



EIROPAS KOMISIJA

Briselē, 25.1.2012.
COM(2012) 12 final

**KOMISIJAS ZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS
EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI,**

**pamatojoties Padomes 2008. gada 27. novembra Pamatlēmuma par tādu personas datu
aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās,
29. panta 2. punktu**

{SEC(2012) 75 final}

**KOMISIJAS ZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS
EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI,**

**pamatojoties Padomes 2008. gada 27. novembra Pamatlēmuma par tādu personas datu
aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās,
29. panta 2. punktu**

1. IEVADS

1.1. Vispārēja informācija

Ar Padomes 2008. gada 27. novembra Pamatlēmumu 2008/977/TI¹ (Pamatlēmums) par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās, ir izveidots vispārējs regulējums datu aizsardzībai policijas un tiesu iestāžu sadarbībā krimināllietās. Tas stājas spēkā 2009. gada 19. janvārī².

Pamatlēmums bija nepieciešams, jo tolaik Eiropas līmenī nepastāvēja vispārējs instruments, kas attiektos uz datu apstrādi, policijas un tiesu iestādēm sadarbojoties krimināllietās³. Eiropas Parlamenta un Padomes Direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti 3. pants paredz, ka direktīva "neattiecas uz personas datu apstrādi tādu pasākumu gaitā, uz kuru neattiecas Kopienas tiesību akti, kā Līguma par Eiropas Savienību VI sadaļā paredzētie pasākumi un, jebkurā gadījumā, uz apstrādes operācijām attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību un uz valsts pasākumiem krimināltiesību jomā."

Pamatlēmuma mērķis ir ES līmenī nodrošināt fizisko personu pamattiesību un pamatbrīvību augsta līmeņa aizsardzību, apstrādājot personas datus, policijas un tiesu iestādēm sadarbojoties krimināllietās. Vienlaikus būtu jānodrošina augsts sabiedrības drošības līmenis⁴. Tas neliedz dalībvalstīm paredzēt stingrākus drošības pasākumus, lai aizsargātu personas datus, kas tiek vākti un apstrādāti valsts līmenī⁵.

Pamatlēmuma darbības joma⁶ attiecas tikai uz personas datu apstrādi, kas veikta, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai veiktu kriminālvajāšanu par tiem, vai saistībā ar kriminālsodu izpildi, ja personas dati ir nosūtīti vai darīti pieejami:

- starp dalībvalstīm;

¹ OV L 350, 30.12.2008., 60. lpp.

² Pamatlēmuma 30. pants.

³ Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti piektais apsvērums, OV L 281, 23.11.1995., 31. lpp.

⁴ Pamatlēmuma 1. pants.

⁵ Pamatlēmuma 1. panta 5. punkts.

⁶ Pamatlēmuma 1. panta 2. punkts.

- dalībvalstis tos ir nosūtījušas vai darījušas pieejamus iestādēm vai informācijas sistēmām, kas izveidotas, pamatojoties uz Līguma par Eiropas Savienību IV sadaļu ("Policijas un tiesu iestāžu sadarbība krimināllietās"); vai

- iestādes vai informācijas sistēmas, kas izveidotas, pamatojoties uz Līgumu par Eiropas Savienību vai Eiropas Kopienas dibināšanas līgumu, tos ir nosūtījušas vai darījušas pieejamus dalībvalstu kompetentām iestādēm.

Personas datus, kas ir nosūtīti no vienas dalībvalsts uz otru, var arī pārsūtīt uz trešām valstīm vai starptautiskām struktūrām, ja ir izpildīti daži nosacījumi⁷.

Pamatlēmums ir pilnībā piemērojams Apvienotajai Karalistei un Īrijai, jo tas ir Šengenas *acquis* pilnveidošana. Apvienotā Karaliste un Īrija piedalās šajā pamatlēmumā saskaņā ar 5. pantu Protokolā par Šengenas *acquis*, kas iekļauts Eiropas Savienības sistēmā, kurš pievienots Līgumam par Eiropas Savienību un Eiropas Kopienas dibināšanas līgumam, un Padomes Lēmumu 2000/365/EK un Padomes Lēmumu 2002/192/EK.

