Piemēram, Eiropols, *Eurojust* vai valstu tiesu iestādes var būt piemērota struktūra, lai tā darbotos kā iestāde, kas veic izraudzītajam(-iem) pakalpojumu sniedzējam(-iem) adresēto datu pieprasījumu pārbaudi un apstiprināšanu.

---

[7] COM(2010) 93 galīgā redakcija, 19.3.2010.

4.6. Sadarbība starp atbildīgajām iestādēm

Turpmāk izklāstītie risinājumi piedāvā dažāda līmeņa sadarbību un informācijas un izlūkdatu apmaiņu starp valstu iestādēm un starp valstu un Eiropas iestādēm. Dažādas dalībvalstis ir ieviesušas atšķirīgus veidus, kā to iestādes sadarbojas terorisma apkarošanā, un jebkurā Eiropas līmeņa darbībā ir jāievēro ierobežojumi, kas ar LESD 72. pantu noteikti dalībvalstu prerogatīvām attiecībā uz likumības un kārtības uzturēšanu un iekšējās drošības nodrošināšanu. Tāpēc ES *TFTS* ir jāparedz, ka dalībvalstīm ir ievērojama līmeņa kontrole pār informāciju un izlūkdatiem, kuru apmaiņu tās vēlas veikt šādas sistēmas kontekstā. Vairākas organizācijas, kas minētas turpmāk, ir izstrādājušas dažādas pieejas šim jautājumam, no kurām dažas varētu tieši piemērot veidojamajai sistēmai.

4.7. Pirmais vispārīgais pārskats par dažādo risinājumu iespējamo finansiālo ietekmi

ES *TFTS* izveidošanas vispārējās izmaksas un to sadalījums starp ES un valstu līmeņiem lielā mērā būs atkarīgs no izvēlētā politikas risinājuma. Jebkurā gadījumā tās ietvers šādas izmaksas:

- izmaksas, kas saistītas ar to datu drošu pārsūtīšanu un uzglabāšanu, kuri saņemti no izraudzītā(-ajiem) pakalpojumu sniedzēja(-iem);
- izmaksas, kas saistītas ar meklējumu veikšanai un meklējumu rezultātu iesniegšanai vajadzīgās programmatūras izstrādi un uzturēšanu;
- izmaksas, kas saistītas ar meklējumu vai analīzes rezultātu izplatīšanu pilnvarotajiem saņēmējiem;
- izmaksas saistībā ar personālu, kas veic meklējumus un analīzi un izplata rezultātus;
- izmaksas saistībā ar personālu, kas atbild par uzraudzības un revīzijas funkcijām;
- izmaksas saistībā ar personālu, kas atbild par datu aizsardzību un pilsoņu tiesībām.

Lai gan šajā posmā sīki izstrādātas izmaksu aplēses vēl nav pieejamas, sākotnējie aprēķini liecina, ka izmaksas, kas saistītas ar pilnībā ES līmeņa pieeju un visiem dažādajiem turpmāk aprakstītajiem apvienotajiem risinājumiem, varētu svārstīties no 33 līdz 47 miljoniem euro sākotnējās izveides izmaksās, kam pieskaitāmi papildu izdevumi 7 līdz 11 miljonu euro apmērā ikgadējās uzturēšanas izmaksās. Dažādie risinājumi ir izklāstīti šā paziņojuma 6. daļā. Visdārgāk izmaksātu 3. risinājums, proti, izveides izmaksas ES būtu 43 miljoni euro, bet dalībvalstīm (visām kopā) — 3,7 miljoni euro un ikgadējās uzturēšanas izmaksas ES būtu 4,2 miljoni euro, bet dalībvalstīm (visām kopā) — 6,8 miljoni euro. Vismazāk izmaksātu 2. risinājums, proti, izveides izmaksas ES būtu 33 miljoni euro un ikgadējās uzturēšanas izmaksas ES līmenī būtu 3,5 miljoni euro, bet ikgadējās uzturēšanas izmaksas dalībvalstīm (visām kopā) būtu 3,3 miljoni euro. Savukārt 1. risinājuma gadījumā izveides izmaksas ES būtu 40,5 miljoni euro un ikgadējās uzturēšanas izmaksas ES līmenī būtu 4 miljoni euro, bet ikgadējās uzturēšanas izmaksas dalībvalstīm (visām kopā) būtu 5 miljoni euro. Protams, šīs izmaksas samazināsies, ja varēs izmantot esošo organizāciju personālu vai esošās infrastruktūras, kā arī programmatūru un aparatūru. Pilnībā valstu līmeņa sistēmas izveides un uzturēšanas izmaksas būtu daudz augstākas (390 miljoni euro izveidošanas izmaksās, 37 miljoni euro ikgadējās uzturēšanas izmaksās), jo visām dalībvalstīm būtu

