



EIROPAS SAVIENĪBA

EIROPAS PARLAMENTS

PADOME

Briselē, 2023. gada 31. augustā
(OR. en)

2021/0393 (COD)

PE-CONS 74/22

COPEN 462
EUROJUST 116
CT 234
ENFOPOL 659
COTER 308
JAI 1734
CODEC 2085

LEĢISLATĪVIE AKTI UN CITI DOKUMENTI

Temats: EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) 2018/1727 un Padomes Lēmumu 2005/671/TI attiecībā uz digitālu informācijas apmaiņu terorisma lietās

**EIROPAS PARLAMENTA UN PADOMES
REGULA (ES) 2023/...**

(... gada ...),

**ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) 2018/1727
un Padomes Lēmumu 2005/671/TI attiecībā uz
digitālu informācijas apmaiņu terorisma lietās**

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 85. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

saskaņā ar parasto likumdošanas procedūru¹,

¹ Eiropas Parlamenta 2023. gada 12. jūlija nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes ... lēmums.

tā kā:

- (1) Ar Eiropas Parlamenta un Padomes Regulu (ES) 2018/1727¹ tika izveidota *Eurojust* un tika noteikti tās uzdevumi, kompetence un funkcijas.
- (2) Padomes Lēmumā 2005/671/TI² ir noteikts, ka terorisma apkarošanā ir būtiski, lai attiecīgie dienesti iegūtu pēc iespējas pilnīgāku un jaunāku informāciju. Minētajā lēmumā prasīts, lai dalībvalstu kompetentās iestādes sniegtu *Eurojust* informāciju par kriminālvajāšanām un notiesāšanām par teroristu nodarījumiem, kas ietekmē vai var ietekmēt divas vai vairākas dalībvalstis.
- (3) Tā kā Lēmuma 2005/671/TI interpretācijā ir nekonsekvence, dažos gadījumos informācija netiek kopīgota laikus, informācija netiek kopīgota vispār vai arī ne visa būtiskā informācija tiek kopīgota. *Eurojust* jāsaņem pietiekama informācija, lai identificētu saiknes starp pārrobežu izmeklēšanām.

¹ Eiropas Parlamenta un Padomes Regula (ES) 2018/1727 (2018. gada 14. novembris) par Eiropas Savienības Aģentūru tiesu iestāžu sadarbībai krimināllietās (*Eurojust*) un ar ko aizstāj un atceļ Padomes Lēmumu 2002/187/TI (OV L 295, 21.11.2018., 138. lpp.).

² Padomes Lēmums 2005/671/TI (2005. gada 20. septembris) par informācijas apmaiņu un sadarbību attiecībā uz teroristu nodarījumiem (OV L 253, 29.9.2005., 22. lpp.).

- (4) Saskaņā ar Regulu (ES) 2018/1727 svarīgs *Eurojust* uzdevums ir palīdzēt dalībvalstu kompetentajām iestādēm nodrošināt iespējami vislabāko izmeklēšanu un kriminālvajāšanu koordināciju, ieskaitot saikņu identificēšanu starp šādām izmeklēšanām un kriminālvajāšanām. Minētā regula ļauj *Eurojust* izmantot proaktīvāku pieeju un sniegt labākus pakalpojumus dalībvalstīm, piemēram, ierosinot sākt izmeklēšanas un identificējot koordinācijas vajadzības, lietas, kurās, iespējams, ir pārkāpts princips *ne bis in idem*, un nepietiekamības kriminālvajāšanā.
- (5) 2019. gada septembrī *Eurojust*, pamatojoties uz Lēmumu 2005/671/TI, izveidoja Eiropas Tiesu iestāžu pretterorisma reģistru ar konkrētu mērķi identificēt iespējamās saiknes starp tiesvedībām pret teroristu nodarījumos aizdomās turētām personām un no šādām saiknēm izrietošās iespējamās koordinācijas vajadzības.
- (6) Eiropas Tiesu iestāžu pretterorisma reģistrs tika izveidots pēc Regulas (ES) 2018/1727 pieņemšanas, un līdz ar to minētais reģistrs nav pienācīgi integrēts *Eurojust* tehniskajā infrastruktūrā un šis reģistrs nav arī minēts Regulā (ES) 2018/1727. Tāpēc ir nepieciešams šo situāciju labot.

- (7) Terorisma iedarbīgā apkarošanā ļoti svarīga ir ar teroristu nodarījumu izmeklēšanu vai kriminālvajāšanu saistītas informācijas apmaiņa starp kompetentajām iestādēm un Savienības aģentūrām. Ir būtiski iegūt pēc iespējas pilnīgāku un atjauninātu informāciju.
- (8) Teroristu organizācijas arvien vairāk iesaistās citu veidu smagos noziegumos un bieži vien ir daļa no organizētiem tīkliem. Šāda iesaiste attiecas uz smagiem noziegumiem, piemēram, cilvēku tirdzniecību, narkotiku tirdzniecību, finanšu noziegumiem un nelikumīgi iegūtu līdzekļu legalizāciju. Attiecībā uz šādiem smagiem noziegumiem ir jāveic tiesvedību šķērspārbaude.
- (9) Lai *Eurojust* varētu identificēt saiknes starp pārrobežu tiesvedībām pret teroristu nodarījumos aizdomās turētām personām, kā arī saiknes starp tiesvedībām pret teroristu nodarījumos aizdomās turētām personām un *Eurojust* apstrādāto informāciju, kas saistīta ar citām smagu noziegumu lietām, ir svarīgi, lai *Eurojust* no kompetentajām iestādēm saskaņā ar šīs regulas attiecīgajiem noteikumiem pēc iespējas ātri saņemtu informāciju, kas vajadzīga, lai *Eurojust*, izmantojot šķērspārbaudes, varētu veikt minēto saikņu identifikāciju.

- (10) Lai valsts kompetentās iestādes *Eurojust* iesniegtu datus, tām ir precīzi jāzina, kāda veida informācija ir jānosūta un kurā valsts kriminālprocesa posmā un kādās lietās tas ir jā dara. Valsts kompetentajām iestādēm informācija *Eurojust* būtu jānosūta strukturētā, organizētā, sistematizētā un daļēji automatizētā veidā. Daļēji automatizēts veids ir tāds, kurā informācijas nosūtīšanai izmantotais režīms ir daļēji automatizēts un daļēji cilvēka kontrolēts. Paredzams, ka minētais nosūtīšanas veids ievērojami palielinās *Eurojust* saņemtās informācijas kvalitāti un relevanci.
- (11) Datu kopīgošana, uzglabāšana un šķērspārbaudes ievērojami palielinās *Eurojust* apstrādāto datu apjomu. Minētie elementi būtu jāņem vērā, saskaņā ar esošajām procedūrām un satvariem nosakot finanšu resursus, cilvēkresursus un tehniskos resursus, kas vajadzīgi *Eurojust*.
- (12) Eiropas Parlamenta un Padomes Direktīva (ES) 2017/541¹, kas transponēta valstu tiesību aktos, ir atsauces punkts valsts kompetentajām iestādēm teroristu nodarījumu definēšanai.