Attiecībā uz Islandi, Norvēģiju, Šveici un Lihtenšteinu Pamatlēmums ir Šengenas *acquis* pilnveidošana saskaņā ar nolīgumu un protokoliem, ko Eiropas Savienības Padome vai Eiropas Savienība noslēgusi ar Islandi, Norvēģiju, Šveices Konfederāciju un Lihtenšteinu, un Padomes lēmumiem 1999/437/EK, 2008/149/TI un 2008/262/TI.

1.2. Pamatlēmuma 2008/977/TI saturs

Pamatlēmuma **darbības joma** neattiecas uz personas datu apstrādi datu izcelsmes dalībvalstī, ko veic kompetentās tiesu iestādes vai policijas iestādes (1. panta 2. punkts).

Nozares tiesību aktiem, kas attiecas uz policijas un tiesu iestāžu sadarbību krimināllietās, kuri satur noteikumus par personas datu aizsardzību un kuri ir pieņemti **pirms** Pamatlēmuma stāšanās spēkā, pamatā ir "lielāks juridiskais spēks" nekā Pamatlēmumam (28. pants). Pamatlēmums neskar instrumentus, kas tiek uzskatīti par "pilnīgu un saskaņotu noteikumu kopumu" attiecībā uz datu aizsardzību (39. apsvērums). Citi nozares pasākumi, kas ietver datu aizsardzības noteikumus, kuru darbības joma ir ierobežotāka, ir piemērojami Pamatlēmuma vietā, ja šie noteikumi ir stingrāki nekā Pamatlēmuma noteikumi. Pretējā gadījumā ir piemērojams Pamatlēmums (40. apsvērums).

Pamatlēmumā ir precizēti datu aizsardzības mērķi policijas un tiesu iestāžu darbības kontekstā. Tas paredz noteikumus par personas datu apstrādes likumību, lai nodrošinātu, ka jebkāda informācija, ar kuru var apmainīties, tiek apstrādāta likumīgi un saskaņā ar datu kvalitātes pamatprincipiem.

Tas nosaka arī datu subjektu tiesības, lai nodrošinātu personas datu aizsardzību, neapdraudot kriminālizmeklēšanas intereses. Šajā nolūkā datu subjekti ir jāinformē un tiem ir jāpiešķir piekļuve saviem personas datiem.

Valsts uzraudzības iestādēm, īstenojot tām uzticētos uzdevumus pilnīgi neatkarīgi, ir jāuzrauga to pasākumu piemērošana, kurus dalībvalstis ir pieņēmušas, lai transponētu Pamatlēmumu, un jāsniedz padomi saistībā ar to.

⁷ Pamatlēmuma 13. pants.

1.3. Komisijas pienākums ziņot par īstenošanu

Saskaņā ar Pamatlēmuma 29. panta 1. punktu dalībvalstīm līdz 2010. gada 27. novembrim ir jāveic pasākumi, lai nodrošinātu atbilstību šim lēmumam.

Saskaņā ar 29. panta 2. punktu dalībvalstīm ir jānosūta Padomes Ģenerālsekretariātam un Komisijai to noteikumu teksts, ar kuriem tām uzliktās saistības, ir transponētas valsts tiesību aktos, kā arī informācija par Pamatlēmuma 25. pantā minētajām uzraudzības iestādēm.

Komisijai ir jā sagatavo ziņojums, izmantojot dalībvalstu sniegto informāciju. Padomei līdz 2011. gada 27. novembrim ir jānovērtē, kā dalībvalstis panākušas atbilstību šim pamatlēmumam.

1.4. Informācijas avoti, uz kuriem balstās šis ziņojums

Līdz **2011. gada 9. novembrim** 26 no 27 dalībvalstīm, kā arī Lihtenšteina, Norvēģija, Islande un Šveice ir nosūtījušas Komisijai informāciju par Pamatlēmuma īstenošanu.