jāizveido īpaši drošas datu apstrādes sistēmas un jānodarbina personāls sistēmas darbības nodrošināšanai.

Summas ir provizoriskas, un tās būs jāanalizē sīkāk, ņemot vērā ietekmes novērtējuma iznākumu.

5. JAUTĀJUMI, KAS JĀIZVĒRTĒ

Neatkarīgi no tā, kurš no daudzajiem risinājumiem tiks izvēlēts ES *TFTS* izveidei un darbībai, attiecībā uz iespējamās ES *TFTS* darbības jomu ir jāapsver vairāki būtiski jautājumi. Šie jautājumi ir iztirzāti turpmāk.

5.1. Terorisms un tā finansēšana, vai plašāka darbības joma?

Piekļuve finanšu ziņojumapmaiņas datiem ir noderīga ne tikai terorisma un tā finansēšanas apkarošanā. Reti kurš apšauba, ka šāda piekļuve būtu arī vērtīgs instruments, apkarojot citus smagu noziegumu veidus, jo īpaši organizēto noziedzību un nelikumīgi iegūtu līdzekļu legalizāciju. Tomēr ES un ASV *TFTP* nolīguma kontekstā samērīguma apsvērumu dēļ tiek stingri ievērots ierobežojums datus izmantot vienīgi terorisma un tā finansēšanas apkarošanas nolūkos. Sākotnējās apspriedes, kas līdz šim ir notikušas, liecina, ka pastāv liela vienprātība par to, ka šādi samērīguma apsvērumi arī norāda, ka tādā pašā veidā ir jāierobežo arī līdzvērtīgas Eiropas sistēmas darbības joma atbilstoši vispārējiem apsvērumiem par pamattiesību ievērošanu, kā izklāstīts šā paziņojuma 2. daļā.

5.2. Vairāk nekā viens pakalpojumu sniedzējs?

ES un ASV *TFTP* nolīgums pašlaik paredz ierobežojumu, ka datus var pieprasīt tikai no viena starptautisko finanšu ziņojumapmaiņas pakalpojumu sniedzēja. Lai gan šis pakalpojumu sniedzējs acīmredzot ir pasaulē vissvarīgākais šādu ziņojumapmaiņas pakalpojumu sniedzējs, tirgū darbojas arī citi šo pakalpojumu sniedzēji. Apsvērumi par efektivitāti un līdzvērtīgu konkurences apstākļu radīšanu visiem tirgus dalībniekiem norāda uz to, ka ir jāizveido sistēma, kas būs piemērojama visiem starptautisko ziņojumapmaiņas pakalpojumu sniedzējiem. Jebkurā gadījumā, izvēloties kādu no pieejamiem risinājumiem, ir jāņem vērā administratīvais slogs uzņēmumiem, kas sniedz finanšu ziņojumapmaiņas pakalpojumus.