¹ Eiropas Parlamenta un Padomes Direktīva (ES) 2017/541 (2017. gada 15. marts) par terorisma apkarošanu un ar ko aizstāj Padomes Pamatlēmumu 2002/475/TI un groza Padomes Lēmumu 2005/671/TI (OV L 88, 31.3.2017., 6. lpp.).

- (13) Ir būtiski apmainītie ar uzticamiem identifikācijas datiem, lai *Eurojust* identificētu saiknes starp terorisma izmeklēšanām un tiesvedībām pret personām, kas tiek turētas aizdomās par teroristu nodarījumiem. Ir arī būtiski, lai *Eurojust* izveidotu un uzglabātu datu kopumu, ar ko nodrošina, ka var ticami identificēt personas, uz kurām attiecas šādas terorisma izmeklēšanas vai tiesvedības. Tāpēc svarīga ir biometrisko datu izmantošana, ņemot vērā to, ka pastāv neskaidrības par burtparu datiem, jo īpaši attiecībā uz trešo valstu valstspiederīgajiem, to, ka aizdomās turētie dažkārt izmanto viltus identitāti vai dubultidentitāti, un to, ka biometriskie dati bieži vien ir vienīgā saikne ar aizdomās turētajiem izmeklēšanas posmā. Tādēļ, ja saskaņā ar valsts tiesību aktiem par kriminālprocesu vai procesuālajām tiesībām kriminālprocesā valsts kompetentās iestādes glabā un vāc biometriskos datus un tām ir atļauts tos nosūtīt, minētajām iestādēm būtu jāspēj ar šādiem datiem, kad tie ir pieejami, apmainīties ar *Eurojust*. Tā kā biometriskie dati ir sensitīvi un biometrisko datu apstrāde ietekmē privātās un ģimenes dzīves neaizskaramību un personas datu aizsardzību, kā paredzēts Eiropas Savienības Pamattiesību hartas 7. un 8. pantā, šādu datu nosūtīšana būtu jāveic, pilnībā ievērojot nepieciešamības, samērīguma un mērķa ierobežojuma principus un tikai nolūkā identificēt personas, uz kurām attiecas ar teroristu nodarījumiem saistīts kriminālprocess.

- (14) Tā kā informācija par pastāvošajām saiknēm ar citām tiesvedībām ir visnoderīgākā izmeklēšanas agrīnā posmā, ir nepieciešams, lai valsts kompetentās iestādes sniegtu informāciju *Eurojust*, tiklīdz lieta tiek nodota tiesu iestādei saskaņā ar valsts tiesību aktiem. Atkarībā no piemērojamiem valsts tiesību aktiem lieta būtu jāuzskata par nodotu tiesu iestādei tad, ja, piemēram, tiesu iestāde ir informēta par notiekošu izmeklēšanu, apstiprina vai uzdod veikt izmeklēšanas pasākumu vai nolemj veikt kriminālvajāšanu. Ja kādai valsts kompetentai iestādei jau ir zināms par saiknēm starp kriminālprocesu savā dalībvalstī un kriminālprocesu citā dalībvalstī, tai būtu attiecīgi jāinformē *Eurojust*.
- (15) Ņemot vērā to, ka dažu dalībvalstu tiesību tradīcijās un sistēmās tiesu iestāde neuzrauga izmeklēšanas un ir iesaistīta tikai vēlākos procesa posmos, šai regulai nebūtu jāliedz valsts kompetentajām iestādēm informāciju par terorisma izmeklēšanām saviem valsts pārstāvjiem sniegt agrākā posmā saskaņā ar saviem valsts tiesību aktiem.

- (16) Lai nodrošinātu Eiropas Tiesu iestāžu pretterorisma reģistrā iekļauto datu precizitāti, pēc iespējas agrīnā izmeklēšanas posmā identificētu saiknes vai noskaidrotu aizdomās turētā identitāti un lai nodrošinātu termiņu ievērošanu, valsts kompetentajām iestādēm būtu jāatjaunina to sniegtā informācija. Šādos atjauninājumos būtu jāiekļauj jauna informācija par personu, pret kuru notiek izmeklēšana, tiesas lēmumiem, piemēram, par pirmstiesas apcietinājumu, tiesas procesa sākšanu, attaisnošanām un galīgiem lēmumiem nesaukt pie kriminālatbildības, kā arī par tiesiskās sadarbības lūgumiem vai identificētajām saiknēm ar citām jurisdikcijām.
- (17) Valsts kompetentajām iestādēm nevajadzētu būt pienākumam agrīnākajā posmā kopīgot ar *Eurojust* informāciju par teroristu nodarījumiem, ja, to darot, varētu tikt apdraudēta notiekošu lietu izmeklēšana vai kādas personas drošība vai tas varētu būt pretrunā būtiskām attiecīgās dalībvalsts drošības interesēm. Šādas atkāpes no pienākuma kopīgot informāciju būtu jāpiemēro tikai ārkārtas apstākļos un izvērtējot katru gadījumu atsevišķi. Apsverot, vai piemērot atkāpi no šā pienākuma, valsts kompetentajām iestādēm būtu pienācīgi jāņem vērā tas, ka *Eurojust* ar šādu iestāžu sniegto informāciju rīkojas saskaņā ar Savienības datu aizsardzības tiesību aktiem, un tiesvedības konfidencialitāte.

- (18) Lai apmainītos ar sensitīviem datiem starp valsts kompetentajām iestādēm un *Eurojust* un apstrādātu šādus datus, būtu jāizmanto droši sakaru kanāli, piemēram, decentralizēta IT sistēma vai droši tālsakaru savienojumi, kas minēti Padomes Lēmumā 2008/976/TI¹, nolūkā aizsargāt šādus datus pret neatļautu izpaušanu un kiberuzbrukumiem. Šādai izmantošanai nebūtu jāskar tehnoloģiju attīstība nākotnē.
- (19) Lai droši apmainītos ar datiem un aizsargātu sakaru un datu apmaiņas integritāti, lietu pārvaldības sistēmai vajadzētu būt savienotai ar šādiem drošiem sakaru kanāliem un būtu jāatbilst augstiem kiberdrošības standartiem. Šādus drošus sakaru kanālus var izmantot arī tam, lai lietu pārvaldības sistēmu savienotu ar citām Savienības informācijas sistēmām, ciktāl minēto sistēmu izveides tiesību akti paredz *Eurojust* piekļuvi.

¹ Padomes Lēmums 2008/976/TI (2008. gada 16. decembris) par Eiropas Tiesiskās sadarbības tīklu (OV L 348, 24.12.2008., 130. lpp.).