No šīm 26 dalībvalstīm 14 dalībvalstis norādīja, ka Pamatlēmums ir īstenots to spēkā esošajos tiesību aktos (Beļģija, Čehijas Republika, Dānija, Vācija, Igaunija, Īrija, Ungārija, Latvija, Lietuva, Luksemburga, Austrija, Slovākija, Zviedrija un Apvienotā Karaliste). Vācija, Īrija, Igaunija un Zviedrija paziņoja, ka tās vēl joprojām pārbauda, vai ir nepieciešami turpmāki īstenošanas pasākumi.

Ir uzskatāms, ka **deviņas** dalībvalstis Pamatlēmumu ir īstenojušas daļēji, jo tās ziņo, ka tiesību akti tā īstenošanai vēl ir jāpieņem.

Četras dalībvalstis vai nu nav reaģējušas uz Komisijas informācijas pieprasījumu (Rumānija), vai ir norādījušas, ka tās Pamatlēmumu nav īstenojušas (Grieķija, Itālija⁸, Kipra).

Informācijas saturs, jo īpaši detalizētības pakāpe, kuru dalībvalstis sniegušas, atbildot uz Komisijas anketu, ir atšķirīgs. Pirmā tabula sniedz pārskatu par atbildēm: tā atspoguļo dalībvalstu novērtējumu par Pamatlēmuma īstenošanas statusu.

2. PAMATLĒMUMA TRANSPONĒŠANA

2.1. Pamatlēmums (Līguma par Eiropas Savienību bijušais 34. panta 2. punkta b) apakšpunkts)

Šis pamatlēmums balstās uz Līgumu par Eiropas Savienību (LES) un jo īpaši tā 30. pantu, 31. panta e) punktu un 34. panta 2. punkta b) apakšpunktu.

⁸ **Itālija** informēja Komisiju, ka īpaši īstenojošie instrumenti vēl nav formāli pieņemti. Tā atsauca uz Personas datu aizsardzības kodeksu, Kriminālprocesa kodeksu un citiem aktiem, kas satur tiesību normas, kas piemērojamas apstrādei šajās jomās. Citas dalībvalstis ir izvēlējušas atšķirīgu pieeju un norāda, ka spēkā esošie datu aizsardzības noteikumi ir piemērojami arī personas datu apstrādei, ko policija un tiesu iestādes veic valsts līmenī, kā arī datu pārrobežu apstrādei, ko policija un tiesu iestādes veic krimināllietās. Turklāt tās ir informējušas Komisiju par papildu īstenošanas pasākumiem, kas pašlaik tiek sagatavoti.

Pamatlēmumi kā tiesību akti ir līdzīgi direktīvām, jo tie saista dalībvalstis attiecībā uz sasniedzamo rezultātu, taču atstāj dalībvalstu iestādēm iespēju izvēlēties formu un metodes. Tomēr pamatlēmumiem nav tiešas ietekmes⁹.

Balstoties uz 10. pantu Protokolā par pārejas noteikumiem attiecībā uz aktiem, kas pieņemti, pamatojoties uz Līguma par Eiropas Savienību V un VI sadaļu, pirms stājas spēkā Lisabonas līgums (Nr. 36), kas pievienots Līgumiem, Komisijas pilnvaras, kas noteiktas LESD 258. pantā, piecu gadu pārejas periodā no Lisabonas līguma stāšanās spēkā (t.i., līdz 2014. gada 1. decembrim) nav piemērojamas "bijušā trešā pīlāra" aktiem (un Eiropas Savienības Tiesas pilnvaras paliek ierobežotas).

Turpmāk ir izklāstīta sīkāka informācija par Pamatlēmuma četru būtisku noteikumu īstenošanu, balstoties uz dalībvalstu atbildēm, kas sniegtas uz Komisijas 2011. gada 9. decembra lūgumu.

