EIROPAS KOPIENU KOMISIJA

Briselē, 4.10.2005
COM(2005) 475 galīgā redakcija

2005/0202 (CNS)

Priekšlikums

PADOMES PAMATLĒMUMS

par personas datu, ko apstrādā, sadarbojoties policijas un tiesu iestādēm krimināllietās, aizsardzību

{SEC(2005) 1241}

(iesniegusi Komisija)

PASKAIDROJUMA RAKSTS

1) PRIEKŠLIKUMA KONTEKSTS

- **Priekšlikuma pamatojums un mērķi**

Eiropadome 2004. gada 4. novembrī pieņēma Hāgas programmu brīvības, drošības un tiesiskuma stiprināšanai Eiropas Savienībā[1]. Šīs programmas ietvaros Komisija tiek aicināta vēlākais līdz 2005. gada beigām iesniegt priekšlikumus par pieejamības principa īstenošanu pārrobežu tiesībaizsardzības informācijas apmaiņas uzlabošanai starp dalībvalstīm. Hāgas programmā uzsvērts, ka šajos priekšlikumos ir stingri jāievēro galvenie nosacījumi datu aizsardzības jomā.

Padome un Komisija 2005. gada jūnijā pieņēma rīcības plānu, par to, kā īstenot Hāgas programmu[2]. Tas ir balstīts uz Komisijas paziņojumu Padomei un Eiropas Parlamentam „Hāgas programma: Desmit prioritātes turpmākajiem pieciem gadiem. Partnerība Eiropas atjaunošanai brīvības, drošības un tiesiskuma telpā"[3]. Saskaņā ar rīcības plānu Komisija 2005. gadā iesniedz *priekšlikumus (1) par tiesību aizsardzībai būtiskas informācijas pieejamības principa noteikšanu un (2) par atbilstošām garantijām personas datu nodošanai policijas un tiesu iestāžu sadarbības nolūkā krimināllietās*. Padome (Tieslietu un iekšlietu) 2005. gada 13. jūlija deklarācijā par ES atbildes pasākumiem attiecībā uz terorisma aktiem Londonā[4] aicināja Komisiju iesniegt šos priekšlikumus līdz 2005. gada oktobrim.

Šis pamatlēmums nodrošina personas datu, kuri apstrādāti policijas un tiesu iestāžu sadarbības ietvaros starp ES dalībvalstīm (Līgums par Eiropas Savienību, VI sadaļa), aizsardzību. Tā mērķis ir uzlabot šo sadarbību, jo īpaši terorisma novēršanā un apkarošanā, turklāt stingri ievērojot galvenos nosacījumus datu aizsardzības jomā. Tas nodrošina pamatbrīvību ievērošanu visā Eiropas Savienībā, īpašu uzmanību pievēršot tiesībām uz privātās dzīves neaizskaramību un personas datu aizsardzību, jo īpaši ņemot vērā informācijas pieejamības principa īstenošanu. Tas arī nodrošina, lai attiecīgās informācijas apmaiņu starp dalībvalstīm nekavētu dalībvalstu atšķirīgie datu aizsardzības līmeņi.

- **Vispārējais konteksts**

Papildus Itālijas iniciatīvai[5] jautājums par personas datu aizsardzību trešajā pīlārā jau tika apspriests 1998. gadā. Tajā laikā Tieslietu un iekšlietu padome pieņēma tā saucamo Vīnes rīcības plānu[6]. Attiecībā uz horizontāla rakstura problēmām policijas un tiesu iestāžu sadarbības kontekstā tas paredzēja, ka iespējas noteikt saskaņotus datu aizsardzības noteikumus ir jāizskata divu gadu laikā pēc līguma stāšanās spēkā. Tomēr 2001. gadā neizdevās pieņemt rezolūcijas projektu par personas datu aizsardzības noteikumiem tiesību aktos, kas ir Eiropas Savienības trešajā pīlārā[7]. Grieķijas prezidentūra trešajā pīlārā[8] 2003. gada jūnijā ierosināja personas datu aizsardzības vispārējo principu kopumu, kura pamatā ir Direktīva 95/46/EK par datu aizsardzību un Eiropas Savienības Pamattiesību harta. Eiropas Savienības dalībvalstu datu aizsardzības iestādes un Eiropas datu aizsardzības

---

1 OV C 53, 3.3.2005., 1. lpp.
2 OV C 198, 12.8.2005., 1. lpp.
3 KOM(2005) 184, Briselē 10.5.2005.
4 Padomes darba dokuments 11158/1/05 REV 1 JAI 255
5 Padomes darba dokuments 8321/98JAI 15
6 OV C 19, 23.1.1999., 1. lpp.
7 Padomes darba dokuments 6316/2/01 REV 2 JAI 13
8 Tieslietu un iekšlietu padomes 2514. sēde, Luksemburgā, 2003. gada 5.-6. jūnijā, Padomes dokuments 9845/03 (*Prese* 150), 32. lpp.

uzraudzītājs (še turpmāk „*EDPS*”) 2005. gadā izteica stingru atbalstu jauna tiesību akta par personas datu aizsardzību izdošanai trešajā pīlārā[9]. Eiropas Parlaments ieteica saskaņot pašreizējos noteikumus personas datu aizsardzības jomā trešā pīlāra tiesību aktos, apvienojot tos vienā dokumentā, kurš garantē tādu pašu datu aizsardzības līmeni kā pirmajā pīlārā[10]. Acīm redzami, Eiropas Padome atzina, ka datu aizsardzības nosacījumi, kas šobrīd pastāv Eiropas līmenī, nebūtu pietiekami, ņemot vērā pieejamības principa īstenošanu, kas var ietvert tādas prasības kā savstarpēja piekļuve valstu datubāzēm vai to savstarpēja savietojamība, vai tieša piekļuve (tiešsaistē).

Bažas par pietiekamu datu aizsardzības līmeni tika atspoguļotas arī nolīgumā par sadarbību, kuru septiņas dalībvalstis parakstīja 2005. gada 27. maijā Prīmē (*Prüm*) (Vācija, Austrija, Beļģija, Nīderlande, Luksemburga, Francija un Spānija) un kuru tās iesaka kā informācijas apmaiņas modeli starp Savienības dalībvalstīm kopumā. Ievērojot īpašus nosacījumus, nolīgums paredz vienas līgumslēdzējas puses tiesībaizsardzības iestādēm tiešu automatizētu piekļuvi personas datiem, kas ir otras līgumslēdzējas puses pārziņā. Tomēr šī sadarbības forma netiek piemērota, līdz nolīgumā paredzētie datu aizsardzības nosacījumi nav transponēti abu pušu valsts tiesību aktos.

- **Pašreizējie noteikumi jomā, uz kuru attiecas šis priekšlikums**

Eiropas Savienības Pamattiesību hartā[11] skaidri atzītas tiesības uz personas datu neaizskaramību (7. pants) un personas datu aizsardzību (8. pants). Minētie dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu leģitīmu pamatojumu, kas paredzēts likumā. Ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos. Šo noteikumu ievērošanu kontrolē neatkarīga iestāde.

Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti[12] satur pamatnoteikumus, kas attiecas uz personas datu apstrādes likumību, kā arī uz šo datu subjekta tiesībām. Tajā ir ietverti nosacījumi attiecībā uz tiesiskās aizsardzības līdzekļiem, atbildību un sankcijām, personas datu pārsūtīšanu uz trešām valstīm, profesionālās ētikas kodeksiem, īpašām uzraudzības iestādēm un darba grupu [personu aizsardzībai] un, visbeidzot, ieviešanas pasākumiem Kopienā. Tomēr šo direktīvu nepiemēro pasākumiem, uz kuriem neattiecas Kopienas tiesību akti, piemēram, pasākumiem, kas paredzēti VI sadaļā Līgumā par Eiropas Savienību. Tādēļ dalībvalstīm ir atļauts pašām lemt par atbilstošiem standartiem datu apstrādei un aizsardzībai. Personas datu aizsardzība VI sadaļas Līgumā par Eiropas Savienību kontekstā ir paredzēta dažādos īpašos dokumentos. Jo īpaši dokumentos, ar kuriem izveido kopējas informācijas sistēmas Eiropas līmenī, piemēram, Konvencijā, ar kuru īsteno 1990. gada Šengenas Līgumu, kurā ietverti specifiski datu aizsardzības nosacījumi, kas piemērojami Šengenas informācijas sistēmai[13]; Eiropola 1995. gada Konvencijā[14] un, *inter alia*, noteikumos, kas reglamentē to, kā Eiropols nosūta personas datus trešām valstīm un

---

9 Deklarācija un priekšlikuma dokuments par tiesību aizsardzību un informācijas apmaiņu ES, kurš tika pieņemts Eiropas datu aizsardzības iestāžu pavasara konferencē, kura notika Krakovā 2005. gada 25.-26. aprīlī

10 Eiropas Parlamenta ieteikums Nr. 1 h Eiropadomei un Padomei par informācijas apmaiņu un sadarbību attiecībā uz teroristu uzbrukumiem (2005/2046(INI), pieņemts 2005. gada 7. jūnijā

11 OV C 364, 18.12.2000., 1., 10. lpp.

12 OV L 281, 23.11.1995., 31. lpp.

13 OV L 239, 22.9.2000., 19. lpp.

14 OV C 316, 27.11.1995., 2. lpp.

trešām organizācijām[15]; 2002. gada lēmumā par Eurojust izveidošanu[16] un Eurojust personas datu apstrādes un aizsardzības reglamentā[17]; 1995. gada Konvencijā par informācijas tehnoloģiju izmantošanu muitas vajadzībām, kurā ietverti personas datu aizsardzības nosacījumi, kas piemērojami Muitas informācijas sistēmai[18]; 2000. gada Konvencijā par Eiropas Savienības dalībvalstu savstarpējo palīdzību krimināllietās, jo īpaši 23. pantā[19]. Attiecībā uz Šengenas informācijas sistēmu īpaša uzmanība ir jāpievērš otrās paaudzes Šengenas informācijas sistēmas (SIS II) izveidošanai, darbībai un izmantošanai, attiecībā uz kuru Komisija jau ir iesniegusi priekšlikumus Padomes lēmumam[20] un divām regulām[21].