- (20) Decentralizētajai IT sistēmai būtu jādod iespēja veikt drošu datu apmaiņu starp valsts kompetentajām iestādēm un *Eurojust*, šādas apmaiņas norisē pēc būtības neiesaistot nevienu Savienības iestādi, struktūru, biroju vai aģentūru. Decentralizētā IT sistēma būtu jāveido no dalībvalstu un *Eurojust* IT aizmugursistēmām, kas ir savstarpēji savienotas ar sadarbspējīgiem piekļuves punktiem. Decentralizētās IT sistēmas piekļuves punktu pamatā vajadzētu būt *e-CODEX*.
- (21) Lai nodrošinātu vienotus nosacījumus šīs regulas īstenošanai attiecībā uz decentralizētās IT sistēmas izveidi un lietošanu lietās, uz kurām attiecas šī regula, būtu jāpiešķir īstenošanas pilnvaras Komisijai. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011¹.

¹ Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).

- (22) Nestrukturētu datu nosūtīšana rada nepieciešamību pēc manuālas iejaukšanās, kā arī papildu administratīvo slogu un samazina šķērspārbaužu rezultātu kvalitāti. Tāpēc valsts kompetentajām iestādēm dati būtu jānosūta strukturētā veidā, vienlaikus izpildot minimālās sadarbības prasības, kas noteiktas Eiropas sadarbības satvarā, kas minēts Komisijas 2017. gada 23. marta paziņojumā “Eiropas sadarbības satvars – Īstenošanas stratēģija”. Turklāt datu pārsūtīšana būtu pēc iespējas jāautomatizē, lai samazinātu valsts kompetento iestāžu administratīvo slogu un nodrošinātu nepieciešamo datu regulāru un ātru sniegšanu.
- (23) Lai *Eurojust* varētu droši apstrādāt sensitīvus personas datus, ir nepieciešama modernizēta lietu pārvaldības sistēma. Jaunajā sistēmā jābūt integrētām un iespējotām Eiropas Tiesu iestāžu pretterorisma reģistra funkcionalitātēm, un tai būtu jāuzlabo *Eurojust* spēja identificēt saiknes, vienlaikus pilnībā izmantojot pastāvošos valstu un Savienības mehānismus biometrisko datu salīdzināšanai.

- (24) Ir svarīgi saglabāt valsts pārstāvju kontroli pār datiem, ko viņi saņem no valsts kompetentajām iestādēm, un atbildību par tiem. Nekādus operatīvos personas datus nevajadzētu kopīgot ar citu dalībvalsti pēc noklusējuma. Operatīvie personas dati būtu jākopīgo tikai tiktāl, ciktāl valsts kompetentās iestādes atļauj datu apmaiņu. Lai digitalizētu un paātrinātu iespējamo saikņu uzraudzību, vienlaikus nodrošinot pilnīgu kontroli pār datiem, būtu jāievieš apstrādes kodi.
- (25) Mūsdienās terorisms, smagi noziegumi un organizētā noziedzība ir ļoti dinamiskas un globalizētas parādības, kas bieži skar divas vai vairākas dalībvalstis. Kaut gan terorismam jau agrāk piemita izteikts transnacionāls komponents, elektroniskās saziņas lietošanas un pieejamības rezultātā transnacionāla sadarbība starp teroristu nodarījumu izdarītājiem ir ievērojami palielinājusies. Kad lieta tiek nodota tiesu iestādei, teroristu nodarījuma transnacionālais raksturs var nebūt zināms, bet to varētu atklāt *Eurojust* veiktas datu šķērspārbaudes laikā. Tāpēc teroristu nodarījumu izmeklēšanai vai kriminālvajāšanai par tiem ir nepieciešama koordinācija un sadarbība starp iestādēm, kas veic kriminālvajāšanu, vai kopīga kriminālvajāšana, kā paredzēts Līguma par Eiropas Savienības darbību (LESD) 85. pantā. Informācijas apmaiņa ar *Eurojust* par terorisma lietām būtu jāveic laikus, ja vien lietas īpašie apstākļi skaidri nenorāda, ka tā attiecas tikai uz vienu valsti.

- (26) Izmeklēšanu un kriminālvajāšanu terorisma lietās bieži kavē informācijas apmaiņas trūkums starp valstu izmeklēšanas un kriminālvajāšanas iestādēm. Lai varētu veikt jaunu terorisma izmeklēšanu šķērspārbaudes attiecībā pret iepriekšējām izmeklēšanām un konstatēt iespējamās saiknes, ir nepieciešams nodrošināt, ka datu glabāšanas periods attiecībā uz visām iepriekšējām izmeklēšanām un notiesāšanām ir adekvāts operatīvo darbību vajadzībām. Tādēļ ir nepieciešams pagarināt termiņus datu glabāšanai Eiropas Tiesu iestāžu pretterorisma reģistrā.
- (27) Iespēja veikt jaunu terorisma izmeklēšanu šķērspārbaudes attiecībā pret iepriekšējām izmeklēšanām var palīdzēt konstatēt potenciālas saiknes un no tās izriet nepieciešamība pēc sadarbības. Šādu šķērspārbaudu veikšana varētu atklāt, ka persona, kuru tur aizdomās vai pret kuru notiek kriminālvajāšana kādā dalībvalstī notiekošā lietā, tika turēta aizdomās vai pret to tika veikta kriminālvajāšana kādā jau pabeigtā lietā citā dalībvalstī. Tā varētu arī konstatēt saiknes starp notiekošām izmeklēšanām vai kriminālvajāšanām, kas citādi nebūtu zināmas. Tas attiecas arī uz gadījumiem, kad iepriekšējās izmeklēšanas ir beigušās ar attaisnošanu vai ar galīgu lēmumu nesaukt pie kriminālatbildības. Tāpēc attiecīgā gadījumā ir jāglabā dati par visām iepriekšējām izmeklēšanām, ne tikai par notiesājošiem spriedumiem.

- (28) Ir jānodrošina, ka dati no izmeklēšanām, kas beigušās ar attaisnošanu vai galīgu lēmumu nesaukt pie kriminālatbildības, tiek apstrādāti tikai kriminālvajāšanas nolūkos. Šādus datus nedrīkst izmantot nekādiem citiem mērķiem, kā vien lai identificētu saiknes ar notiekošām izmeklēšanām un kriminālvajāšanām un atbalstītu šādas izmeklēšanas un kriminālvajāšanas. Ja vien valsts kompetentā iestāde nav nolēmusi citādi, *Eurojust*, izskatot katru gadījumu atsevišķi, vajadzētu būt iespējai turpināt apstrādāt šādus operatīvos datus. Ja pēc tam, kad lēmums attaisnot vai nesaukt pie kriminālatbildības ir kļuvis galīgs, valsts kompetentā iestāde nolemj, ka attaisnoto vai pie kriminālatbildības nesaukto personu datu apstrāde nav nepieciešama, tostarp lietas specifiskuma vai attaisnošanas vai nesaukšanas pie kriminālatbildības iemeslu dēļ, minētie dati būtu jādzēš.
- (29) *Eurojust* ir noslēgusi ar trešām valstīm 12 sadarbības nolīgumus, kas ļauj pārsūtīt operatīvos personas datus, kā arī norīkot trešo valstu prokuroorus koordinatorus darbam *Eurojust*. Arī Tirdzniecības un sadarbības nolīgums starp Eiropas Savienību un Eiropas Atomenerģijas kopienu, no vienas puses, un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, no otras puses¹, ļauj norīkot prokurooru koordinatoru. 2021. gada martā Padome piešķīra Komisijai pilnvaras risināt sarunas par sadarbības nolīgumiem starp *Eurojust* un vēl 13 trešām valstīm, proti, ar Alžīriju, Argentīnu, Armēniju, Bosniju un Hercegovinu, Brazīliju, Ēģipti, Izraēlu, Jordāniju, Kolumbiju, Libānu, Maroku, Tunisiju un Turciju.