2.1.1. Valsts īstenošanas pasākumu darbības joma

Pamatlēmumu piemēro tikai personas datu apstrādei, kas nosūti vai darīti pieejami starp dalībvalstīm (1. panta 2. punkts). Personas datu apstrāde, ko policija un tiesu iestādes veic krimināllietās valsts līmenī, neietilpst Pamatlēmuma darbības jomā.

Pielikuma 2. tabulā sniegts pārskats par dalībvalstu īstenošanas pasākumiem. Lielākā daļa dalībvalstu atsaucās uz vispārējiem datu aizsardzības tiesību aktiem kā vienu no Pamatlēmuma īstenošanas pasākumiem un pievienoja atsauci uz piemērojamiem nozares tiesību aktiem, kas attiecas uz policiju, tiesu iestādēm, muitas un nodokļu iestādēm. Dažas dalībvalstis nolēma nepieņemt leģislatīvus aktus, bet īstenot lēmumu, izdodot administratīvus apkārtrakstus (piemēram, Vācija un Apvienotā Karaliste).

Lielākā daļa dalībvalstu norādīja, ka **vispārējie datu aizsardzības tiesību akti ir piemērojami datu apstrādei, ko veic policijas iestādes gan valsts līmenī, gan pārrobežu kontekstā¹⁰, tomēr bieži tie ir piemērojami līdztekus kriminālprocesa likumiem un policijas (datu) likumiem¹¹**. Trīspadsmit dalībvalstis (Beļģija, Čehijas Republika, Vācija, Igaunija, Itālija, Luksemburga, Ungārija, Malta, Nīderlande, Slovēnija, Slovākija, Somija un Zviedrija) minēja kriminālprocesa likumus vai līdzīgus tiesību aktus. Septiņas dalībvalstis (Čehijas Republika, Vācija, Ungārija, Nīderlande, Slovēnija, Somija un Zviedrija) paziņoja par īpaša policija (datu) likuma pastāvēšanu¹². Trīs dalībvalstis (t.i., Bulgārija, Polija, Lietuva) paziņoja, ka tās ir arī pieņēmušas īpašus tiesību aktus, lai īstenotu dažus Pamatlēmuma noteikumus, kas nebija iekļauti vispārējos tiesību aktos, kuri ir piemērojami tikai personas datu pārrobežu apstrādei¹³.

Trīs dalībvalstis uzskatīja, ka Pamatlēmuma ierobežotā darbības joma ir problemātiska. Itālija un Nīderlande ziņoja par grūtībām praksē nošķirt datu pārrobežu apstrādi, pamatojoties uz Pamatlēmumu 2008/977/TI, un apstrādi valsts līmenī un saistītās grūtības tiesībaizsardzības

⁹ Skat. 2005. gada 16. maija spriedumu lietā C-105/03 *Pupino*, 34., 43. – 45., 47., 61. punkts, kurā Tiesa lēma, ka valstu tiesām, interpretējot valsts tiesību aktus, ir pienākums censties panākt atbilstīgu interpretāciju, ieskaitot pamatlēmumus.

¹⁰ Šāda situācija bija jau pirms Pamatlēmuma pieņemšanas (skat. Komisijas darba dienestu dokumentu, Ietekmes novērtējumu, SEC(2005)1241, 4.10.2005., 5.1.2. punkts).

¹¹ Skat. 2. tabulu.

¹² Skat. 2. tabulu.

¹³ Skat. Nīderlandes komentārus.

iestādēm dalībvalstīs dažādo apstrādes noteikumu dēļ, kas piemērojami vieniem un tiem pašiem personas datiem. Polija norādīja uz Pamatlēmuma trūkumiem kopumā un jo īpaši uzsvēra savu atbalstu Komisijas mērķim izveidot visaptverošu regulējumu un attiecināt vispārīgos datu aizsardzības noteikumus uz policijas un tiesu iestāžu sadarbību krimināllietās¹⁴.