Turklāt ir jāpievērš uzmanība 8. pantam Konvencijā par cilvēka tiesību un pamatbrīvību aizsardzību un Eiropas Padomes 1981. gada Konvencijai Nr. 108 par personu aizsardzību attiecībā uz personisko datu automātisko apstrādi, tās 2001. gada papildu Protokolam, kas attiecas uz uzraudzības iestādēm un pārrobežu datu plūsmām, un 1987. gada Ieteikumam Nr. R (87) 15, kurā reglamentēta personas datu izmantošana policijas vajadzībām. Visas dalībvalstis ir šīs Konvencijas līgumslēdzējas puses, bet ne visas ir papildu protokola līgumslēdzējas puses.

- **Atbilstība Eiropas Savienības mērķiem un politikai citās jomās**

Ir jāatzīst datu apstrādes un datu aizsardzības specifika VI sadaļas Līgumā par Eiropas Savienību darbības jomā. No vienas puses, tā nedrīkst kavēt atbilstību Eiropas Savienības vispārējai politikai privātās dzīves un datu aizsardzības jomā, pamatojoties uz Eiropas Savienības Pamattiesību hartu un Direktīvu 95/46/EK. Datu aizsardzības pamatprincipi attiecas uz datu apstrādi pirmajā pīlāra un trešajā pīlārā. Turklāt ir jānodrošina saskanība ar citiem tiesību aktiem, kuri nosaka konkrētus pienākumus attiecībā uz informāciju, kas var izrādīties būtiska noziedzības profilaksei un apkarošanai. Ir jāpievērš uzmanība norisēm, kas attiecas uz datu saglabāšanu, kuri apstrādāti un uzglabāti saistībā ar publiski pieejamu elektronisko sakaru pakalpojumu sniegšanu, vai uz informāciju par publiskiem sakaru tīkliem noziedzības un kriminālnoziegumu, tostarp terorisma, novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem. Ir jāizdara īpaša atsauce uz ciešo saistību starp ierosināto pamatlēmumu un Komisijas priekšlikumu Eiropas Parlamenta un Padomes direktīvai par datu, kuri apstrādāti saistībā ar publisko elektronisko sakaru pakalpojumu sniegšanu, saglabāšanu, ar ko labo Direktīvu 2002/58/EK[22].

2) APSPRIEŠANĀS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMS

- **Apspriešanās ar ieinteresētajām personām**

Apspriešanās metodes, galvenās mērķnozares un vispārējs respondentu raksturojums

Komisija 2004. gada 22. novembrī un 2005. gada 21. jūnijā uzaicināja uz tikšanos un apspriedās ar dalībvalstu, Islandes, Norvēģijas un Šveices valdību ekspertiem, bet 2005. gada 11. janvārī – ar šo valstu datu aizsardzības iestāžu ekspertiem. Tajā bija pārstāvēts Eiropas datu aizsardzības uzraudzītājs (*EDPS*), Eiropols, Eurojust un uzraudzības kopējās iestādes. Apspriešanās galvenais mērķis bija apzināt vajadzību pēc tiesību akta par personas datu

---

15 OV C 88, 30.3.1999., 1. lpp.
16 OV L 63, 6.3.2002., 1. lpp.
17 OV C 68, 19.3.2005., 1. lpp.
18 OV C 316, 27.11.1995., 34. lpp.
19 OV C 197, 12.7.2000., 1., 15. lpp.
20 KOM(2005) 230.
21 KOM(2005) 236, KOM(2005) 237.
22 KOM(2005) 438, 21.9.2005.

apstrādi un aizsardzību trešajā pīlārā un, ja tāda būtu, noskaidrot, kādam ir jābūt minētā tiesību akta saturam. Komisija, izmantojot aptauju un diskusiju dokumentu, jautāja apspriešanās dalībniekiem, *inter alia*, par viņu nostāju attiecībā uz vispārējo pieeju jauna tiesību akta sagatavošanai un tā saistību ar spēkā esošajiem tiesību aktiem, juridisko bāzi, iespējamo darbības jomu, principiem, kas attiecas uz datu kvalitāti, kritērijiem, kas padara likumīgu datu apstrādi policijas un tiesu iestāžu vajadzībām, par aizdomās neturētu personu datiem, prasībām attiecībā uz personas datu pārsūtīšanu kompetentām iestādēm citās dalībvalstīs un trešās valstīs, datu subjekta tiesībām, uzraudzības iestādēm un iespējamo padomdevējas iestādes izveidošanu datu aizsardzībai trešajā pīlārā.

Darba grupa, kas izveidota atbilstoši 29. pantam Direktīvā 95/46/EK, tika regulāri informēta par pašreizējām norisēm. Komisija 2005. gada 12. aprīlī un 21. jūnijā piedalījās Eiropas datu aizsardzības iestāžu konferences policijas darba grupas sanāksmēs. Komisija 2005. gada 31. janvārī piedalījās publiskā seminārā „Datu aizsardzība un pilsoņu drošība: kādi ir Eiropas Savienības principi?", kuru organizēja Pilsoņu brīvību, tieslietu un iekšlietu komiteja. Komisija ņēma vērā 2005. gada 25.-26. aprīlī Krakovā notikušās Eiropas datu aizsardzības iestāžu pavasara konferences rezultātus un Eiropas Parlamenta nostāju, kas, *inter alia*, izklāstīta Eiropas Parlamenta ieteikumā Eiropadomei un Padomei par informācijas apmaiņu un sadarbību attiecībā uz teroristu uzbrukumiem (2005/2046(INI)), kas pieņemts 2005. gada 7. jūnijā.

Atbilžu kopsavilkums un tas, kā tās ņemtas vērā

Gan Eiropas Parlaments, gan Eiropas Savienības datu aizsardzības iestādes stingri atbalsta tiesību akta par personas datu aizsardzību izdošanu trešajā pīlārā. Dalībvalstu un Islandes, Norvēģijas un Šveices valdību un Eiropola un Eurojust pārstāvji neizteica kopēju nostāju minētajā sakarā. Tomēr Komisija varēja izdarīt secinājumu, ka nav principiālu iebildumu minētā tiesību akta izveides idejai. Visi šķietami piekrita, ka līdz ar informācijas pieejamības principu ir jāievieš atbilstoši līdzsvarojoši nosacījumi datu aizsardzības jomā. Dažas dalībvalstis paziņoja, ka vispirms ir jādefinē, kā notiks informācijas apmaiņa nākotnē, un pēc tam jānosaka personas datu aizsardzības noteikumi. Dažas deva priekšroku konkrētu nosacījumu attiecībā uz pieejamības principu iekļaušanai šajā aktā.

Pēc atšķirīgo nostāju izvērtēšanas Komisijas nostāja ir tāda, ka informācijas pieejamības principa ieviešana turpmāk attīstīs un pamatos mainīs informācijas apmaiņas starp dalībvalstīm kvalitāti un intensitāti. Minētā attīstība lielā mērā ietekmēs personu datus un tiesības uz datu aizsardzību. Tā ir atbilstoši jālīdzsvaro. Jaunākās iniciatīvas, kuru mērķis ir tieša automatizēta piekļuve, vismaz pēc rezultatīvo/nerezultatīvo meklējumu principa var paaugstināt nelikumīgu, neprecīzu un neatjaunotu datu apmaiņas risku, un tās ir jāņem vērā. Šīs iniciatīvas nozīmē, ka datu apstrādātājs vairs nevarēs katrā atsevišķā gadījumā pārbaudīt nosūtīšanas likumību un attiecīgo datu precizitāti. Līdz ar to tām ir jāpievieno stingras saistības pastāvīgi nodrošināt un pārbaudīt to datu kvalitāti, kuriem ir noteikta tieša automatizēta piekļuve.

Pievēršot īpašu uzmanību informācijas pieejamības principa ieviešanai, nosacījumi, kuri vienīgi risina datu aizsardzības individuālos aspektus, nav pietiekami. Tiesību akts par personas datu aizsardzību trešajā pīlārā principā var dot ieguldījumu policijas un tiesu iestāžu sadarbības veicināšanā krimināllietās gan attiecībā uz tās efektivitāti, gan arī tās likumību un atbilstību pamattiesībām, jo īpaši tiesībām uz personas datu aizsardzību.

Ņemot vērā informācijas pieejamības principa ieviešanu, minētais tiesību akts ir jo īpaši nepieciešams un ir jāizstrādā vienlaikus ar šā principa ieviešanu. Pamatlēmumā, ciktāl iespējams, ir jāievēro Direktīvas 95/46/EK gars un struktūra, tajā pašā laikā ņemot vērā policijas un tiesu iestāžu sadarbības vajadzības krimināllietās un proporcionalitātes principu.

Ir ņemts vērā Eiropas Padomes 1987. gada Ieteikums Nr. R(87)15, kas reglamentē personas datu izmantošanu policijas vajadzībām, lai transponētu tā galvenos principus juridiski saistošos nosacījumos ES līmenī. Ir jānosaka skaidri personas datu aizsardzības noteikumi, kuri ir vai bija jāatklāj citu dalībvalstu kompetentām iestādēm. Tas nozīmē izveidot sistēmu, kura nodrošina attiecīgo datu apstrādes kvalitāti. Minētajā sistēmā ir jāietver nosacījumi, kas paredz attiecīgas datu subjekta tiesības un uzraudzības iestāžu pilnvaras, jo minēto tiesību un pilnvaru īstenošana var ietekmēt attiecīgo datu kvalitāti.