¹ OV L 149, 30.4.2021., 10. lpp.

- (30) Lai gan Regula (ES) 2018/1727 nodrošina juridisko pamatu sadarbībai un datu apmaiņai ar trešām valstīm, tā nesatur nekādus noteikumus par formālajiem un tehniskajiem aspektiem sadarbībā ar trešo valstu prokuroriem koordinatoriem, kas norīkoti darbam *Eurojust*, jo īpaši attiecībā uz viņu piekļuvi lietu pārvaldības sistēmai. Juridiskās noteiktības labad Regulā (ES) 2018/1727 būtu jāsniedz skaidrs juridiskais pamats sadarbībai starp *Eurojust* un trešo valstu prokuroriem koordinatoriem un viņu piekļuvei lietu pārvaldības sistēmai. *Eurojust* būtu jāīsteno atbilstīgi aizsardzības pasākumi un drošības pasākumi datu un pamattiesību aizsardzībai, izmantojot atjauninātu tehnisko uzbūvi un stingrus iekšējos noteikumus.

- (31) Apstrādājot operatīvos personas datus saskaņā ar šo regulu, *Eurojust* būtu jānodrošina augsts datu aizsardzības līmenis. Operatīvo personas datu apstrādei *Eurojust* piemēro Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725¹ 3. pantu un IX nodaļu, kā arī īpašos noteikumus par operatīvo personas datu apstrādi, kas paredzēti Regulā (ES) 2018/1727, kura grozīta ar Eiropas Parlamenta un Padomes Regulu (ES) 2022/838² un šo regulu. Minētos noteikumus piemēro visai *Eurojust* apstrādāto operatīvo personas datu apstrādei. Jo īpaši tos piemēro visiem operatīvajiem personas datiem, ko apstrādā lietu pārvaldības sistēmā, neatkarīgi no tā, vai tos apstrādā valsts pārstāvji, valsts korespondenti, prokurori koordinatori vai citas pilnvarotas personas saskaņā ar Regulu (ES) 2018/1727.
- (32) Lēmumiem par to, vai un kā *Eurojust* būtu jāatbalsta koordinācija un sadarbība starp iestādēm, kas veic izmeklēšanas un kriminālvajāšanas, būtu jāpaliek vienīgi attiecīgo dalībvalstu kompetento iestāžu ziņā, ievērojot piemērojamos valsts tiesību aktus, Savienības tiesību aktus vai starptautiskos tiesību aktus, kas ietver konvencijas vai citus starptautiskus nolīgumus par savstarpēju palīdzību krimināllietās.

¹ Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

² Eiropas Parlamenta un Padomes Regula (ES) 2022/838 (2022. gada 30. maijs), ar ko groza Regulu (ES) 2018/1727 attiecībā uz *Eurojust* veiktu tādu pierādījumu saglabāšanu, analīzi un uzglabāšanu, kas saistīti ar genocīdu, noziegumiem pret cilvēci, kara noziegumiem un saistītiem noziedzīgiem nodarījumiem (OV L 148, 31.5.2022., 1. lpp.).

- (33) Juridiskās noteiktības labad būtu jāprecizē saikne starp informācijas apmaiņu, kas notiek starp valsts kompetentajām iestādēm un *Eurojust* par terorisma lietām saskaņā ar Lēmumu 2005/671/TI un saskaņā ar Regulu (ES) 2018/1727. Tāpēc attiecīgie noteikumi būtu jāsvīturo no Lēmuma 2005/671/TI un būtu jāiekļauj Regulā (ES) 2018/1727.
- (34) Lai gan dažas valsts kompetentās iestādes jau ir pieslēgtas drošam tālsakaru savienojumam, kas minēts Lēmuma 2008/976/TI 9. pantā, daudzas valsts kompetentās iestādes vēl nav savienotas ar minēto drošo tālsakaru savienojumu vai drošiem sakaru kanāliem. Lai nodrošinātu, ka dalībvalstīm ir pietiekami daudz laika, lai valsts kompetentajām iestādēm nodrošinātu šādu savienojumu, īstenošanai būtu jāparedz pārejas periods.

- (35) Saskaņā ar 1. un 2. pantu un 4.a panta 1. punktu Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots Līgumam par Eiropas Savienību (LES) un LESD, un neskarot minētā protokola 4. pantu, Īrija nepiedalās šīs regulas pieņemšanā, un šī regula tai nav saistoša un nav jāpiemēro.
- (36) Saskaņā ar 1. un 2. pantu Protokolā Nr. 22 par Dānijas nostāju, kas pievienots LES un LESD, Dānija nepiedalās šīs regulas pieņemšanā, un šī regula tai nav saistoša un nav jāpiemēro.
- (37) Saskaņā ar Regulas (ES) 2018/1725 42. pantu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2022. gada 26. janvārī sniedza atzinumu,

IR PIEŅĒMUŠI ŠO REGULU.

1. pants
Grozījumi Regulā (ES) 2018/1727

Regulu (ES) 2018/1727 groza šādi:

1) regulas 3. panta 5. punktu aizstāj ar šādu:

"5. *Eurojust* var palīdzēt arī tādā izmeklēšanā un kriminālvajāšanā, kas skar tikai kādu dalībvalsti un trešo valsti vai kādu dalībvalsti un starptautisku organizāciju, ar noteikumu, ka ar minēto trešo valsti vai starptautisko organizāciju ir noslēgts sadarbības nolīgums vai vienošanās, ar ko izveido sadarbību saskaņā ar 52. pantu, vai ar noteikumu, ka konkrētā gadījumā ir ievērojama interese, lai tiktu sniegta šāda palīdzība.