2.1.2. Informācija par datu subjektiem (16. pants, 26. – 27. apsvērums)

Saskaņā ar Pamatlēmumu dalībvalstīm ir jānodrošina, ka to kompetentās iestādes informē datu subjektus par to, ka personas dati tiek vākti, apstrādāti vai nosūtīti citai dalībvalstij, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus un veiktu kriminālvajāšanu par tiem, vai izpildītu kriminālsodus. Forma, saturs, metode un izņēmumi (t.i., informācijas nesniegšana vai ierobežota informācijas sniegšana), ko izmanto, lai to darītu, būtu jānosaka valsts tiesību aktos. Tas var notikt vispārīgā formā, pieņemot likumu vai publicējot apstrādes darbību sarakstu. Ja datus nosūta citai dalībvalstij, katra dalībvalsts var lūgt otru dalībvalsti neinformēt datu subjektu.

Trešā tabula atklāj, ka **gandrīz visas** dalībvalstis ir norādījušas, ka tās sniedz datu subjektiem **kādu** informāciju par to personas datu apstrādi. **Francija** norādīja, ka tā to nedara. Arī **Dānija** nepiešķir šādas tiesības, bet ziņoja, ka personas datu apstrādātājam ir jāuztur reģistrs un jāinformē sabiedrība.

Lielākajā daļā dalībvalstu tiesībām uz informāciju tiek **piemēroti ierobežojumi**. Valsts tiesību akti vai nu ierobežo šīs tiesības, lai novērstu, izmeklētu, atklātu un veiktu kriminālvajāšanu par noziedzīgiem nodarījumiem, vai nodrošina, ka šīs tiesības neattiecas uz datu apstrādi, ko veic īpaši personas datu apstrādātāji (policija un/vai tiesu iestādes). Dažos gadījumos ierobežojumi/izņēmumi ir noteikti, neprecizējot uz kādām darbībām tie attiecas. Vairākas dalībvalstis ziņo par šādu ierobežojumu pastāvēšanu attiecībā uz policiju, militāro policiju, tiesām, muitas un nodokļu iestādēm.

Nīderlande paziņoja, ka vispārējs pienākums informēt datu subjektus nebija pilnībā atbilstošs policijas un tiesu iestāžu darba raksturam, bet pastāv daži pasākumi, lai nodrošinātu datu subjektu pietiekamu informēšanu par policijas un tiesu iestāžu veiktu datu apstrādi (t.i., no tiesību aktiem var iegūt informāciju par datu apstrādes gadījumiem un nosacījumiem; prokurors informē datu subjektu par īpašu izmeklēšanas pilnvaru īstenošanu, ja izmeklēšanas intereses to atļauj). Nīderlande paziņoja arī, ka šī tiesību norma nav jāīsteno, jo 16. panta 1. punktā ir ietverta tikai atsauce uz dalībvalstu valsts tiesību aktiem.

Pamatlēmumā ir noteiktas datu subjekta tiesības uz informāciju, bet metodes vai iespējamie izņēmumi sīkāk nav noteikti. Pat ja saskaņā ar dalībvalstu apgalvoto tiesības uz informāciju parasti tiek nodrošinātas, to īstenošana būtiski atšķiras.

2.1.3. Datu subjektu piekļuves tiesības (17. pants)

Pamatlēmums nosaka, ka datu subjektam ir tiesības bez ierobežojumiem, pārmērīgas kavēšanās vai izmaksām saņemt:

¹⁴ Skat. arī Polijas komentārus (Iekšlietu ministrija) sabiedriskajā apspriešanā, ko Komisija uzsāka 2010. gadā (minēti atbildē uz anketu): http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/pl_min_pl.pdf.

- a) vismaz apstiprinājumu, ko sniedz personas datu apstrādātājs vai valsts uzraudzības iestāde, vai uz viņu attiecināmie dati ir pārsūtīti vai atklāti, un informāciju par saņēmējiem vai saņēmēju kategorijām, kuriem dati atklāti, un paziņojumu par apstrādē esošiem datiem; vai
- b) vismaz apstiprinājumu, ko sniedz valsts uzraudzības iestāde, ka ir izdarītas visas vajadzīgās pārbaudes.