5.3. Tikai starptautiski ziņojumapmaiņas pakalpojumi, vai arī valsts mēroga pakalpojumi?

ES un ASV *TFTP* nolīgums pašlaik paredz ierobežojumu, ka datus var pieprasīt tikai no uzņēmumiem, kas sniedz starptautiskus finanšu ziņojumapmaiņas pakalpojumus, tas ir, ziņojumapmaiņas pakalpojumus, ko izmanto starptautisku darījumu veikšanai, arī starp ES dalībvalstīm, taču izslēdzot finanšu ziņojumapmaiņas datus, kas attiecas uz Vienoto euro maksājumu zonu *(SEPA)*. Izveidojot ES *TFTS*, būs arī jāizvērtē, vai ir jāiekļauj finanšu ziņojumapmaiņas pakalpojumi starp dalībvalstīm, vai arī sistēma aptvers vienīgi starptautiskus finanšu ziņojumapmaiņas pakalpojumus, kā tas ir ES Pasažieru datu reģistra gadījumā. ES un ASV *TFTP* nolīguma darbības jomā pašlaik nav iekļauti pilnībā valsts līmeņa finanšu ziņojumapmaiņas pakalpojumi (ko izmanto tikai saistībā ar valsts mēroga finanšu darījumiem). Piekļuve šādiem valsts finanšu ziņojumapmaiņas pakalpojumiem būtu terorisma un citu noziedzības veidu apkarošanas interesēs. Tomēr, pat ja neņem vērā jautājumu par to, vai piekļuve šādiem pilnībā valsts mēroga darījumiem būtu jāreglamentē ES

līmenī, sākotnējās apspriedes apstiprināja uzskatu, ka šāda piekļuve tiek plaši uzskatīta par nesamērīgu un tāpēc nebūtu iekļaujama ES sistēmas darbības jomā.

5.4. Kāda veida finanšu ziņojumapmaiņas dati būtu iekļaujami?

Ir daudz dažādu finanšu ziņojumapmaiņas datu veidu, kas tiek izmantoti starptautiskajā banku sistēmā. ES un ASV *TFTP* nolīgums attiecas tikai uz vienu konkrētu finanšu ziņojumapmaiņas datu veidu. Piekļuve pārējiem finanšu ziņojumapmaiņas datu veidiem būtu terorisma un tā finansēšanas un, iespējams, citu noziedzības veidu apkarošanas interesēs. Tomēr arī attiecībā uz šo izvēli apsvērumi par samērīgumu un pilsoņu pamattiesību ievērošanu norāda uz to, ka ir jāierobežo ziņojumapmaiņas veidi, kas būtu iekļaujami sistēmā. Plašāka informācija par šo tehnisko jautājumu būs iekļauta ietekmes novērtējumā.

6. RISINĀJUMI ATTIECĪBĀ UZ ES *TFTS*

Turpmāk aprakstītos risinājumus Komisija pašlaik izvērtē kā daļu no notiekošā ietekmes novērtējuma. Tie nav katrā ziņā ierobežojoši un nekādā ziņā iepriekšēji neietekmē galīgo ietekmes novērtējumu vai izvēli, ko Komisija izdarīs, pamatojoties uz minēto novērtējumu.

Viens no risinājumiem, kas vienmēr tiek apsvērts jaunu iniciatīvu un to papildinošo ietekmes novērtējumu sagatavošanas procesā, ir *status quo* saglabāšana — šajā gadījumā tas nozīmētu saglabāt ES un ASV *TFTP* nolīgumu un neiesniegt nekādus priekšlikumus par ES *TFTS*. Ja tiks īstenots šis risinājums, tas nozīmē, ka netiks atbildēts uz Padomes un Parlamenta aicinājumu Komisijai nākt klajā ar priekšlikumu par "juridisku un tehnisku sistēmu datu ieguvei ES teritorijā", kā minēts šā paziņojuma 1. daļā. Turklāt šis risinājums neveicinātu uz trešām valstīm nosūtīto personas datu apjoma ierobežošanu un neparedzētu datu apstrādi ES teritorijā, ievērojot ES principus un tiesību aktus datu aizsardzības jomā. Visi pārējie risinājumi, kas sīkāk izklāstīti turpmāk šajā paziņojumā, ir pašlaik iespējamie veidi, kā izveidot ES *TFTS*.