Lēmums par to, vai un kā dalībvalstis sniedz tiesisko palīdzību kādai trešai valstij vai starptautiskai organizācijai, paliek vienīgi attiecīgās dalībvalsts kompetentās iestādes ziņā, ievērojot piemērojamos valsts tiesību aktus, Savienības vai starptautiskos tiesību aktus.";

2) regulas 20. pantu groza šādi:

a) pantā iekļauj šādu punktu:

"2.a Katra dalībvalsts izraugās kādu kompetento iestādi par *Eurojust* valsts korespondentu terorisma jautājumos. Minētais valsts korespondents terorisma jautājumos ir tiesu iestāde vai cita kompetentā iestāde. Ja valsts tiesību sistēma to prasa, dalībvalstij ir iespēja izraudzīties vairāk nekā vienu valsts kompetento iestādi par *Eurojust* valsts korespondentu terorisma jautājumos. Valsts korespondentam terorisma jautājumos ir piekļuve visai attiecīgajai informācijai saskaņā ar 21. a panta 1. punktu. Tas ir kompetents vākt šādu informāciju un nosūtīt to *Eurojust* saskaņā ar valsts un Savienības tiesību aktiem, jo īpaši valsts kriminālprocesuālajiem tiesību aktiem un piemērojamiem datu aizsardzības noteikumiem.";

b) panta 8. punktu aizstāj ar šādu:

"8. Lai sasniegtu šā panta 7. punktā minētos mērķus, personas, kas minētas šā panta 3. punkta a), b) un c) apakšpunktā, pievieno lietu pārvaldības sistēmai saskaņā ar šo pantu un 23., 24., 25. un 34. pantu. Izmaksas saistībā ar pievienošanu lietu pārvaldības sistēmai sedz no Savienības vispārējā budžeta.";

3) regulas 21. pantu groza šādi:

a) panta 9. punktu aizstāj ar šādu:

"9. Šis pants neskar citus pienākumus, kas saistīti ar informācijas nosūtīšanu *Eurojust.*";

b) panta 10. punktu aizstāj ar šādu:

"10. Valsts kompetentajām iestādēm nav pienākuma sniegt šajā pantā minēto informāciju, ja šāda informācija jau nosūtīta *Eurojust* saskaņā ar citiem šīs regulas noteikumiem.";

4) iekļauj šādu pantu:

"21.a pants

Informācijas apmaiņa terorisma lietās

- "1. Attiecībā uz teroristu nodarījumiem valsts kompetentās iestādes informē savus valsts pārstāvjus par visām notiekošām vai pabeigtām kriminālizmeklēšanām, ko uzrauga tiesu iestādes, tiklīdz lietu nodod tiesu iestādēm saskaņā ar valsts tiesību aktiem, jo īpaši valsts kriminālprocesuālajiem tiesību aktiem, par visām notiekošām vai pabeigtām kriminālvajāšanām un tiesas procesiem un par jebkādiem tiesas lēmumiem par teroristu nodarījumiem. Minētais pienākums attiecas uz visām kriminālizmeklēšanām, kas saistītas ar teroristu nodarījumiem, neatkarīgi no tā, vai ir zināma saikne ar citu dalībvalsti vai kādu trešo valsti, ja vien kriminālizmeklēšana tās īpašo apstākļu dēļ nepārprotami neskar tikai vienu dalībvalsti.
2. Šā panta 1. punktu nepiemēro, ja:
 - a) informācijas apmaiņa apdraudētu kādu notiekošu izmeklēšanu vai kādas personas drošību; vai
 - b) informācijas apmaiņa būtu pretrunā būtiskām attiecīgās dalībvalsts drošības interesēm.
3. Teroristu nodarījumi šā panta nozīmē ir Eiropas Parlamenta un Padomes Direktīvā (ES) 2017/541* minētie nodarījumi.

4. Saskaņā ar 1. punktu nodotā informācija ietver III pielikumā izklāstītos operatīvos personas datus un nepersonālos datus. Šāda informācija var ietvert personas datus saskaņā ar III pielikuma d) punktu, bet tikai tad, ja šādi personas dati ir valsts kompetento iestāžu rīcībā vai tos var tām paziņot saskaņā ar valsts tiesību aktiem un ja to nosūtīšana ir nepieciešama, lai ticami identificētu datu subjektu saskaņā ar 27. panta 5. punktu.
5. Ievērojot 2. punktu, valsts kompetentās iestādes bez liekas kavēšanās un, ja iespējams, ne vēlāk kā 10 darba dienās pēc šādām izmaiņām informē savus valsts pārstāvjus par visām izmaiņām informācijā, kas nosūtīta saskaņā ar 1. punktu.
6. Valsts kompetentajai iestādei nav pienākuma sniegt šādu informāciju, ja tā jau nosūtīta *Eurojust*.
7. Valsts kompetentā iestāde jebkurā posmā var lūgt *Eurojust* atbalstu turpmākiem pasākumiem attiecībā uz saiknēm, kas identificētas, pamatojoties uz informāciju, kas sniegta saskaņā ar šo pantu.

* Eiropas Parlamenta un Padomes Direktīva (ES) 2017/541 (2017. gada 15. marts) par terorisma apkarošanu un ar ko aizstāj Padomes Pamatlēmumu 2002/475/TI un groza Padomes Lēmumu 2005/671/TI (OV L 88, 31.3.2017., 6. lpp.).";

5) iekļauj šādus pantus:

"22.a pants

Droša digitālā saziņa un datu apmaiņa starp valsts kompetentajām iestādēm un Eurojust

1. Saziņu starp valsts kompetentajām iestādēm un *Eurojust* saskaņā ar šo regulu veic, izmantojot decentralizēto IT sistēmu. Šīs regulas 23. pantā minētā lietu pārvaldības sistēmu savieno ar IT sistēmu un sadarbspējīgu *e-CODEX* piekļuves punktu tīklu, kas darbojas katras dalībvalsts un *Eurojust* individuālā atbildībā un pārvaldībā, ļaujot veikt drošu un uzticamu informācijas pārrobežu apmaiņu ("decentralizēta IT sistēma").
2. Ja informācijas apmaiņa saskaņā ar 1. punktu nav iespējama decentralizētās IT sistēmas nepieejamības vai ārkārtēju apstākļu dēļ, to veic, izmantojot ātrākos un piemērotākos alternatīvos līdzekļus. Dalībvalstis un *Eurojust* nodrošina, ka alternatīvie saziņas līdzekļi ir uzticami un nodrošina līdzvērtīgu drošības un datu aizsardzības līmeni.