- **Ietekmes novērtējums**

Tika izskatīti šādi varianti. Direktīvas 95/46/EK piemērojamība; priekšlikuma neierosināšana vai priekšlikuma vēlāka ierosināšana par personas datu aizsardzību trešajā pīlārā; ierobežots īpašu nosacījumu kopums tiesību aktā attiecībā uz informācijas apmaiņu atbilstoši pieejamības principam; pamatlēmums par personas datu aizsardzību trešajā pīlārā. Attiecībā uz pamatlēmumu tika izpētīts, vai minētajam tiesību aktam ir jāattiecas arī uz informācijas apmaiņu, izmatojot informācijas sistēmas, un informācijas apmaiņu, ko veic organizācijas, kas izveidotas ES līmenī.

Direktīvas 95/46/EK pamata un visaptverošie nosacījumi nav piemērojami trešajā pīlārā, kā noteikts tās 3. panta 2. punktā. Pat šī panta svītrošana automātiski nepadarītu šo direktīvu piemērojamu policijas un tiesu iestāžu sadarbībai krimināllietās. Pirmkārt, direktīvā nav pilnībā ņemta vērā šīs sadarbības specifika, un to vajadzētu sīkāk precizēt. Otrkārt, ir jāievēro tiesību aktu prasības, kas attiecas uz VI sadaļu Līgumā par Eiropas Savienību, kuras mērķis ir veicināt policijas un tiesu iestāžu sadarbību krimināllietās. Variants, kas paredz priekšlikuma neierosināšanu vai priekšlikuma par personas datu apstrādes noteikumiem un personas datu aizsardzību trešajā pīlārā vēlāku ierosināšanu, ir jāizslēdz. Šis variants var nozīmēt to, ka līdz ar pieejamības principa ieviešanu tiek ieviestas jaunas informācijas apmaiņas formas, nenodrošinot galveno nosacījumu datu aizsardzības jomā stingru ievērošanu. Ierobežots specifisku nosacījumu kopums tiesību aktā attiecībā uz informācijas apmaiņu atbilstoši pieejamības principam nav pietiekams, ņemot vērā šā principa iespējamo ietekmi. Pamatlēmums par personas datu, ko apstrādā, sadarbojoties policijas un tiesu iestādēm krimināllietās, aizsardzību, ir vienīgais pilnībā apmierinošais variants. Maz ticams, ka šis variants varētu radīt dalībvalstīm ievērojamas administratīvās izmaksas, ja vispār tādas būtu.

Komisija veica ietekmes novērtējumu, kurš ir minēts darba programmā, un šis ietekmes novērtējums ir pieejams tīmekļa vietnē: http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3) PRIEKŠLIKUMA TIESISKIE FAKTORI

- **Ierosinātās rīcības kopsavilkums**

Ierosinātajā pamatlēmumā ir ietverti vispārīgie noteikumi attiecībā uz personas datu apstrādes likumību, nosacījumi attiecībā uz konkrētiem apstrādes veidiem (personas datu nosūtīšana un to atklāšana dalībvalstu kompetentām iestādēm, no dalībvalstu kompetentām iestādēm saņemtu datu vai datu, kurus šīs iestādes atklājušas, turpmāka apstrāde, īpaši tālāka pārsūtīšana), datu subjekta tiesības, apstrādes konfidencialitāte un drošība, tiesiskās aizsardzības līdzekļi, atbildība, sankcijas, uzraudzības iestādes un darba grupa fizisku personu aizsardzībai attiecībā uz personas datu apstrādi kriminālnoziegumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem. Īpaša uzmanība ir jāpievērš principam, kas paredz, ka personas dati tiek nosūtīti tikai tām trešām valstīm un starptautiskām organizācijām, kuras

nodrošina atbilstošu aizsardzības līmeni. Pamatlēmumā paredzēts mehānisms, kura mērķis ir šā principa ievērošana visā ES.

- **Juridiskais pamats**

Šis pamatlēmums ir balstīts uz 30. pantu, 31. pantu un 34. panta 2. punkta b) apakšpunktu Līgumā par Eiropas Savienību. Īpaši ievērojot pieejamības principa ieviešanu, atbilstīgi nosacījumi attiecībā uz personas datu apstrādi un aizsardzību, tostarp kopēji standarti personas datu nosūtīšanai trešām valstīm un starptautiskām organizācijām, ir būtiski svarīgi policijas un tiesu iestāžu sadarbības uzlabošanai krimināllietās, īpaši cīņā pret terorismu un nopietniem noziegumiem. Turklāt dalībvalstis tikai tad pilnībā uzticēsies viena otrai, ja būs skaidri un kopēji noteikumi attiecībā uz apmainīto datu iespējamu tālāku pārsūtīšanu citām personām, īpaši trešām valstīm. Ierosinātie nosacījumi arī nodrošina, ka informācijas apmaiņu starp kompetentām iestādēm nekavē dalībvalstu datu aizsardzības atšķirīgie līmeņi.

- **Subsidiaritātes un proporcionalitātes princips**

Šis pamatlēmums pievēršas situācijām, kas ir īpaši nozīmīgas policijas un tiesu iestāžu sadarbībai starp dalībvalstīm krimināllietās, jo īpaši informācijas apmaiņai, lai nodrošinātu un veicinātu efektīvus un likumīgus pasākumus noziedzības novēršanā un apkarošanā *visās* dalībvalstīs, īpaši attiecībā uz nopietniem noziegumiem un terorismu. Atsevišķām dalībvalstīm var būt lietderīgi valstu, divpusēji vai daudzpusēji risinājumi, bet tajos nebūtu ņemta vērā visas Eiropas Savienības nepieciešamība pēc iekšējās drošības. Tiesībaizsardzības iestāžu nepieciešamību pēc informācijas lielā mērā nosaka integrācijas līmenis starp valstīm. Tiek lēsts, ka informācijas apmaiņa starp dalībvalstīm tiesībaizsardzības mērķiem pieaugs, un tāpēc tā ir jāpapildina ar vienotiem noteikumiem par datu apstrādi un datu aizsardzību. Pamatlēmumā ir ievērots subsidiaritātes princips, kas paredzēts 2. pantā Līgumā par Eiropas Savienību un 5. pantā Eiropas Kopienas dibināšanas līgumā, ciktāl tā mērķis ir tuvināt dalībvalstu tiesību aktus un noteikumus, ko dalībvalstis nevar atbilstoši izdarīt, darbojoties vienpusēji, un attiecībā uz kuriem ir nepieciešama saskaņota rīcība Eiropas Savienībā. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šis pamatlēmums nepārsniedz to, kas ir vajadzīgs šā mērķa sasniegšanai. Īpaši šis lēmums attiecas vienīgi uz personas datu apstrādi, ciktāl tā skar policijas un tiesu iestāžu sadarbību krimināllietās.

- **Tiesību aktu izvēle**

Ierosinātais tiesību akts: pamatlēmums. Šā tiesību akta mērķis ir tuvināt dalībvalstu tiesību aktus un noteikumus attiecībā uz personas datu, ko apstrādā noziedzības novēršanas un apkarošanas mērķiem, aizsardzību.

4) IETEKME UZ BUDŽETU

Ierosinātā pamatlēmuma īstenošana ir saistīta vienīgi ar nelieliem administratīviem izdevumiem, kas atskaitāmi no Eiropas Kopienu budžeta, un tie ir saistīti ar komitejas un padomdevējas iestādes, kura jāizveido atbilstoši 16. un 31. pantam, sanāksmēm un sekretāru pakalpojumiem.

2005/0202 (CNS)

Priekšlikums

PADOMES PAMATLĒMUMS

par personas datu, ko apstrādā, sadarbojoties policijas un tiesu iestādēm krimināllietās, aizsardzību

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienību, un jo īpaši tā 30. pantu, 31. pantu un 34. panta 2. punkta b) apakšpunktu,

ņemot vērā Komisijas priekšlikumu,[23]

ņemot vērā Eiropas Parlamenta atzinumu,[24]

tā kā:

(1) Eiropas Savienība ir noteikusi sev mērķi uzturēt un attīstīt Eiropas Savienību kā brīvības, drošības un tiesiskuma telpu; dalībvalstu kopīgai rīcībai ir jānodrošina augsts drošības līmenis policijas un tiesu iestāžu sadarbības jomā krimināllietās.

(2) Kopīga rīcība policijas sadarbības jomā atbilstoši 30. panta 1. punkta b) apakšpunktam Līgumā par Eiropas Savienību un kopīga rīcība tiesu iestāžu sadarbībā krimināllietās atbilstoši 31. panta 1. punkta a) apakšpunktam Līgumā par Eiropas Savienību norāda uz nepieciešamību pēc attiecīgās informācijas, uz kuru jāattiecina atbilstoši personas datu aizsardzības noteikumi, apstrādes.

(3) Tiesību aktiem, kas attiecas uz VI sadaļu Līgumā par Eiropas Savienību, ir jāveicina policijas un tiesu iestāžu sadarbība krimināllietās attiecībā uz tās efektivitāti, kā arī tās likumību un atbilstību pamattiesībām, jo īpaši tiesībām uz privātās dzīves neaizskaramību un personas datu aizsardzību. Kopēji standarti, kas attiecas uz personas datu, kuri apstrādāti noziedzības novēršanas un apkarošanas mērķiem, apstrādi un aizsardzību, var dot ieguldījumu abu mērķu sasniegšanā.