Teorētiski visas ES *TFTS* pamatfunkcijas, kas minētas šā paziņojuma 3. daļā, varētu īstenot vai nu ES līmenī, vai valstu līmenī. Minētās funkcijas var arī uzticēt vienai vai vairākām dažādām organizācijām atbilstoši to pašreizējiem pienākumiem, vai arī var izveidot jaunas organizācijas šo funkciju īstenošanai. Šādas organizācijas varētu būt vai nu Eiropas, vai valstu organizācijas. Tas nozīmē, ka — arī teorētiski — vienlīdz iespējama ir gan tikai ES līmeņa pieeja, kurā visas pamatfunkcijas ir uzticētas ES līmeņa organizācijām, gan arī tikai valstu līmeņa pieeja, kurā visas funkcijas tiek īstenotas valstu līmenī. Kopumā ir arī jāatceras, ka izvēle starp centralizētu, decentralizētu sistēmu vai apvienotu sistēmu šajā konkrētajā gadījumā nav katrā ziņā tāda pati kā izvēles, kas tiek izdarītas attiecībā uz citām iniciatīvām, kuras saistītas ar datu apstrādi terorisma un organizētās noziedzības apkarošanas mērķiem, — katra iniciatīva šajā jomā ir jāizvērtē individuāli.

Gan pilnībā centralizētām, gan pilnībā valstu līmeņa pieejām ir būtiski trūkumi. Piemēram, pilnībā Eiropas līmeņa pieeja būtu nošķirta no dalībvalstu tiesībaizsardzības un izlūkdatu vākšanas organizācijām un prakses, un tāpēc tā nebūtu īpaši efektīva. Bez to valsts iestāžu līdzdalības, kas atbild par šo jautājumu risināšanu, būtu gandrīz neiespējami precīzi noteikt, kuras datu kategorijas ir jāpieprasa no izraudzītā(-ajiem) pakalpojumu sniedzēja(-iem). Sistēmas lietderīgums mazinātos arī tad, ja vaicājumi datubāzē notiktu, pamatojoties tikai uz ES līmenī pieejamiem izlūkdatiem, — pašreizējā ES integrācijas līmenī šādi izlūkdati lielā mērā ir pieejami tikai valstu līmenī. Turklāt dalībvalstis, visticamāk, neatzītu šādu pilnībā ES

līmeņa pieeju, jo tā nepiešķirtu pievienoto vērtību to individuālajiem centieniem apkarot terorismu un tā finansēšanu. Apspriežu laikā dalībvalstis arī norādīja, ka šo risinājumu būtu politiski grūti atzīt juridisku un darbības apsvērumu dēļ.

Turpretī otra galējība — pilnībā valsts līmeņa pieeja — varētu izraisīt īstenošanas atšķirības dažādās dalībvalstīs un palielinātu datu drošības pārkāpumu risku, jo būtu vajadzīgas 27 dažādas sniegto datu kopijas. Pilnībā valsts līmeņa pieeja arī nozīmētu grūtības īstenot saskaņotu datu aizsardzības sistēmu, kā arī saskaņotu pieeju attiecībā uz citiem vajadzīgajiem ierobežojumiem, piemēram, attiecināšanai tikai uz terorismu un tā finansēšanu, vai šādu ierobežojumu kontroli. Turklāt, ja tiek izmantota pilnībā valsts līmeņa pieeja, nav skaidrs, kura dalībvalsts būtu atbildīga par to meklējumu pieprasījumu apstrādi, kas saņemti no trešām valstīm, un tādējādi tiktu zaudēta pievienotā vērtība, kas piemīt meklējumu rezultātu analīzei Eiropas līmenī. Turklāt, kā minēts iepriekš, ar šo risinājumu saistītās izmaksas būtu ievērojami augstākas, jo visām dalībvalstīm vajadzētu izveidot īpaši drošas datu apstrādes sistēmas un būtu jānodarbina personāls sistēmas darbības nodrošināšanai.