3. Valsts kompetentās iestādes šīs regulas 21. un 21.a pantā minēto informāciju nosūta *Eurojust* daļēji automatizētā un strukturētā veidā no valstu reģistriem. Šādas nosūtīšanas kārtību Komisija, apspriežoties ar *Eurojust*, nosaka īstenošanas aktā saskaņā ar šīs regulas 22.b pantu. Konkrēti, minētajā īstenošanas aktā nosaka to datu formātu, kurus nosūta, ievērojot šīs regulas III pielikuma d) punktu, un nepieciešamos tehniskos standartus attiecībā uz šādu datu nosūtīšanu, un tajā izklāsta digitālos procesuālos standartus, kas definēti Eiropas Parlamenta un Padomes Regulas (ES) 2022/850* 3. panta 9. punktā.
4. Komisija ir atbildīga par tādas references īstenošanas programmatūras izveidi, uzturēšanu un attīstīšanu, ko dalībvalstis un *Eurojust* var izvēlēties piemērot kā savu aizmugursistēmu. Minētās references īstenošanas programmatūras pamatā ir modulāra uzbūve, kas nozīmē, ka programmatūra ir pakotnē un piegādāta atsevišķi no *e-CODEX* komponentiem, kuri vajadzīgi, lai to savienotu ar decentralizēto IT sistēmu. Minētā uzbūve ir tāda, kas dod iespēju dalībvalstīm pārrobežu lietojuma vajadzībām atkārtoti lietot vai paplašināt savas esošās valsts tiesu iestāžu saziņas infrastruktūras un kas ļauj *Eurojust* savienot savu lietu pārvaldības sistēmu ar decentralizēto IT sistēmu.

5. Komisija references īstenošanas programmatūru nodrošina, uztur un atbalsta bez maksas. References īstenošanas programmatūras izveidi, uzturēšanu un attīstīšanu finansē no Savienības vispārējā budžeta.
6. Dalībvalstis un *Eurojust* sedz savas attiecīgās izmaksas par Regulas (ES) 2022/850 3. panta 3. punktā definētā autorizētā *e-CODEX* piekļuves punkta izveidi un darbību un par savu attiecīgo IT sistēmu izveidi un koriģēšanu nolūkā padarīt tās sadarbspējīgas ar piekļuves punktiem.

22.b pants

Īstenošanas akti, ko pieņem Komisija

1. Komisija pieņem īstenošanas aktus, kuri vajadzīgi, lai izveidotu un izmantotu decentralizēto IT sistēmu saziņai saskaņā ar šo regulu, un kuros nosaka:
 - a) tehniskās specifikācijas, kas definē elektroniskās saziņas metodes decentralizētās IT sistēmas vajadzībām;
 - b) komunikācijas protokolu tehniskās specifikācijas;

- c) informācijas drošības mērķus un attiecīgos tehniskos pasākumus, kas nodrošina minimālos informācijas drošības standartus un augsta kibernetikas drošības līmeņa standartus informācijas apstrādei un paziņošanai decentralizētajā IT sistēmā;
 - d) minimālos pieejamības mērķus un iespējamās saistītās tehniskās prasības attiecībā uz pakalpojumiem, ko sniedz decentralizētā IT sistēma;
 - e) tādas koordinācijas komitejas izveidi, kurā ir dalībvalstu pārstāvji, lai nodrošinātu decentralizētās IT sistēmas darbību un uzturēšanu nolūkā sasniegt šīs regulas mērķus.
2. Šā panta 1. punktā minētos īstenošanas aktus pieņem līdz ... [divi gadi pēc šīs grozošās regulas spēkā stāšanās dienas] saskaņā ar 22.c panta 2. punktā minēto pārbaudes procedūru.

22.c pants

Komiteju procedūra

1. Komisijai palīdz komiteja. Minētā komiteja ir komiteja Eiropas Parlamenta un Padomes Regulas (ES) Nr. 182/2011** nozīmē.
2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.

Ja komiteja atzinumu nesniedz, Komisija nepieņem īstenošanas akta projektu un tiek piemērota Regulas (ES) Nr. 182/2011 5. panta 4. punkta trešā daļa.

* Eiropas Parlamenta un Padomes Regula (ES) 2022/850 (2022. gada 30. maijs) par datorizētu sistēmu datu pārrobežu elektroniskai apmaiņai tiesu iestāžu sadarbības civillietās un krimināllietās jomā (*e-CODEX* sistēma) un ar ko groza Regulu (ES) 2018/1726 (OV L 150, 1.6.2022., 1. lpp.).

** Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).";

6) regulas 23., 24. un 25. pantu aizstāj ar šādiem:

"23. pants

Lietu pārvaldības sistēma

1. *Eurojust* izveido lietu pārvaldības sistēmu II pielikumā uzskaitīto operatīvo personas datu, III pielikumā uzskaitīto datu un nepersondatu apstrādei.
2. Lietu pārvaldības sistēmas uzdevumi ir:
 - a) atbalstīt tādu izmeklēšanas un kriminālvajāšanas lietu pārvaldību un koordinēšanu, saistībā ar kuru *Eurojust* sniedz palīdzību;
 - b) nodrošināt drošu piekļuvi informācijai par notiekošu izmeklēšanu un kriminālvajāšanu un drošu šīs informācijas apmaiņu;
 - c) nodrošināt iespēju veikt informācijas šķērspārbaudi un identificēt saiknes;
 - d) nodrošināt iespēju izgūt datus operatīviem un statistikas nolūkiem;
 - e) atvieglot pārraudzību, kuras mērķis ir nodrošināt, ka operatīvo personas datu apstrāde ir likumīga un atbilst šai regulai un piemērojamajiem datu aizsardzības noteikumiem.

3. Lietu pārvaldības sistēmu var saistīt ar drošu tālsakaru savienojumu, kas minēts Padomes Lēmuma 2008/976/TI* 9. pantā, un citiem drošiem sakaru kanāliem saskaņā ar piemērojamajiem Savienības tiesību aktiem.
4. Ja *Eurojust* ir piešķirta piekļuve datiem citās Savienības informācijas sistēmās vai no citām Savienības informācijas sistēmām, kas izveidotas saskaņā ar citiem Savienības tiesību aktiem, tā var izmantot lietu pārvaldības sistēmu, lai piekļūtu datiem šādās informācijas sistēmās vai lai pievienotos šādām informācijas sistēmām nolūkā izgūt un apstrādāt informāciju, tostarp personas datus, ar noteikumu, ka tas ir nepieciešams tās uzdevumu veikšanai un ir saskaņā ar Savienības tiesību aktiem, ar ko šādas informācijas sistēmas izveido.
5. Šā panta 3. un 4. punkts nepaplašina *Eurojust* piešķirtās piekļuves tiesības attiecībā uz citām Savienības informācijas sistēmām saskaņā ar Savienības tiesību aktiem, ar ko izveidotas minētās sistēmas.
6. Pildot savus pienākumus, valsts pārstāvji var apstrādāt personas datus attiecībā uz atsevišķām lietām, ar kurām tie strādā, saskaņā ar šo regulu vai citiem piemērojamajiem instrumentiem. Tie ļauj datu aizsardzības speciālistam piekļūt lietu pārvaldības sistēmā apstrādātajiem personas datiem.

7. Operatīvo personas datu apstrādei *Eurojust* neizveido citu automatizētu datu datni kā vien to, kas ir lietu pārvaldības sistēmā.