(4) Hāgas programmā brīvības, drošības un tiesiskuma stiprināšanai Eiropas Savienībā, kuru Eiropadome pieņēma 2004. gada 4. novembrī, ir uzsvērta vajadzība pēc novatoriskas pieejas tiesībaizsardzības informācijas pārrobežu apmaiņai, stingri ievērojot galvenos nosacījumus datu aizsardzības jomā, un aicināja Komisiju vēlākais līdz 2005. gada beigām iesniegt priekšlikumus šajā sakarā. Tas bija atspoguļots *Padomes un Komisijas rīcības plānā par to, kā īstenot Hāgas programmu brīvības, drošības un tiesiskuma stiprināšanai Eiropas Savienībā*[25].

(5) Skaidriem, saistošiem noteikumiem, kas veicina kompetento iestāžu savstarpēju uzticēšanos un attiecīgās informācijas aizsardzību, ir jāatbalsta personas datu apmaiņa, kura tiek veikta, sadarbojoties policijai un tiesu iestādēm krimināllietās, īpaši saskaņā ar informācijas pieejamības principu, kā noteikts Hāgas programmā, tā, lai izslēgtu

---

23 …

24 …

25 OV C 198, 12.8.2005., 1. lpp.

jebkādus šķēršļus šai sadarbībai starp dalībvalstīm, pilnībā ievērojot fizisku personu pamattiesības. Eiropas līmenī spēkā esošie tiesību akti nav pietiekami. Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EC par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti[26] nepiemēro personas datu apstrādes darbībām jomās, uz kurām neattiecas Kopienas tiesību akti, piemēram, tiesību akti, kas paredzēti VI sadaļā Līgumā par Eiropas Savienību, un, jebkurā gadījumā, apstrādes darbībām attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību un valsts pasākumiem krimināltiesību jomā.

(6) Tiesību aktam par kopējiem standartiem, kas attiecas uz personas datu, kuri apstrādāti noziedzības novēršanas un apkarošanas mērķiem, aizsardzību, ir jābūt saskanīgiem ar Eiropas Savienības vispārējo politiku privātās dzīves neaizskaramības un datu aizsardzības jomā. Kur vien iespējams, ņemot vērā vajadzību paaugstināt policijas, muitas, tiesu iestāžu un citu kompetentu iestāžu likumīgo darbību efektivitāti, tajā līdz ar to ir jāievēro pašreizējie un pārbaudītie principi un definīcijas, jo īpaši tie principi un definīcijas, kas noteiktas Eiropas Parlamenta un Padomes Direktīvā 95/46/EK, vai kas attiecas uz informācijas apmaiņu starp Eiropolu un Eurojust, vai informācijas, kura apstrādāta, izmantojot Muitas informācijas sistēmu, apmaiņu, vai citi salīdzināmi tiesību akti.

(7) Dalībvalstu noteikumu tuvināšana nedrīkstētu radīt to sniegtās datu aizsardzības jebkādu samazinājumu, bet gan tieši pretēji, tai jācenšas nodrošināt Kopienā augstu aizsardzības līmeni.

(8) Ir jāprecizē datu aizsardzības mērķi policijas un tiesu iestāžu darbībā un jāizstrādā noteikumi, kas attiecas uz personas datu apstrādi, lai nodrošinātu, ka jebkura informācija, ar ko varētu apmainīties, tiek apstrādāta likumīgi un atbilstoši pamatprincipiem, kas attiecas uz datu kvalitāti. Tajā pašā laikā nekādā veidā nedrīkst apdraudēt policijas, muitas, tiesu iestāžu un citu kompetentu iestāžu likumīgās darbības.

(9) Lai nodrošinātu Eiropas pilsoņu personas datu augstu aizsardzības līmeni, ir vajadzīgi kopēji nosacījumi, lai noteiktu datu, kurus apstrādājušas kompetentas iestādes citās dalībvalstīs, likumību un kvalitāti.

(10) Ir lietderīgi noteikt Eiropas līmenī nosacījumus, saskaņā ar kuriem dalībvalstu kompetentām iestādēm atļauts personas datus nosūtīt vai atklāt iestādēm un privātpersonām citās dalībvalstīs.

(11) Personas datu, kuri saņemti no citu dalībvalstu kompetentām iestādēm, vai kurus tās atklājušas, turpmākai apstrādei, jo īpaši minēto datu tālākai pārsūtīšanai vai atklāšanai ir jāpiemēro kopēji noteikumi Eiropas līmenī.

(12) Gadījumos, kad personas dati tiek nosūtīti no Eiropas Savienības dalībvalsts uz trešām valstīm vai starptautiskām organizācijām, šiem datiem principā ir jāsaņem pienācīga aizsardzības līmeņa priekšrocības.

(13) Šim pamatlēmumam ir jānosaka kārtība, kādā tiek pieņemti pasākumi, kas nepieciešami, lai novērtētu kādas trešās valsts vai starptautiskas organizācijas datu aizsardzības līmeni.

(14) Lai nodrošinātu personas datu aizsardzību, nekaitējot kriminālizmeklēšanas mērķiem, ir nepieciešams noteikt datu subjekta tiesības.

---

[26] OV L 281, 23.11.1995., 31. lpp.

(15) Ir lietderīgi izveidot kopējus noteikumus attiecībā uz datu apstrādes konfidencialitāti un drošību, kompetento iestāžu atbildību un tām piemērojamām sankcijām par datu nelikumīgu izmantošanu, kā arī attiecībā uz tiesiskās aizsardzības līdzekļiem, kas ir pieejami datu subjektam. Turklāt ir nepieciešams, lai dalībvalstis paredz krimināl sankcijas par īpaši nopietniem un starptautiska mēroga datu aizsardzības nosacījumu pārkāpumiem.

(16) Uzraudzības iestāžu, kuras pilda savas funkcijas pilnīgi neatkarīgi, izveide dalībvalstīs ir būtiska aizsardzības sastāvdaļa attiecībā uz personas datiem, ko apstrādā, sadarbojoties dalībvalstu policijas un tiesu iestādēm.

(17) Minēto iestāžu rīcībā jābūt nepieciešamajiem līdzekļiem to pienākumu veikšanai, tostarp pilnvarām veikt izmeklēšanu un iejaukties, jo īpaši personu sūdzību gadījumos, un pilnvarām iesaistīties tiesvedībā. Šīm pilnvarām jāpalīdz nodrošināt datu apstrādes caurskatāmību dalībvalstīs, kuru jurisdikcijā ir šīs iestādes. Tomēr šo iestāžu pilnvaras nedrīkst būt pretrunā ar īpašajiem noteikumiem, kas paredzēti kriminālprocesā, un ietekmēt tiesu varas neatkarību.

(18) Ir jāizveido savu funkciju veikšanā pilnīgi neatkarīga darba grupa fizisku personu aizsardzībai attiecībā uz personas datu apstrādi kriminālnoziegumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem. Tai ir jāsniedz padomi Komisijai un dalībvalstīm un jo īpaši jāveicina valstu noteikumu, kas pieņemti saskaņā ar šo pamatlēmumu, vienāda piemērošana.

(19) Līguma par Eiropas Savienību 47. pants nosaka, ka neviens no šā Līguma noteikumiem neierobežo Eiropas Kopienu dibināšanas līgumus vai vēlākus līgumus un aktus, kas tos groza vai papildina. Tādējādi šis pamatlēmums neietekmē personas datu aizsardzību, kas paredzēta Kopienas tiesību aktos, jo īpaši Eiropas Parlamenta un Padomes Direktīvā 95/46/EK, Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulā (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un organizācijās un par šādu datu brīvu apriti[27] un Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvā 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju)[28].

(20) Šis pamatlēmums neierobežo īpašos datu aizsardzības nosacījumus, kas paredzēti attiecīgajos tiesību aktos par personas datu apstrādi un aizsardzību, ko veic Eiropols, Eurojust un Muitas informācijas sistēma.

(21) Jautājumos, uz kuriem attiecas Līgums par Eiropas Savienību, nosacījumi attiecībā uz personas datu aizsardzību, kas paredzēta IV sadaļā 1990. gada Konvencijā, ar ko īsteno 1985. gada 14. jūnijā noslēgto Šengenas Līgumu par pakāpenisku kontroles atcelšanu pie kopīgajām robežām[29] (še turpmāk „Šengenas Konvencija”), un kas iekļauta Eiropas Savienības sistēmā atbilstoši protokolam, kas pievienots Līgumam par Eiropas Savienību un Eiropas Kopienas dibināšanas līgumam, ir jāaizstāj ar šā pamatlēmuma noteikumiem.

(22) Ir lietderīgi šo pamatlēmumu piemērot personas datiem, ko apstrādā otrās paaudzes Šengenas informācijas sistēmā, un ar to saistītajai papildu informācijas apmaiņai

---

27 OV L 8, 12.1.2001., 1. lpp.
28 OV L 201, 31.7.2001., 37. lpp.
29 OV L 239, 22.9.2000., 19. lpp.

atbilstoši Lēmumam TI/2006/ … par otrās paaudzes Šengenas informācijas sistēmas izveidošanu, darbību un izmantošanu.

(23) Šis pamatlēmums neierobežo noteikumus, kas attiecas uz nelikumīgu piekļuvi datiem, kā paredzēts Padomes Pamatlēmumā 2005/222/TI (2005. gada 24. februāris) par uzbrukumiem informācijas sistēmām[30].

(24) Ir lietderīgi aizstāt 23. pantu Konvencijā par Eiropas Savienības dalībvalstu savstarpējo palīdzību krimināllietās[31].

(25) Ikvienu atsauci uz Eiropas Padomes 1981. gada 28. janvāra Konvenciju Personu aizsardzībai attiecībā uz personisko datu automātisko apstrādi uzskata par atsauci uz šo pamatlēmumu.