Dalībvalstis var tiesību aktos noteikt šo piekļuves tiesību ierobežojumus, lai izvairītos no oficiālas vai tiesiskas izmeklēšanas vai procedūru kavēšanas; lai izvairītos no noziedzīgu nodarījumu novēršanas, izmeklēšanas un atklāšanas un kriminālvajāšanas kavēšanas; lai aizsargātu sabiedrības drošību; lai aizsargātu valsts drošību; lai aizsargātu datu subjektu vai citu personu tiesības un brīvības (17. panta 2. punkts). Personas datu apstrādātāja atteikums sniegt šo informāciju ir jāpaziņo rakstiski (17. panta 3. punkts).

Dalībvalstu sniegtā informācija par piekļuves tiesībām, kas apkopota 4. tabulā, atspoguļo situāciju attiecībā uz informācijas sniegšanu datu subjektam. Secināms, ka **visas dalībvalstis¹⁵ datu subjektam piešķir noteikta veida piekļuves tiesības**. Šīs tiesības parasti ir noteiktas valsts vispārīgajos datu aizsardzības tiesību aktos. Daudzas dalībvalstis piekļuves tiesības sīkāk nosaka nozares tiesību aktos (piemēram, policijas likumos).

Tāpat visas dalībvalstis paredz **izņēmumus no piekļuves tiesībām**. Visbiežāk minētie iemesli piekļuves tiesību nepiešķiršanai ir:

- noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana un kriminālvajāšana par tiem;
- valsts drošība, aizsardzība un sabiedrības drošība;
- ES un dalībvalsts ekonomikas un finanšu interešu aizsardzība (tai skaitā monetārie, budžeta un nodokļu jautājumi)¹⁶;
- datu subjektu un citu personu tiesību un brīvību aizsardzība.

Attiecībā uz **veidu, kādā tiek piešķirta piekļuve personas datiem** – dažas dalībvalstis ir īpaši pievērsušās šim jautājumam, savukārt citas to nav darījušas. Dažas dalībvalstis norādīja, ka tās piešķir datu subjektam tiesības nosūtīt pieprasījumu par piekļuvi saviem datiem tieši kompetentajai iestādei (t.i., Austrija, Vācija, Bulgārija, Somija, Īrija, Latvija, Malta, Nīderlande, Polija, Slovākija, Zviedrija, Apvienotā Karaliste), savukārt citas atļauj tikai "netiešu" piekļuvi (Beļģija, Francija). Otrajā gadījumā valsts uzraudzības iestādei ir tiesības datu subjekta vietā piekļūt visiem personas datiem, kas attiecas uz datu subjektu. Somijā un Lietuvā datu subjektam tiek dota iespēja izvēlēties. Portugālē tieša piekļuve ir pamatnoteikums, taču netieša piekļuve tiek nodrošināta gadījumos, kad personas datu apstrādei ir ietekme uz valsts drošību vai noziedzīga nodarījuma novēršanu vai izmeklēšanu. Līdzīga situācija ir Luksemburgā, kur pamatā piekļuve tiek piešķirta tieši, bet, ja ir piemērojams izņēmums, piekļuves pieprasījums ir jāadresē valsts datu aizsardzības uzraudzības iestādei.

¹⁵ Šo secinājumu var izdarīt, lai gan dažas dalībvalstis nesniedza sīkāku informāciju (skat. 3. tabulu).

¹⁶ Šis nav izņēmums, kas īpaši minēts Pamatlēmuma 2008/977/TI 17. pantā. Tomēr tas atspoguļo izņēmumu, kas minēts Direktīvas 95/46/EK 13. panta 1. punktā.

Pamatlēmumā ir paredzēti vispārēji noteikumi, kas nodrošina datu subjektiem tiesības piekļūt to datiem. Tas sīkāk neprecizē, kāda informācija ir jāsniedz datu subjektam. Tas ļauj arī dalībvalstīm izlemt, vai datu subjekti var īstenot savas piekļuves tiesības tieši, vai tiem ir jāizmanto netiešais ceļš.