Tāpēc, veicot sagatavošanas darbu kopā ar ieinteresētajām personām, ātri vien tika secināts, ka abējādi galējie iespējamie risinājumi nav atbalstāmi; radās vienprātība par to, ka risinājums, kas, visticamāk, varētu nodrošināt labākos iespējamos rezultātus abu galveno mērķu sasniegšanā, ir apvienots risinājums, kas paredz dažādo funkciju sadalīšanu starp dažādām organizācijām ES un valstu līmenī. Kaut arī šī vienprātība palīdz noteikt vispiemērotāko risinājumu, arī apvienotā pieeja joprojām ietver vairākas būtiskas izvēles, kas ir jāizdara. Turpmākajās sadaļās visi trīs apvienotie risinājumi, kas pašreiz notiekošajā sagatavošanas darbā tika noteikti kā visticamākie, ir aprakstīti sīkāk — risinājumi ir arī apkopoti tabulā šā paziņojuma pielikumā.

6.1. ES *TFTS* koordinācijas un analītiskais dienests (1. risinājums)

Šajā risinājumā tiktu izveidota ES centrālā *TFTS* vienība, un lielākā daļa tās uzdevumu un funkciju tiktu īstenotas ES līmenī. "Izejas" datu pieprasījumu iesniegšana izraudzītajam(-iem) pakalpojumu sniedzējam(-iem), šādu pieprasījumu pārbaude, meklējumu pieprasījumu apstrāde un meklējumu veikšana, meklējumu rezultātu pārvaldība un ziņojumu nosūtīšana meklējumu pieprasītājiem notiktu ES līmenī. Tomēr pieprasījumu sagatavošana izraudzītajam(-iem) pakalpojumu sniedzējam(-iem) varētu notikt, apspriežoties ar dalībvalstu atbildīgajām iestādēm, un dalībvalstis varētu arī izvēlēties norīkot savus analītiķus uz centrālo vienību dalībai meklējumu veikšanā. Pretstatā pilnībā centralizētajam risinājumam dalībvalstis varētu pieprasīt, lai meklējumi tiek veikti to vārdā, līdzīgi kā pašreizējā procedūrā, kas tiek īstenota saistībā ar ASV *TFTP*, vai lai meklējumus veic viņu pašu analītiķi.

Dalībvalstīm būtu jāveic informācijas apmaiņa ar ES centrālo *TFTS* vienību, lai "pamatotu" pieprasījumu un tā saistību ar terorismu, pirms šādus meklējumus var sākt, vai arī jānodrošina, ka to pieprasījumus iepriekš apstiprina valsts iestādes. Šādas valsts iestādes varētu būt, piemēram, valstu pretterorisma prokurori vai izmeklēšanas tiesneši — ja tie apstiprinātu konkrētu meklējumu attiecībā uz sniegtajiem datiem, tad ES centrālā *TFTS* vienība varētu piekrist veikt meklējumus bez turpmākas pārbaudes. Pēc šāda scenārija nebūtu vajadzības iesniegt ES centrālajai *TFTS* vienībai papildu izlūkdatus. ES centrālā *TFTS* vienība nosūtītu meklējumu un to analīzes rezultātus un varētu arī uzreiz sniegt informāciju. Arī ASV un citām trešām valstīm būtu jāpieprasa meklējumu veikšana, ievērojot līdzīgu procesu.