(26) Tā kā šīs rīcības mērķus, proti, kopēju noteikumu noteikšanu personas datu, ko apstrādā, sadarbojoties policijas un tiesu iestādēm krimināllietās, aizsardzībai, nevar pietiekamā mērā sasniegt, ja dalībvalstis darbojas vienas pašas, un minētās rīcības mērogu un seku dēļ tos labāk var sasniegt Eiropas Savienības līmenī, Padome var pieņemt pasākumus atbilstoši subsidiaritātes principam, kā noteikts 5. pantā EK Līgumā un kā minēts 2. pantā Līgumā par Eiropas Savienību. Saskaņā ar proporcionalitātes principu, kā to paredz 5. pants EK Līgumā, šis pamatlēmums nepārsniedz minēto mērķu sasniegšanai vajadzīgos pasākumus.

(27) Apvienotā Karaliste piedalās šajā pamatlēmumā saskaņā ar 5. pantu Protokolā par Šengenas *acquis* iekļaušanu Eiropas Savienības sistēmā, kas pievienots Līgumam par Eiropas Savienību un Eiropas Kopienas dibināšanas līgumam, un 8. panta 2. punktu Padomes Lēmumā 2000/365/EK (2000. gada 29. maijs) par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā[32].

(28) Īrija piedalās šajā lēmumā saskaņā ar 5. pantu Protokolā, ar ko Šengenas *acquis* integrē Eiropas Savienībā un kas pievienots Līgumam par Eiropas Savienību un Eiropas Kopienas dibināšanas līgumam, un 6. panta 2. punktu Padomes Lēmumā 2002/192/EK (2002. gada 28. februāris) par Īrijas lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā.

(29) Attiecībā uz Islandi un Norvēģiju šis lēmums turpmāk attīsta Šengenas *acquis* nosacījumus, kā tas paredzēts nolīgumā, ko noslēgusi Eiropas Savienības Padome, Islandes Republika un Norvēģijas Karaliste par šo divu valstu asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un izstrādē, un tas pieder jomai, kas minēta 1. panta H punktā Padomes 1999. gada 17. maija Lēmumā 1999/437/EK par dažiem pasākumiem, lai piemērotu minēto nolīgumu[33].

(30) Attiecībā uz Šveici šis pamatlēmums turpmāk attīsta Šengenas *acquis* nosacījumus, kā tas paredzēts Nolīgumā, ko noslēgusi Eiropas Savienība, Eiropas Kopiena un Šveices Konfederācija par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un izstrādē, un tas pieder jomai, kas minēta 1. panta H punktā Padomes 1999. gada 17. maija Lēmumā 1999/437/EK par dažiem pasākumiem, lai piemērotu minēto nolīgumu, un kas skatāma saistībā ar 4. panta 1. punktu Padomes

---

30 OV L 69, 16.3.2005., 67. lpp.
31 OV C 197, 12.7.2000., 3. lpp.
32 OV L 131, 1.6.2000., 43. lpp.
33 OV L 176, 10.7.1999., 31. lpp.

Lēmumā 2004/849/EK par nolīguma parakstīšanu Eiropas Savienības vārdā un par dažu tā noteikumu provizorisku piemērošanu[34].

(31) Šis pamatlēmums ir dokuments, ar kuru attīsta Šengenas *acquis*, vai kas ar to citādi saistīts 2003. gada Pievienošanās akta 3. panta 1. punkta nozīmē.

(32) Šis pamatlēmums ievēro pamattiesības un principus, kas jo īpaši atzīti Eiropas Savienības Pamattiesību hartā. Šā pamatlēmuma mērķis ir nodrošināt tiesību uz privātās dzīves neaizskaramību ievērošanu pilnībā un 7. un 8. pantā Eiropas Savienības Pamattiesību hartā minēto personas datu aizsardzību,

IR PIEŅĒMUSI ŠO PAMATLĒMUMU.

I NODAĻA
MĒRĶIS, DEFINĪCIJAS UN DARBĪBAS JOMA

1. pants
Mērķis

1. Šis pamatlēmums nosaka kopējus standartus, lai nodrošinātu fizisku personu aizsardzību attiecībā uz personas datu apstrādi, kura tiek veikta, sadarbojoties policijas un tiesu iestādēm krimināllietās, kā paredzēts VI sadaļā Līgumā par Eiropas Savienību.

2. Dalībvalstis nodrošina, lai personas datu atklāšana citu dalībvalstu kompetentām iestādēm netiktu ierobežota vai aizliegta, pamatojoties uz šajā pamatlēmumā paredzēto personas datu aizsardzību.

2. pants
Definīcijas

Šajā pamatlēmumā:

(a) „personas dati" ir jebkura informācija attiecībā uz identificētu vai identificējamu fizisku personu („datu subjektu"); identificējama persona ir tā, kuru var identificēt tieši vai netieši, jo īpaši, norādot personas kodu vai vienu vai vairākus šai personai raksturīgus fiziskās, fizioloģiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktorus;

(b) „personu datu apstrāde" („apstrāde") ir jebkura ar personas datiem veikta darbība vai darbību kopums ar vai bez automatizētiem līdzekļiem, kā vākšana, reģistrēšana, organizēšana, uzglabāšana, piemērošana vai pārveidošana, atgūšana, konsultēšana, izmantošana, atklāšana, pielietojot pārsūtīšanu, izplatīšanu vai, atklājot tos citādā veidā, saskaņošana vai savienošana, piekļuves noslēgšana, dzēšana vai iznīcināšana;

(c) „personu datu kartotēka" („kartotēka") ir jebkurš sakārtots personu datu kopums, kurā šie dati ir pieejami saskaņā ar īpašiem kritērijiem – centralizētiem, decentralizētiem vai izkliedētiem, pamatojoties uz funkcionālu vai ģeogrāfisku motivāciju;

(d) „personas datu apstrādātājs" ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita organizācija, kura viena pati vai kopīgi ar citām nosaka personas

[34] OV L 368, 15.12.2004., 26. lpp.

datu apstrādes nolūkus un līdzekļus; ja apstrādes nolūkus un līdzekļus nosaka valsts tiesību akti vai tiesību akti, kas pieņemti saskaņā ar VI sadaļu Līgumā par Eiropas Savienību, personas datu apstrādātāju vai viņa iecelšanas konkrētos kritērijus var noteikt valsts tiesību akti vai tiesību akti, kas paredzēti VI sadaļā Līgumā par Eiropas Savienību;

(e) „apstrādātājs" ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita organizācija, kura personas datu apstrādātāja interesēs apstrādā personas datus;

(f) „trešā persona" ir jebkura fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita organizācija, kura nav datu subjekts, personas datu apstrādātājs, apstrādātājs, un personas, kuras ir pilnvarotas apstrādāt datus personas datu apstrādātāja vai apstrādātāja tiešā vadībā;

(g) „saņēmējs" ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita organizācija, kurai tiek atklāti dati neatkarīgi no tā, vai tās ir vai nav trešās personas;

(h) „datu subjekta piekrišana" ir jebkurš labprātīgi sniegts šīs personas vēlmju konkrēts un paziņots norādījums, ar kuru datu subjekts izsaka savu piekrišanu uz viņu attiecināmu personas datu apstrādei;

(i) „starptautiskas organizācijas" ir struktūras vai organizācijas, kuras izveidotas atbilstoši starptautiskiem nolīgumiem;

(j) „kompetentas iestādes" ir policijas spēki, muitas, tiesu un citas kompetentas dalībvalstu iestādes 29. panta Līgumā par Eiropas Savienību nozīmē.

3. pants
Darbības joma

1. Šis pamatlēmums attiecas uz personas datu apstrādi ar pilnībā vai daļēji automatizētiem līdzekļiem un uz personas datu, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, apstrādi, kura netiek veikta ar automatizētiem līdzekļiem, ko veic kompetentas iestādes kriminālnoziegumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem.

2. Šis pamatlēmums neattiecas uz personas datu apstrādi, ko veic

– Eiropas Policijas birojs (Eiropols),

– Eiropas Tiesiskās sadarbības vienība (Eurojust),

– Muitas informācijas sistēma, kas izveidota atbilstoši Konvencijai par informācijas tehnoloģijas izmantošanu muitas nolūkiem, kura sastādīta, pamatojoties uz K.3 pantu Līgumā par Eiropas Savienību, un jebkādiem tajā izdarītajiem grozījumiem.

II NODAĻA
VISPĀRĪGI NOTEIKUMI PAR PERSONAS DATU APSTRĀDES LIKUMĪBU

4. pants
Principi, kas attiecas uz datu kvalitāti

1. Dalībvalstis nosaka to, ka personas datiem jābūt

(a) apstrādātiem godīgi un likumīgi;

(b) vāktiem konkrētiem, precīzi formulētiem un likumīgiem nolūkiem, un tos nedrīkst turpmāk apstrādāt ar šiem nolūkiem nesavienojamā veidā. Turpmāka datu apstrāde vēsturiskiem, statistiskiem vai zinātniskiem nolūkiem nav uzskatāma par neatbilstīgu, ja dalībvalstis sniedz atbilstošas garantijas;

(c) adekvātiem, attiecīgiem un ne pārmērīgā apjomā attiecībā uz nolūkiem, kādiem tie savākti un/vai turpmāk apstrādāti;

(d) precīziem un nepieciešamības gadījumā atjauninātiem. Jāveic visi pamatotie pasākumi, lai nodrošinātu, ka datus, kuri ir neprecīzi vai nepilnīgi, dzēš vai izlabo, ņemot vērā to vākšanas vai turpmākās apstrādes nolūkus. Dalībvalstis var noteikt atšķirīgas datu apstrādes precizitātes un uzticamības pakāpes, un tādā gadījumā tām ir jānosaka, ka datus izšķir atbilstoši to precizitātes un uzticamības pakāpei, un jo īpaši, ka datus, kas pamatojas uz faktiem, atšķir no datiem, kas pamatojas uz viedokļiem vai personīgiem vērtējumiem;

(e) saglabātiem veidā, kas pieļauj datu subjektu identifikāciju ne ilgāk, kā tas nepieciešams nolūkiem, kuriem datus vāca, vai kuriem tos turpmāk apstrādā. Dalībvalstis nosaka atbilstošas garantijas personas datiem, kurus uzglabā ilgāku laiku, lai izmantotu vēsturiskiem, statistiskiem vai zinātniskiem nolūkiem.