Valsts pārstāvji var uz laiku uzglabāt un analizēt personas datus, lai noteiktu, vai šādi dati ir būtiski saistībā ar *Eurojust* uzdevumiem un vai tos var iekļaut lietu pārvaldības sistēmā. Minētos datus var uzglabāt ne ilgāk par trim mēnešiem.

24. pants

Informācijas pārvaldība lietu pārvaldības sistēmā

1. Valsts pārstāvis informāciju, kas minētajam valsts pārstāvim nosūtīta saskaņā ar šo regulu vai citiem piemērojamajiem instrumentiem, uzglabā lietu pārvaldības sistēmā.

Valsts pārstāvis ir atbildīgs par to datu pārvaldību, kurus minētais valsts pārstāvis apstrādā.

2. Valsts pārstāvis katrā atsevišķā gadījumā pieņem lēmumu, vai saglabāt ierobežotu piekļuvi informācijai vai atļaut piekļūt tai vai tās daļām citiem valsts pārstāvjiem, prokuroriem koordinatoriem, kas norīkoti darbā *Eurojust*, pilnvarotajiem *Eurojust* darbiniekiem vai jebkurai citai personai, kas strādā *Eurojust* uzdevumā un ir saņēmusi nepieciešamo administratīvā direktora atļauju.
3. Valsts pārstāvis, apspriežoties ar valsts kompetentajām iestādēm, vispārīgi vai konkrēti norāda visus ierobežojumus, ko piemēro turpmākai informācijas apstrādei, piekļuvei tai un tās pārsūtīšanai, ja ir identificēta 23. panta 2. punkta c) apakšpunktā minētā saikne.

25. pants

Piekļuve lietu pārvaldības sistēmai valsts līmenī

1. Personām, kas minētas 20. panta 3. punkta a), b) un c) apakšpunktā, ir piekļuve tikai šādiem datiem:
 - a) datiem, ko kontrolē viņu dalībvalsts valsts pārstāvis;
 - b) datiem, kurus kontrolē citu dalībvalstu valsts pārstāvji un kuriem viņu dalībvalsts valsts pārstāvis ir saņēmis piekļuvi, ja vien valsts pārstāvis, kurš datus kontrolē, šādu piekļuvi nav liedzis.

2. Valsts pārstāvis, ievērojot šā panta 1. punktā paredzētos ierobežojumus, lemj par to, kāda apmēra piekļuvi viņa dalībvalstī piešķir personām, kuras minētas 20. panta 3. punkta a), b) un c) apakšpunktā.
3. Datiem, kas sniegti saskaņā ar 21. a pantu, valsts līmenī var piekļūt tikai *Eurojust* valsts korespondenti terorisma jautājumos, kas minēti 20. panta 3. punkta c) apakšpunktā.
4. Katra dalībvalsts pēc apspriešanās ar savu valsts pārstāvi var nolemt, ka 20. panta 3. punkta a), b) un c) apakšpunktā minētās personas, ievērojot šā panta 1., 2. un 3. punktā paredzētos ierobežojumus, var ievadīt lietu pārvaldības sistēmā informāciju, kas attiecas uz viņu dalībvalsti. Ievadīto informāciju apstiprina attiecīgais valsts pārstāvis. Sīkākus šā punkta praktiskās īstenošanas aspektus nosaka Kolēģija. Dalībvalstis paziņo *Eurojust* un Komisijai par savu lēmumu attiecībā uz šā punkta īstenošanu. Komisija par to informē pārējās dalībvalstis.

* Padomes Lēmums 2008/976/TI (2008. gada 16. decembris) par Eiropas Tiesiskās sadarbības tīklu (OV L 348, 24.12.2008., 130. lpp.).";

7) regulas 27. pantu groza šādi:

a) panta 4. punktu aizstāj ar šādu:

"4. *Eurojust* var apstrādāt īpašas operatīvo personas datu kategorijas saskaņā ar Regulas (ES) 2018/1725 76. pantu. Ja šādi citi dati attiecas uz lieciniekiem vai cietušajiem šā panta 2. punkta nozīmē, lēmumu tos apstrādāt pieņem attiecīgie valsts pārstāvji.";

b) pantam pievieno šādu punktu:

"5. Ja operatīvos personas datus nosūta saskaņā ar 21.a pantu, *Eurojust* var apstrādāt šādu personu operatīvos personas datus, kas uzskaitīti III pielikumā:

a) personas, par kurām saskaņā ar attiecīgās dalībvalsts tiesību aktiem ir nopietns pamats uzskatīt, ka tās ir izdarījušas vai gatavojas izdarīt noziedzīgu nodarījumu, kas ir *Eurojust* kompetencē;

- b) personas, kuras ir notiesātas par šādu noziedzīgu nodarījumu.

Ja vien valsts kompetentā iestāde nenolemj citādi, katru gadījumu skatot atsevišķi, *Eurojust* var turpināt pirmās daļas a) apakšpunktā minēto operatīvo personas datu apstrādi arī pēc tam, kad tiesvedība ir pabeigta saskaņā ar attiecīgās dalībvalsts tiesību aktiem, pat attaisnošanas gadījumā vai ja ir pieņemts galīgs lēmums nesaukt pie kriminālatbildības. Ja tiesvedības rezultātā nav pieņemts notiesājošs spriedums, operatīvo personas datu apstrādi veic tikai, lai identificētu saiknes starp notiekošām, turpmākām vai pabeigtām izmeklēšanām un kriminālvajāšanām, kā minēts 23. panta 2. punkta c) apakšpunktā.";

- 8) regulas 29. pantu groza šādi:

- a) pantā iekļauj šādu punktu:

"1.a. *Eurojust* operatīvos personas datus, kas nosūtīti saskaņā ar 21.a pantu, neuzglabā ilgāk par agrāko no šiem datumiem:

- a) datums, kurā kriminālvajāšana ir izbeigta noilguma dēļ visās dalībvalstīs, kas saistītas ar attiecīgo izmeklēšanu vai kriminālvajāšanu;

- b) pieci gadi pēc datuma, kurā tiesas nolēmums pēdējā no dalībvalstīm, kas saistītas ar attiecīgo izmeklēšanu vai kriminālvajāšanu, ir kļuvis galīgs, vai divi gadi attaisnošanas gadījumā vai ja ir pieņemts galīgs lēmums nesaukt pie kriminālatbildības;
- c) datums, kurā *Eurojust* tiek informēta par valsts kompetentās iestādes lēmumu, ievērojot 27. panta 5. punktu.";

b) panta 2. un 3. punktu aizstāj ar šādiem:

"2. Šā panta 1. un 1.a. punktā minēto glabāšanas termiņu ievērošanu pastāvīgi pārbauda, *Eurojust* veicot atbilstīgu automatizētu apstrādi, jo īpaši no brīža, kad *Eurojust* pārtrauc sniegt atbalstu.

Reizi trijos gados pēc datu ievadīšanas pārskata arī datu uzglabāšanas nepieciešamību.