2.1.4. *Valsts uzraudzības iestādes (25. pants)*

Pamatlēmumā 2008/977/TI ir atzīts, ka uzraudzības iestāžu izveide dalībvalstīs, kuras darbojas pilnīgi neatkarīgi, ir "būtiska aizsardzības sastāvdaļa attiecībā uz personas datiem, ko apstrādā, sadarbojoties dalībvalstu policijas un tiesu iestādēm" (33. apsvērums). Tas nosaka arī, ka uzraudzības iestādēm, kas dalībvalstīs jau izveidotas saskaņā ar direktīvu "būtu jāspēj veikt arī" šādas funkcijas (34. apsvērums). Pamatlēmuma 2008/977/TI 25. pants atspoguļo būtisku Direktīvas 95/46/EK 28. panta daļu par uzraudzības iestādēm (1. – 4. punktu, 7. punktu) attiecībā uz iestādes pilnvarām, tās pienākumu rīkoties pilnīgi neatkarīgi un pienākumu aizsargāt dienesta noslēpumu. Katrai iestādei ir jāpiešķir virkne pilnvaru, kas sastāv no izmeklēšanas pilnvarām (tai skaitā piekļuves datiem un pilnvarām vākt nepieciešamo informāciju), efektīvām iejaukšanās pilnvarām (piemēram, sniegt un publicēt atzinumus pirms datu apstrādes darbību veikšanas; liegt piekļuvi datiem, dzēst vai iznīcināt datus, noteikt pagaidu vai galīgu aizliegumu datu apstrādei, brīdināt vai izteikt aizrādījumu personas datu apstrādātājam vai nodot jautājumu izskatīšanai valstu parlamentiem vai citām politiskām iestādēm) un pilnvaras uzsākt procesuālas darbības.

Piektā tabula atklāj, ka lielākajā daļā gadījumu valsts uzraudzības iestādes, kas atbild par vispārīgo datu aizsardzības noteikumu īstenošanas uzraudzību un piemērošanu, parasti ir atbildīgas arī par Pamatlēmuma 2008/977/TI īstenošanu un piemērošanu.

Zviedrija norādīja, ka tās Datu inspekcijas valde (*Data Inspection Board*) vēl ir jānosaka par atbildīgo uzraudzības iestādi saskaņā ar Pamatlēmuma 25. pantu.

Dažas dalībvalstis īpaši pievērsās jautājumam par datu apstrādes uzraudzību, ko veic tiesu iestādes¹⁷. Dānija norādīja, ka Tiesu administrācija ir atbildīga par tiesu iestāžu veiktās datu apstrādes uzraudzību, un Austrija norādīja, ka datu aizsardzības uzraudzības iestādei nav kompetences lemt par sūdzībām, kas attiecas uz tiesu iestāžu izdarītiem datu aizsardzības noteikumu pārkāpumiem. Luksemburgā datu apstrādes uzraudzība kopumā ir Datu aizsardzības komisijas kompetencē. Apstrādes darbības, kas tiek veiktas, pamatojoties uz valsts tiesību normu, ar kuru tiek īstenota starptautiska konvencija, uzrauga iestāde, kuras sastāvā ir *Procureur Général d'Etat* vai viņa pārstāvis un divi Datu aizsardzības komisijas locekļi, kurus pēc šīs komisijas ierosinājuma ieceļ ministrs.

2.1.5. *Citas dalībvalstu izvirzītās problēmas*

No 26 dalībvalstīm 20 dalībvalstis neziņoja par īpašām problēmām saistībā ar Pamatlēmumu; astoņas no šīm valstīm vispār neatbildēja uz šo jautājumu (Beļģija, Dānija, Igaunija, Grieķija, Ungārija, Luksemburga, Kipra un Austrija). Kā norādīts 6. tabulā, sešas dalībvalstis iesniedza komentārus par problēmjautājumiem, ar kuriem tās saskārušās:

¹⁷ Skat. Pamatlēmuma 35. apsvēruma pēdējo teikumu, kas nosaka, ka uzraudzības iestāžu pilnvarām "nevajadzētu būt pretrunā īpašajiem noteikumiem, kas paredzēti kriminālprocesā, un tām nebūtu jāietekmē tiesu neatkarība".