2. Personas datu apstrādātājam jānodrošina 1. punkta izpilde.

3. Dalībvalstīm jānosaka skaidrs dalījums starp tādu personu personas datiem,

– kuras tiek turētas aizdomās par noziedzīga nodarījuma izdarīšanu vai līdzdalību tajā,

– kuras ir tiesātas par noziedzīgu nodarījumu,

– attiecībā uz kurām pastāv nopietns iemesls uzskatīt, ka tās izdarīs noziedzīgu nodarījumu,

– kuras var tikt uzaicinātas liecināt izmeklēšanās, kas tiek veiktas saistībā ar noziedzīgiem nodarījumiem, vai turpmākos kriminālprocesos,

– kuras ir bijušas noziedzīgu nodarījumu upuri, vai attiecībā uz kurām zināmi fakti dod iemeslu uzskatīt, ka tās varētu būt noziedzīgu nodarījumu upuri,

– kuras var sniegt informāciju par noziedzīgiem nodarījumiem,

– kuras ir saskarē ar kādu no iepriekš minētajām personām vai ir to līdzzinātājas,

– kuras neatbilst nevienai no iepriekš minētajām kategorijām.

4. Dalībvalstis paredz to, ka personas datu apstrāde ir nepieciešama tikai tad, ja:

– pamatojoties uz konstatētiem faktiem, ir pamatots iemesls uzskatīt, ka attiecīgie personas dati padarīs iespējamu, atvieglos vai paātrinās noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu,

– nav citu līdzekļu, kuri mazāk ietekmē datu subjektu,

– datu apstrāde nav pārmērīga attiecībā pret attiecīgo noziedzīgo nodarījumu.

5. pants

Kritēriji datu apstrādes atzīšanai par likumīgu

Dalībvalstis nosaka, ka kompetentās iestādes var apstrādāt personas datus tikai tad, ja to paredz tiesību akts, kas nosaka, ka šī apstrāde ir nepieciešama attiecīgās iestādes likumīgo uzdevumu izpildei un noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem.

6. pants

Īpašu kategoriju datu apstrāde

1. Dalībvalstis aizliedz tādu personas datu apstrādi, kas atklāj rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās, kā arī uz veselību vai seksuālo dzīvi attiecināmu datu apstrādi.

2. Šā panta 1. punktu nepiemēro, ja

   – apstrāde paredzēta kādā no tiesību aktiem un ir pilnīgi nepieciešama attiecīgās institūcijas likumīgā uzdevuma izpildei noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem vai, ja datu subjekts ir devis skaidri izteiktu piekrišanu apstrādei,

   – dalībvalstis paredz atbilstīgas un konkrētas garantijas, piemēram, piekļuvi attiecīgajiem datiem tikai tiem darbiniekiem, kuri ir atbildīgi par likumīgā uzdevuma, kas pamato šo apstrādi, izpildi.

7. pants

Personas datu uzglabāšanas ierobežojumi

1. Dalībvalstis nosaka, ka personas datus uzglabā ne ilgāk, kā tas nepieciešams nolūkiem, kuriem datus vāca, ja vien valsts tiesību akti neparedz citādi. To personu datus, kuras minētas 4. panta 3. punkta pēdējā ievilkumā, uzglabā tik ilgi, cik tas ir pilnīgi nepieciešams nolūkiem, kuriem datus vāca.

2. Dalībvalstis nosaka atbilstošus procedūras un tehniskos pasākumus, kas nodrošina, lai tiktu ievēroti personas datu uzglabāšanas termiņi. Minēto termiņu ievērošanu regulāri pārbauda.

III NODAĻA – Datu apstrādes īpašie veidi

I IEDAĻA – PERSONAS DATU NOSŪTĪŠANA UN ATKLĀŠANA CITU DALĪBVALSTU KOMPETENTĀM IESTĀDĒM

8. pants

Personas datu nosūtīšana un atklāšana citu dalībvalstu kompetentām iestādēm

Dalībvalstis nosaka, ka personas datus var apstrādāt vai atklāt citu dalībvalstu kompetentām iestādēm tikai tad, ja tas ir nepieciešams nosūtītājas vai saņēmējas iestādes likumīgo uzdevumu izpildei un noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem.

9. pants

Nosūtīto vai atklāto datu kvalitātes pārbaude

1. Dalībvalstis nosaka, ka personas datu kvalitāti pārbauda vēlākais pirms to nosūtīšanas vai atklāšanas. Ciktāl iespējams, visos datu nosūtīšanas gadījumos ir jānorāda tiesu nolēmumi, kā arī lēmumi neveikt kriminālvajāšanu, un dati, kas pamatojas uz viedokļiem vai personīgiem vērtējumiem, pirms nosūtīšanas ir jāpārbauda to izcelsmes vietā un jānorāda to precizitātes vai uzticamības pakāpe.

2. Dalībvalstis nosaka, ka personas datu, kuri atklāti citu dalībvalstu kompetentām iestādēm automatizētā veidā, kvalitāti regulāri pārbauda, lai nodrošinātu pieeju precīziem un atjauninātiem datiem.

3. Dalībvalstis nosaka, ka personas datus, kuri vairs nav precīzi vai nav atjaunināti, nenosūta un neatklāj.

4. Dalībvalstis nosaka, ka kompetenta iestāde, kura personas datus nosūtījusi vai atklājusi citas dalībvalsts kompetentai iestādei, tūlīt to informē, ja pēc pašas iniciatīvas vai datu subjekta pieprasījuma tiek konstatēts, ka attiecīgos datus nedrīkstēja nosūtīt vai atklāt, vai, ka ir nosūtīti vai atklāti neprecīzi vai novecojuši dati.

5. Dalībvalstis nosaka, ka kompetentā iestāde, kura informēta atbilstoši 4. punktam, dzēš vai izlabo attiecīgos datus. Turklāt minētā iestāde izlabo attiecīgos datus, ja tā atklāj, ka šie dati ir neprecīzi. Ja minētajai iestādei ir pamats uzskatīt, ka saņemtie personas dati ir neprecīzi vai dzēšami, tā tūlīt informē kompetento iestādi, kura attiecīgos datus ir nosūtījusi vai atklājusi.

6. Neierobežojot valsts kriminālprocesu, dalībvalstis nosaka, ka pēc datu subjekta pieprasījuma personas datus iezīmē, ja datu subjekts noliedz to precizitāti vai, ja par to precizitāti vai neprecizitāti nav iespējams pārliecināties. Minēto atzīmi dzēš vienīgi ar datu subjekta piekrišanu vai, pamatojoties uz kompetentas tiesas vai kompetentas uzraudzības iestādes lēmumu.

7. Dalībvalstis nosaka, ka personas dati, kas saņemti no citas dalībvalsts iestādes, tiek dzēsti,

   – ja šos datus nedrīkstēja nosūtīt, atklāt vai saņemt,

   – pēc citas dalībvalsts tiesību aktā paredzētā termiņa beigām, ja iestāde, kura attiecīgos nosūtījusi vai atklājusi, nosūtot vai atklājot attiecīgos datus, ir informējusi saņēmēju par minēto termiņu, ja vien šie personas dati nav turpmāk nepieciešami tiesas procesā,

   – ja šie dati nav vai vairs nav nepieciešami nolūkiem, kuriem tos nosūtīja vai atklāja.

8. Ja personas dati nosūtīti bez pieprasījuma, saņēmējs tūlīt pārbauda, vai šie dati ir nepieciešami nolūkiem, kuriem tos nosūtīja.

9. Personas datus nedzēš, bet slēdz piekļuvi šiem datiem atbilstoši valsts tiesību aktiem, ja ir pamats uzskatīt, ka dzēšana var ietekmēt datu subjekta aizsargājamās intereses. Datus, kuriem piekļuve slēgta, izmanto vai nosūta tikai tam nolūkam, kuram datus neizdzēsa.

10. pants
Reģistrēšana un dokumentēšana

1. Dalībvalstis nosaka, ka personas datu katru automatizētu nosūtīšanu vai saņemšanu, jo īpaši, izmantojot tiešu automatizētu piekļuvi, reģistrē, lai nodrošinātu nosūtīšanas iemeslu, nosūtīto datu, nosūtīšanas laika, iesaistīto iestāžu un, ciktāl tas attiecas uz saņēmēju, personu, kuras saņēmušas šos datus, un personu, kuras ierosinājušas to saņemšanu, turpmāku noskaidrošanu.

2. Dalībvalstis nosaka, ka personas datu katru neautomatizētu nosūtīšanu vai saņemšanu reģistrē, lai nodrošinātu nosūtīšanas iemeslu, nosūtīto datu, nosūtīšanas laika, iesaistīto iestāžu un, ciktāl tas attiecas uz saņēmēju, personu, kuras saņēmušas šos datus, un personu, kuras ierosinājušas to saņemšanu, turpmāku noskaidrošanu.

3. Iestāde, kas reģistrējusi vai dokumentējusi minēto informāciju, pēc pieprasījuma tūlīt par to paziņo kompetentai uzraudzības iestādei. Šo informāciju izmanto vienīgi datu aizsardzības nolūkā un, lai nodrošinātu datu atbilstīgu apstrādi, kā arī datu integritāti un drošību.