Ja 27. panta 4. punktā minētos operatīvos personas datus glabā ilgāk par pieciem gadiem, par to informē EDAU.

3. Pirms beidzas viens no 1. un 1.a. punktā minētajiem glabāšanas termiņiem, *Eurojust* pārskata nepieciešamību arī turpmāk uzglabāt operatīvos personas datus, ja un cik ilgi tas ir nepieciešams, lai tā varētu pildīt savus uzdevumus.

Izņēmuma kārtā tā var nolemt uzglabāt minētos datus līdz nākamajai pārskatīšanai. Turpmākas glabāšanas iemeslus pamato un reģistrē. Ja pārskatīšanas laikā netiek pieņemts lēmums par operatīvo personas datu turpmāko glabāšanu, minētos datus automātiski dzēš.";

- 9) iekļauj šādu pantu:

"54.a pants

Trešo valstu prokurori koordinatori

1. Darbā *Eurojust* var norīkot prokuroru koordinatoru no trešās valsts, pamatojoties uz sadarbības nolīgumu, kas pirms 2019. gada 12. decembra noslēgts starp *Eurojust* un minēto trešo valsti, vai starptautisku nolīgumu, kas, ievērojot LESD 218. pantu, noslēgts starp Savienību un trešo valsti un paredz iespēju norīkot darbā prokuroru koordinatoru.
2. Prokurora koordinatora tiesības un pienākumus izklāsta sadarbības nolīgumā vai starptautiskajā nolīgumā, kas minēts 1. punktā, vai sadarbības vienošanās dokumentā, kas noslēgts saskaņā ar 47. panta 3. punktu.

3. Prokuroriem koordinatoriem, kas norīkoti darbā *Eurojust*, piešķir piekļuvi lietu pārvaldības sistēmai drošas datu apmaiņas nolūkā. Saskaņā ar 45. un 46. pantu *Eurojust* saglabā atbildību par prokuroru koordinatoru veikto personas datu apstrādi lietu pārvaldības sistēmā.

Operatīvo personas datu pārsūtīšana trešo valstu prokuroriem koordinatoriem, izmantojot lietu pārvaldības sistēmu, var notikt tikai saskaņā ar noteikumiem un nosacījumiem, kas izklāstīti šajā regulā, nolīgumā ar attiecīgo valsti vai citos piemērojamajos juridiskajos instrumentos.

Šīs regulas 24. panta 1. punkta otro daļu un 24. panta 2. punktu mutatis mutandis piemēro prokuroriem koordinatoriem.

Kolēģija nosaka sīki izstrādātus piekļuves nosacījumus.";

10) regulas 80. pantam pievieno šādus punktus:

- "9. *Eurojust* var turpināt izmantot lietu pārvaldības sistēmu, kas sastāv no pagaidu darba datnēm un indeksa, līdz ... [nākamā mēneša pirmā diena pēc tam, kad ir pagājuši divi gadi pēc šīs grozošās regulas spēkā stāšanās dienas], ja jaunā lietu pārvaldības sistēma vēl nav ieviesta.
10. Valsts kompetentās iestādes un *Eurojust* var turpināt izmantot citus sakaru kanālus, kas nav minēti 22.a panta 1. punktā, līdz nākamā mēneša pirmajai dienai pēc tam, kad ir pagājuši divi gadi pēc šīs regulas 22.b pantā minētā īstenošanas akta spēkā stāšanās dienas, ja 22.a panta 1. punktā minētie sakaru kanāli vēl nav pieejami tiešai apmaiņai starp tām.
11. Valsts kompetentās iestādes var turpināt sniegt informāciju citos veidos, nevis daļēji automatizētā veidā, saskaņā ar 22.a panta 3. punktu līdz nākamā mēneša pirmajai dienai pēc tam, kad ir pagājuši divi gadi pēc šīs regulas 22.b pantā minētā īstenošanas akta spēkā stāšanās dienas, ja tehniskās prasības vēl nav noteiktas.";

11) pievieno šādu pielikumu:

"III pielikums:

a) informācija, kas nepieciešama, lai identificētu aizdomās turēto, apsūdzēto, notiesāto vai attaisnoto personu:

attiecībā uz fizisku personu:

- uzvārds (dzimtais uzvārds);
- vārds(-i);
- visi pseidonīmi;
- dzimšanas datums;
- dzimšanas vieta (pilsēta un valsts);
- valstspiederība vai valstspiederības;
- identifikācijas dokuments (veids un dokumenta numurs);
- dzimums;
- dzīvesvieta;

attiecībā uz juridisku personu:

- nosaukums;
- juridiskā forma;
- galvenā biroja atrašanās vieta;

attiecībā uz fiziskām un juridiskām personām:

- tālruņa numuri;
- e-pasta adreses;
- informācija par kontiem bankās vai citās finanšu iestādēs;

b) informācija par teroristu nodarījumu:

- informācija par juridiskām personām, kas iesaistītas teroristu nodarījuma sagatavošanā vai veikšanā;
- nodarījuma juridiskā kvalifikācija saskaņā ar valsts tiesību aktiem;
- piemērojamais smaga nozieguma veids no I pielikumā izklāstītā saraksta;

- jebkāda saistība ar teroristu grupu;
 - terorisma veids, piemēram, džihādisti, separātisti, kreisi noskaņotie vai labēji noskaņotie;
 - īss lietas kopsavilkums;
- c) informācija par valsts procesu:
- šāda procesa statuss;
 - atbildīgā prokuratūra;
 - lietas numurs;
 - oficiālas tiesvedības sākšanas datums;
 - saiknes ar citām attiecīgām lietām;
- d) papildu informācija, kas nepieciešama, lai identificētu aizdomās turēto:
- pirkstu nospiedumu dati, kas saskaņā ar valsts tiesību aktiem iegūti kriminālprocesā;
 - fotoattēli."

2. pants

Grozījumi Lēmumā 2005/671/TI

Lēmumu 2005/671/TI groza šādi:

1) lēmuma 1. pantā svītrot c) punktu;

2) lēmuma 2. pantu groza šādi:

a) panta 2. punktu svītrot;

b) panta 3. punktu aizstāj ar šādu:

"3. Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka Eiropalam saskaņā ar valsts tiesību aktiem un Eiropas Parlamenta un Padomes Regulu (ES) 2016/794 * tiek nosūtīta vismaz 4. punktā minētā attiecīgās iestādes apkopotā informācija par tādu teroristu nodarījumu kriminālizmeklēšanu, kuri ietekmē vai var ietekmēt divas vai vairākas dalībvalstis.

* Eiropas Parlamenta un Padomes Regula (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI (OV L 135, 24.5.2016., 53. lpp.).";

c) panta 5. punktu svītrot.

3. pants
Stāšanās spēkā

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

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

....

Eiropas Parlamenta vārdā –
priekšsēdētāja

Padomes vārdā –
priekšsēdētājs / priekšsēdētāja