- Polija uzskatīja, ka Pamatlēmumam ir vairāki trūkumi, kurus būtu jālabo, un izteica atbalstu reformai, lai izveidotu visaptverošu un saskaņotu datu aizsardzības sistēmu ES līmenī;

- Itālija un Nīderlande ziņoja par grūtībām praksē nošķirt datu pārrobežu apstrādi, pamatojoties uz Pamatlēmumu 2008/977/TI, un apstrādi valsts līmenī un saistītās grūtības tiesībaizsardzības iestādēm dalībvalstīs dažādo apstrādes noteikumu dēļ, kas piemērojami vieniem un tiem pašiem personas datiem;

- Itālija, Čehijas Republika un Nīderlande kritizēja Pamatlēmuma noteikumus par starptautisku pārsūtīšanu. Jo īpaši Itālija apgalvoja, ka ir nepieciešams nodrošināt atbilstošu un vienotāku datu aizsardzības līmeni datu pārsūtīšanai uz trešām valstīm. Nīderlande uzskatīja, ka problēma ir kritēriju trūkums Pamatlēmumā, lai noteiktu, vai trešā valstī pastāv pienācīgs aizsardzības līmenis, kā rezultātā īstenošana dalībvalstīs ir atšķirīga. Visbeidzot, Čehijas Republika uzskatīja, ka Pamatlēmuma noteikumi par starptautisku pārsūtīšanu nav "reālistiski";

- Francija atsaucās uz īpašu problēmu valsts līmenī attiecībā uz tādu personas datu uzglabāšanas periodiem, kas nosūtīti uz trešo valsti vai no tās, attiecībā uz ko pastāv atšķirīgas prasības;

- Slovākija apgalvoja, ka ir nepieciešams vairāk nošķirt datu apstrādi, ko veic policija, un datu apstrādi, ko veic tiesu iestādes (tiesvedību);

- gan Čehijas Republika, gan Nīderlande norādīja, ka tiesībaizsardzības iestādes mulsina nepieciešamība ievērot vairākus datu aizsardzības noteikumus, starptautiskā (piemēram, Eiropas Padomes), ES un valsts līmenī.

3. TURPMĀKAIS DARBS

Šajā ziņojumā ir izvērtēta Pamatlēmuma par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās, īstenošana un darbība.

Praktiskās grūtības, ar kurām saskārušās dalībvalstis, nošķirot noteikumus, kas attiecas uz valsts līmeņa apstrādi un pārrobežu apstrādi, varētu atrisināt ar vienotu noteikumu kopumu, kas attiektos gan uz valsts līmeni, gan pārrobežu kontekstu. Būtu nepieciešams turpmāk precizēt datu subjektu tiesību uz informāciju darbības jomu un iespējamus izņēmumus ES līmenī. Harmonizēti minimuma noteikumi par datu subjekta piekļuves tiesībām varētu nostiprināt datu subjektu tiesības, vienlaikus paredzot izņēmumus, lai ļautu policijas un tiesu iestādēm pienācīgi veikt savus uzdevumus.

Balstoties uz Līguma par Eiropas Savienības darbību 16. pantu, kurā noteiktas tiesības uz personas datu aizsardzību, tagad pastāv iespēja izveidot visaptverošu datu aizsardzības regulējumu, nodrošinot gan personas datu augsta līmeņa aizsardzību policijas un tiesu iestāžu sadarbībā krimināllietās, gan personas datu raitāku apmaiņu starp dalībvalstu policijas un tiesu iestādēm, pilnībā ievērojot subsidiaritātes principu.