II IEDAĻA – DATU, KAS SAŅEMTI NO CITU DALĪBVALSTU KOMPETENTĀM IESTĀDĒM, VAI KURUS TĀS ATKLĀJUŠAS, TURPMĀKA APSTRĀDE, JO ĪPAŠI TĀLĀKA NOSŪTĪŠANA UN PĀRSŪTĪŠANA

11. pants
Datu, kas saņemti no citu dalībvalstu kompetentām iestādēm, vai kurus tās atklājušas, turpmāka apstrāde

1. Dalībvalstis nosaka, ka datus, kas saņemti no citu dalībvalstu kompetentām iestādēm, vai kurus tās atklājušas, turpmāk apstrādā vienīgi saskaņā ar šo pamatlēmumu, jo īpaši tā 4., 5. un 6. pantu

   (a) konkrēti tam mērķim, kuram tie nosūtīti vai atklāti,

   (b) vajadzības gadījumā noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem vai, lai novērstu draudus sabiedrības vai kādas personas drošībai, izņemot gadījumus, kad nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības ir svarīgāka par minētajiem apsvērumiem.

2. Attiecīgos personas datus turpmāk apstrādā mērķiem, kas minēti šā panta 1. punkta b) apakšpunktā, vienīgi ar iestādes, kura nosūtījusi vai atklājusi personas datus, iepriekšēju piekrišanu.

3. Ja īpašie tiesību akti, kas minēti VI sadaļā Līgumā par Eiropas Savienību, skaidri nosaka, ka personas datus, kas saņemti no citas dalībvalsts kompetentās iestādes, vai kurus tā atklājusi, turpmāk apstrādā vienīgi mērķiem, kuriem tos nosūtīja vai atklāja, 1. punkta b) apakšpunktu nepiemēro.

12. pants
Pārsūtīšana citām kompetentām iestādēm

Dalībvalstis nosaka, ka personas datus, kas saņemti no citu dalībvalstu kompetentām iestādēm, vai kurus tās atklājušas, tālāk pārsūta vai atklāj dalībvalsts citām kompetentām iestādēm vienīgi, ja tiek izpildītas šādas prasības:

(a) pārsūtīšana vai atklāšana ir paredzēta tiesību aktos, kas skaidri uzliek par pienākumu vai atļauj to;

(b) pārsūtīšana vai atklāšana ir nepieciešama iestādes, kura saņēmusi attiecīgos datus, vai iestādes, kurai tos tālāk pārsūta, likumīgā uzdevuma izpildei;

(c) pārsūtīšana vai atklāšana ir nepieciešama konkrēti tam mērķim, kuram tie pārsūtīti vai atklāti, vai noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem vai, lai novērstu draudus sabiedrības vai kādas personas drošībai, izņemot gadījumus, kad nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības ir svarīgāka par minētajiem apsvērumiem;

(d) tās dalībvalsts kompetentā iestāde, kas pārsūtījusi vai atklājusi attiecīgos datus kompetentajai iestādei, kura ir iecerējusi tos pārsūtīt vai atklāt, ir devusi iepriekšēju piekrišanu to tālākai pārsūtīšanai vai atklāšanai.

13. pants
Pārsūtīšana iestādēm, kas nav kompetentas iestādes

Dalībvalstis nosaka, ka personas datus, kas saņemti no citas dalībvalsts kompetentām iestādēm, vai kurus tās atklājušas, tālāk pārsūta vai atklāj citas dalībvalsts iestādēm, kas nav kompetentas iestādes, vienīgi īpašos gadījumos un, ja tiek izpildītas visas turpmāk minētās prasības:

(a) pārsūtīšana ir paredzēta tiesību aktos, kas skaidri uzliek par pienākumu vai atļauj to;

(b) pārsūtīšana ir

nepieciešama konkrēti tam mērķim, kuram tie nosūtīti vai atklāti, vai noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem vai, lai novērstu draudus sabiedrības vai kādas personas drošībai, izņemot gadījumus, kad nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības ir svarīgāka par minētajiem apsvērumiem,

vai

nepieciešama tāpēc, ka attiecīgie dati ir obligāti vajadzīgi iestādei, kurai tos tālāk pārsūta, lai tā varētu izpildīt savu likumīgo uzdevumu, un, ja datu vākšanas un apstrādes, ko veic minētā iestāde, mērķis nav nesavienojams ar sākotnējo apstrādi un ar to nav pretrunā kompetentās iestādes, kura ir iecerējusi šos datus nosūtīt, juridiskās saistības,

vai

neapšaubāmi datu subjekta interesēs, un vai nu datu subjekts ir piekritis, vai arī apstākļi ir tādi, kas ļauj nepārprotami uzskatīt, ka minētā piekrišana ir saņemta.

(c) Tās dalībvalsts kompetentā iestāde, kas nosūtījusi vai atklājusi attiecīgos datus kompetentajai iestādei, kura ir iecerējusi tos pārsūtīt tālāk, ir devusi iepriekšēju piekrišanu to tālākai pārsūtīšanai.

14. pants
Pārsūtīšana privātpersonām

Dalībvalstis nosaka ka, neierobežojot atbilstību valsts kriminālprocesa noteikumiem, personas datus, kas saņemti no citas dalībvalstu kompetentās iestādes, vai kurus tā atklājusi, var tālāk

pārsūtīt vai atklāt privātpersonām kādā dalībvalstī vienīgi īpašos gadījumos un, ja tiek izpildītas visas turpmāk minētās prasības:

(a) pārsūtīšana ir paredzēta tiesību aktos, kas skaidri uzliek par pienākumu vai atļauj to;

(b) pārsūtīšana nepieciešama tam mērķim, kuram tie nosūtīti vai atklāti, vai noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem vai, lai novērstu draudus sabiedrības vai kādas personas drošībai, izņemot gadījumus, kad nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības ir svarīgāka par minētajiem apsvērumiem;

(c) tās dalībvalsts kompetentā iestāde, kas nosūtījusi vai atklājusi attiecīgos datus kompetentajai iestādei, kura ir iecerējusi tos pārsūtīt, ir devusi iepriekšēju piekrišanu to tālākai pārsūtīšanai privātpersonām.

15. pants

Pārsūtīšana kompetentām iestādēm trešās valstīs vai starptautiskām organizācijām

1. Dalībvalstis nosaka, ka personas datus, kas saņemti no citu dalībvalstu kompetentām iestādēm, vai kurus tās atklājušas, tālāk nepārsūta trešo valstu iestādēm vai starptautiskām organizācijām, izņemot gadījumus, kad minētā pārsūtīšana ir saskaņā ar šo pamatlēmumu un, ja tiek izpildītas visas turpmāk minētās prasības.

   (a) Pārsūtīšana ir paredzēta tiesību aktos, kas skaidri uzliek par pienākumu vai atļauj to.

   (b) Pārsūtīšana ir nepieciešama tam mērķim, kuram tie nosūtīti vai atklāti, vai noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem vai, lai novērstu draudus sabiedrības vai kādas personas drošībai, izņemot gadījumus, kad nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības ir svarīgāka par minētajiem apsvērumiem.

   (c) Citas dalībvalsts kompetentā iestāde, kura ir nosūtījusi vai atklājusi attiecīgos datus kompetentajai iestādei, kura ir iecerējusi tos tālāk pārsūtīt, ir devusi iepriekšēju piekrišanu to tālākai pārsūtīšanai.

   (d) Trešā valsts vai starptautiskā organizācija, kurai tiek pārsūtīti attiecīgie dati, nodrošina pietiekamu datu aizsardzības līmeni.

2. Dalībvalstis nodrošina, ka aizsardzības līmeņa, kuru sniedz kāda trešā valsts vai starptautiska organizācija, pietiekamību novērtē, ievērojot visus pārsūtīšanas vai pārsūtīšanas kategorijas apstākļus. Jo īpaši novērtējums izriet no šādu elementu pārbaudes: datu veids, apstrādes, kurai dati tiek nosūtīti, nolūks un ilgums, izcelsmes valsts un valsts, kura ir galamērķis, trešā valstī vai attiecīgajā organizācijā spēkā esošās vispārējo un nozaru tiesību normas, šajā valstī ievērotie profesionālie un drošības noteikumi, kā arī pietiekamu aizsardzības pasākumu, kurus ieviesis sūtījuma saņēmējs, esamība.

3. Dalībvalstis un Komisija informē viena otru par gadījumiem, kad tās uzskata, ka trešā valsts vai starptautiska organizācija nenodrošina pietiekamu aizsardzības līmeni 2. punkta nozīmē.

4. Ja saskaņā ar 16. pantā paredzēto procedūru tiek konstatēts, ka trešā valsts vai starptautiska organizācija nenodrošina pietiekamu aizsardzības līmeni 2. punkta

nozīmē, dalībvalstis veic vajadzīgos pasākumus, lai novērstu personas datu jebkādu pārsūtīšanu uz attiecīgo trešo valsti vai starptautisko organizāciju.

5. Saskaņā ar 16. pantā minēto procedūru var konstatēt, ka trešā valsts vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni šā panta 2. punkta nozīmē, pamatojoties uz savas valsts tiesību aktiem vai uz starptautiskajām saistībām, kuras tā noslēgusi personu privātās dzīves un pamatbrīvību un tiesību aizsardzībai.

6. Izņēmuma kārtā personas datus, kas saņemti no citas dalībvalsts kompetentās iestādes, var tālāk pārsūtīt trešo valstu kompetentām iestādēm vai starptautiskām organizācijām, kuras nenodrošina pietiekamu datu aizsardzības līmeni, ja tas ir pilnīgi nepieciešams, lai aizsargātu kādas dalībvalsts būtiski svarīgās intereses vai, lai darbotos pret nenovēršamām, nopietnām briesmām, kas apdraud sabiedrības vai kādas konkrētas personas vai personu drošību.

16. pants
Komiteja

1. Ja ir atsauce uz šo pantu, Komisijai palīdz komiteja, kurā ir dalībvalstu pārstāvji un kuras priekšsēdētājs ir Komisijas pārstāvis.