Arī aizsardzības un kontroles pasākumu ievērošanas uzraudzība notiktu centralizēti, iespējams, pārraudzībā iesaistot neatkarīgus ekspertus, piemēram, tos, kas pārstāv izraudzīto(-

s) pakalpojumu sniedzēju(-s), un tos, kas iecelti kā neatkarīgi pārraudzītāji. Datu aizsardzība, integritāte un drošība arī tiktu nodrošināta centrālā līmenī.

Galvenās sistēmā iesaistītās iestādes varētu būt Eiropols un *Eurojust*. Tādā gadījumā Eiropola un *Eurojust* veicamajiem uzdevumiem ir jāatbilst to pamatuzdevumiem, kas noteikti Līgumā par Eiropas Savienības darbību (LESD). Būs arī jānosaka, ciktāl būs nepieciešams grozīt juridiskos instrumentus, kas pašlaik reglamentē minēto struktūru darbību. Ja Eiropols tiktu izvēlēts par ES centrālo *TFTS* iestādi, tam būtu arī jāapstrādā ES pilsoņu iesniegtie piekļuves, labošanas un piekļuves liegšanas pieprasījumi saskaņā ar spēkā esošo tiesisko regulējumu un datu aizsardzības noteikumiem. ES centrālā *TFTS* vienība veiktu savus uzdevumus saskaņā ar spēkā esošo tiesisko regulējumu, un arī tiesību aizsardzības un pārsūdzības jautājumi tiktu risināti saskaņā ar spēkā esošajām tiesību normām. Valstu līmenī meklējumu pieprasījumu pārbaudīšanai un apstiprināšanai tiktu iesaistītas valstu tiesībaizsardzības iestādes. Var paredzēt iespēju izveidot jaunas valstu iestādes, bet šo izvēli labāk atstāt dalībvalstu ziņā, pamatojoties uz subsidiaritātes principu[8].

6.2. ES *TFTS* ieguves dienests (2. risinājums)

Tāpat kā pirmais politikas risinājums, arī šis risinājums nozīmētu, ka ir jāizveido ES centrālā *TFTS* vienība, kuras pienākumi ietvertu "izejas" datu pieprasījumu iesniegšanu izraudzītajam(-iem) pakalpojumu sniedzējam(-iem), šādu pieprasījumu pārbaudi, meklējumu veikšanu un meklējumu pieprasījumu apstrādi. Tomēr šajā risinājumā ES *TFTS* vienībai nebūtu atļauts analizēt meklējumu rezultātus un salīdzināt tos ar citu pieejamo informāciju vai izlūkdatiem, ja šādi meklējumi tiek veikti pēc dalībvalstu iestāžu pieprasījuma, — šādos gadījumos tās uzdevums būtu vienīgi sagatavot un izplatīt meklējumu rezultātus pārskatāmā formā.

Tāpat kā 1. risinājumā "izejas" datu pieprasījumi, kas jāiesniedz izraudzītajam(-iem) pakalpojumu sniedzējam(-iem), tiktu sagatavoti, cieši apspriežoties ar dalībvalstīm, kas varētu darīt zināmas savas konkrētās vajadzības centrālajai TFTS vienībai, kura tās izanalizētu un sagatavotu pieprasījumu(-s), pamatojoties uz veikto analīzi.

Dalībvalstu iestādes pieprasītu, lai meklējumi tiek veikti to vārdā. Tas, ciktāl šādi pieprasījumi ir pamatoti un ir saistīti ar terorismu, tiktu pārbaudīts un apstiprināts valstu līmenī. ES centrālā *TFTS* vienība veiktu meklējumus un atsūtītu dalībvalstīm pilnīgu rezultātu kopumu, kas strukturēts pārskatāmā formātā. Dalībvalstu iestādes būtu vienīgās, kas veiktu meklējumu analīzi, un varētu arī izvēlēties uzreiz sniegt informāciju.

ES centrālajai *TFTS* vienībai tiktu uzticēta meklējumu veikšana un rezultātu analizēšana ES iestāžu, ASV un citu trešo valstu vārdā. Tā arī varētu uzreiz sniegt informāciju, pamatojoties uz minēto.

Tāpat kā iepriekšējos risinājumos aizsardzības un kontroles pasākumu ievērošanas uzraudzība notiktu centralizēti, iespējams, pārraudzībai iesaistot neatkarīgus ekspertus, piemēram, tos, kas pārstāv izraudzīto(-s) pakalpojumu sniedzēju(-s), un tos, kas iecelti kā neatkarīgi pārraudzītāji. Arī datu aizsardzība, integritāte un drošība tiktu nodrošināta centrālā līmenī.

---

[8] Šajā posmā vēl nav zināma ietekme uz to ES aģentūru budžetu, kuras varētu būt iesaistītas sistēmas īstenošanā.

Tāpat kā iepriekšējā risinājumā galvenās sistēmā iesaistītās iestādes varētu būt Eiropols un *Eurojust*. Valstu līmenī galvenās iesaistītās struktūras būtu valstu tiesībaizsardzības vai izlūkdatu vākšanas iestādes. Tāpat kā iepriekšējā risinājumā jaunu valstu iestāžu izveide tiktu atstāta dalībvalstu ziņā, pamatojoties uz subsidiaritātes principu. Eiropols un/vai valstu vienības apstrādātu no ES pilsoņiem saņemtos piekļuves, labošanas un dzēšanas pieprasījumus, iesaistot gan valstu datu aizsardzības iestādes, gan Eiropola Apvienoto uzraudzības iestādi. Tiesību aizsardzības un pārsūdzības jautājumi tiktu risināti saskaņā ar piemērojamām tiesību normām valstu vai ES līmenī[9].

6.3. Finanšu ziņu vākšanas vienību *(FIU)* koordinācijas dienests (3.risinājums)

Šajā politikas risinājumā tiktu izveidota uzlabota *FIU* platforma, kurā tiktu iekļautas visas dalībvalstu *FIU*. Minētā ES līmeņa *ad-hoc* iestāde iesniegtu "izejas" datu pieprasījumus izraudzītajam(-iem) pakalpojumu sniedzējam(-iem), apkopojot *FIU* norādītās vajadzības vienotā pieprasījumā, kas arī tiktu pārbaudīts un apstiprināts centrālā līmenī.

Katra *FIU* būtu atbildīga par meklējumu veikšanu un meklējumu rezultātu pārvaldību savas dalībvalsts vārdā, kā arī par analīzes veikšanu un ziņojumu nosūtīšanu adresātiem, kuriem tie, pēc *FIU* ieskatiem, ir jāsaņem. Tas, ciktāl meklējumi ir pamatoti un ir saistīti ar terorismu, tiktu pārbaudīts un apstiprināts valstu vai ES līmenī. *FIU* būtu arī atbildīgas par tūlītēju informācijas sniegšanu.

Uzlabotā *FIU* platforma varētu veikt meklējumus un analizēt rezultātus ES iestāžu un to citu trešo valstu vārdā, ar kurām ES ir noslēgusi nolīgumu. Tā varētu arī uzreiz sniegt informāciju.

Aizsardzības un kontroles pasākumu ievērošanas uzraudzība notiktu centralizēti, iespējams, pārraudzībai iesaistot neatkarīgus ekspertus, piemēram, tos, kas pārstāv izraudzīto(-s) pakalpojumu sniedzēju(-s), un tos, kas iecelti kā neatkarīgi pārraudzītāji. Datu aizsardzība, integritāte un drošība arī tiktu nodrošināta centrālā līmenī.

Uzlabotajai *FIU* platformai tiktu piešķirts formāls juridiskais statuss ar skaidri definētiem pienākumiem un atbildību. Valstu līmenī galvenās iesaistītās struktūrvienības būtu *FIU* un valstu tiesībaizsardzības un izlūkdatu vākšanas iestādes.

Jebkura ES līmeņa iestāde apstrādātu no ES pilsoņiem saņemtos piekļuves, labošanas un dzēšanas pieprasījumus, bet tiesību aizsardzības un pārsūdzības jautājumi tiktu risināti saskaņā ar piemērojamām tiesību normām valstu vai ES līmenī.

7. SECINĀJUMI

Pamatojoties uz sagatavošanas darbu, ko līdz šim veikusi Komisija, un ņemot vērā ietekmes novērtējuma rezultātus, šajā paziņojumā ir aprakstīti dažādi pieejamie risinājumi, kā izveidot "juridisku un tehnisku sistēmu datu ieguvei ES teritorijā" teroristu finansēšanas izsekošanas sistēmas kontekstā. Dažādie šajā paziņojumā izvērtētie risinājumi liecina, ka joprojām būs jāizdara svarīgas izvēles un jāpieņem būtiski lēmumi, tostarp attiecībā uz pamattiesību ievērošanu, un turpmākajā sagatavošanas darba gaitā daudzi juridiski, tehniski un organizatoriski jautājumi būs jārisina daudz detalizētāk. Ņemot vērā šos būtiskos aspektus,

[9] Skatīt 8. zemsvītras piezīmi.

Komisija uzskata, ka vajadzīgs pietiekams laiks turpmākam sagatavošanas darbam un apspriedēm ar Padomi un Parlamentu.

* * *

Pielikums. Apvienoto risinājumu pārskats tabulas formā

	ES *TFTS* koordinācijas un analītiskais dienests (1. risinājums)	ES *TFTS* ieguves dienests (2. risinājums)	Finanšu ziņu vākšanas vienību *(FIU)* koordinācijas dienests (3. risinājums)
"Izejas" datu pieprasījumu sagatavošana un iesniegšana	ES centrālā *TFTS* vienība, to saskaņojot ar DV	ES centrālā *TFTS* vienība, to saskaņojot ar DV	Uzlabotā FIU platforma
"Izejas" datu pieprasījumu uzraudzība un apstiprināšana	*Eurojust* vai cita esoša iestāde	*Eurojust* vai cita esoša iestāde	*Eurojust* vai cita esoša iestāde
"Izejas" datu saņemšana un uzglabāšana, datu drošība	Eiropols vai cita ES struktūra, piemēram, IT aģentūra	Eiropols vai cita ES struktūra, piemēram, IT aģentūra	Eiropols vai cita ES struktūra, piemēram, IT aģentūra
Meklējumu veikšana "izejas" datos	ES centrālā *TFTS* vienība, DV norīkoti analītiķi, vai abu apvienojums	ES centrālā *TFTS* vienība	*FIU*, uzlabotā *FIU* platforma
Meklējumu veikšanas uzraudzība un pilnvarošana	Neatkarīgi pārraudzītāji, iespējams, valstu iestādes	Neatkarīgi pārraudzītāji, valstu iestādes	Neatkarīgi pārraudzītāji
Meklējumu rezultātu analizēšana	ES centrālā *TFTS* vienība, DV norīkoti analītiķi, vai abu apvienojums	Valstu iestādes valstu meklējumiem, ES centrālās *TFTS* analītiķi ES un trešo valstu meklējumiem	Uzlabotā *FIU* platforma, valstu *FIU*
Meklējumu rezultātu izplatīšana	Eiropola analītiķi vai DV norīkoti analītiķi	Valstu iestādes valstu meklējumiem, ES centrālās *TFTS* analītiķi ES un trešo valstu meklējumiem	Uzlabotā *FIU* platforma, valstu *FIU*
Atbilstoša datu aizsardzības režīma īstenošana	Eiropols vai cita ES struktūra, piemēram, IT aģentūra	Eiropols vai cita ES struktūra, piemēram, IT aģentūra	Eiropols vai cita ES struktūra, piemēram, IT aģentūra