2. Komiteja apstiprina savu reglamentu pēc priekšsēdētāja priekšlikuma, pamatojoties uz standarta reglamentu, kas publicēts *Eiropas Savienības Oficiālajā Vēstnesī*.

3. Komisijas pārstāvis iesniedz komitejai veicamo pasākumu projektu. Komiteja sniedz savu atzinumu par projektu termiņā, ko atkarībā no jautājuma steidzamības var noteikt priekšsēdētājs. Atzinumu sniedz ar balsu vairākumu, kas 205. panta 2. punktā Eiropas Kopienas dibināšanas līgumā paredzēts lēmumiem, kuri Padomei jāpieņem pēc Komisijas priekšlikuma. Dalībvalstu pārstāvju balsu skaitu šajā komitejā vērtē saskaņā ar minēto pantu. Priekšsēdētājs nebalso.

4. Komisija pieņem paredzētos pasākumus, ja tie saskan ar komitejas atzinumu. Ja paredzētie pasākumi nesaskan ar komitejas atzinumu vai, ja atzinums nav sniegts, Komisija tūlīt iesniedz Padomei priekšlikumu par veicamajiem pasākumiem un informē par to Eiropas Parlamentu.

5. Divu mēnešu laikā no priekšlikuma iesniegšanas dienas Padome ar kvalificētu balsu vairākumu var lemt par priekšlikumu.

Ja minētajā termiņā Padome ar kvalificētu balsu vairākumu ir norādījusi, ka tā iebilst priekšlikumam, Komisija to izskata atkārtoti. Tā var iesniegt Padomei grozītu priekšlikumu, iesniegt atkārtotu priekšlikumu vai tiesību akta projektu. Ja minētā termiņa beigās Padome nav pieņēmusi ierosināto ieviešanas aktu vai norādījusi iebildumus ieviešanas pasākumu priekšlikumam, ierosināto ieviešanas aktu pieņem Komisija.

17. pants
12., 13., 14. un 15. panta izņēmumi

Ja īpašie tiesību akti, kas minēti VI sadaļā Līgumā par Eiropas Savienību, skaidri nosaka, ka personas datus, kas saņemti no citas dalībvalsts kompetentās iestādes, vai kurus tā atklājusi, tālāk nepārsūta vai tālāk pārsūta vienīgi saskaņā ar konkrētākiem nosacījumiem, 12., 13., 14. un 15. pantu nepiemēro.

18. pants
Kompetentās iestādes informēšana pēc pieprasījuma

Dalībvalstis nosaka, ka kompetento iestādi, no kuras saņemti personas dati, vai kura tos ir saņēmusi vai atklājusi, pēc pieprasījuma informē par to turpmāku apstrādi un iegūtajiem rezultātiem.

IV NODAĻA
DATU SUBJEKTA TIESĪBAS

19. pants
Tiesības uz informāciju gadījumos, kad datus ievāc no datu subjekta ar viņa ziņu

1. Dalībvalstis paredz, ka personas datu apstrādātājs vai viņa pārstāvis bez maksas sniedz datu subjektam, no kura ar viņa ziņu ievāc datus, kas uz viņu attiecas, vismaz šādu informāciju, ja vien datu subjektam tā nav zināma:

   (a) personas datu apstrādātāja un viņa pārstāvja, ja tāds ir, personas dati;

   (b) apstrādes, kurai dati paredzēti, nolūki;

   (c) jebkura turpmāka informācija, kā,

   – apstrādes juridiskais pamats,

   – datu saņēmēji vai datu saņēmēju kategorijas,

   – vai atbildes uz jautājumiem vai citas sadarbības formas ir obligātas vai brīvprātīgas, kā arī atbildes nesniegšanas vai nesadarbošanās iespējamās sekas,

   – datu piekļuves tiesību un tiesību koriģēt datus, kas uz viņu attiecas, pastāvēšana,

   ciktāl šāda turpmāka informācija vajadzīga, ņemot vērā konkrētos apstākļus, kādos dati ievākti, lai nodrošinātu godprātīgu apstrādi attiecībā uz datu subjektu.

2. Informācijas, kas minēta 1. punktā, sniegšanu atsaka vai ierobežo vienīgi, ja tas ir vajadzīgs,

   (a) lai personas datu apstrādātājs varētu pienācīgi izpildīt savus likumīgos pienākumus,

   (b) lai izvairītos no notiekošu izmeklēšanu vai lietu izskatīšanas vai kompetento iestāžu likumīgo pienākumu izpildes kavēšanas,

   (c) lai aizsargātu sabiedrisko drošību un kārtību dalībvalstī,

   (d) lai aizsargātu trešo personu tiesības un brīvības,

   izņemot gadījumus, kad nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības ir svarīgāka par minētajiem apsvērumiem.

3. Ja 1. punktā minētās informācijas sniegšanu atsaka vai ierobežo, personas datu apstrādātājs informē datu subjektu, ka, neierobežojot tiesiskas aizsardzības līdzekļus un valsts kriminālprocesa noteikumus, viņš var iesniegt sūdzību kompetentajai uzraudzības iestādei.

4. Atteikuma vai ierobežojuma iemeslus atbilstoši 2. punktam neatklāj, ja to paziņošana apdraud atteikuma nolūku. Šādā gadījumā personas datu apstrādātājs informē datu subjektu, ka, neierobežojot tiesiskas aizsardzības līdzekļus un valsts kriminālprocesa noteikumus, viņš var iesniegt sūdzību kompetentajai uzraudzības iestādei. Ja datu

subjekts iesniedz sūdzību uzraudzības iestādei, tā izskata šo sūdzību. Izskatot sūdzību, uzraudzības iestāde viņu vienīgi informē, vai dati ir apstrādāti pareizi, un, ja nē, vai ir izdarīti jebkādi vajadzīgi labojumi.

20. pants

Tiesības uz informāciju, ja dati nav iegūti no datu subjekta vai, ja tie iegūti no datu subjekta bez viņa ziņas

1. Ja dati nav iegūti no datu subjekta vai, ja tie iegūti no datu subjekta bez viņa ziņas vai, viņam neapzinoties, ka tiek vākti dati, kas uz viņu attiecas, dalībvalstis paredz to, ka personas datu apstrādātājam vai viņa pārstāvim personas datu reģistrācijas pasākuma laikā vai, ja ir paredzēta datu atklāšana trešai personai, atbilstošā laikā pēc tam, kad datus pirmoreiz atklāj, bez maksas jāsniedz datu subjektam vismaz šāda informācija, ja viņam tā jau nav zināma vai, ja šīs informācijas sniegšana nav neiespējama vai būtu saistīta ar nesamērīgām pūlēm:

   (a) personas datu apstrādātāja un viņa pārstāvja, ja tāds ir, personas dati;

   (b) apstrādes nolūki;

   (c) jebkura turpmāka informācija, kā

   – apstrādes juridiskais pamats,

   – attiecīgo datu kategorijas,

   – saņēmēji vai saņēmēju kategorijas,

   – datu piekļuves tiesību un tiesību koriģēt datus, kas uz viņu attiecas, pastāvēšana,

   ciktāl šāda turpmāka informācija ir vajadzīga, ņemot vērā konkrētos apstākļus, kādos datus apstrādā, lai nodrošinātu godprātīgu apstrādi attiecībā uz datu subjektu.

2. Informāciju, kas minēta 1. punktā, nesniedz, ja tā ir vajadzīga,

   (a) lai personas datu apstrādātājs varētu pienācīgi izpildīt savus likumīgos pienākumus,

   (b) lai izvairītos no notiekošu izmeklēšanu vai lietu izskatīšanas, vai kompetento iestāžu likumīgo pienākumu izpildes kavēšanas,

   (c) lai aizsargātu sabiedrisko drošību un kārtību dalībvalstī,

   (d) lai aizsargātu trešo personu tiesības un brīvības,

   izņemot gadījumus, kad nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības ir svarīgāka par minētajiem apsvērumiem.

21. pants

Piekļuves tiesības, izlabošana, dzēšana vai piekļuves noslēgšana

1. Dalībvalstis garantē visiem datu subjektiem tiesības iegūt no personas datu apstrādātāja:

   (a) bez ierobežojumiem, samērīgos termiņos un bez pārmērīgas vilcināšanās vai izdevumiem:

   – apstiprinājumu, vai uz viņu attiecināmos datus apstrādā vai neapstrādā, un informāciju vismaz attiecībā uz apstrādes nolūkiem, attiecīgo datu kategorijām,

apstrādes juridisko pamatu un saņēmējiem vai saņēmēju kategorijām, kuriem datus atklāj,

– paziņojumu datu subjektam saprotamā formā par apstrādē esošajiem datiem un par jebkuru pieejamu informāciju attiecībā uz to avotu;

(b) atkarībā no apstākļiem datu izlabošanu, dzēšanu vai piekļuves noslēgšanu, ja šo datu apstrāde neatbilst šā pamatlēmuma nosacījumiem, īpaši datu nepilnības vai neprecizitātes dēļ;

(c) paziņojumu trešām personām, kurām dati atklāti, par jebkuru saskaņā ar b) apakšpunktu veikto izlabošanu, dzēšanu vai piekļuves noslēgšanu, ja vien tas neizrādās neiespējami vai nav saistīts ar nesamērīgām pūlēm.

2. Jebkuras darbības, uz kurām datu subjektam ir tiesības saskaņā ar 1. punktu, vajadzības gadījumā atsaka,

(a) lai personas datu apstrādātājs varētu pienācīgi izpildīt savus likumīgos pienākumus,

(b) lai izvairītos no notiekošu izmeklēšanu vai lietu izskatīšanas, vai kompetento iestāžu likumīgo pienākumu izpildes kavēšanas,

(c) lai aizsargātu sabiedrisko drošību un kārtību dalībvalstī,

(d) lai aizsargātu trešo personu tiesības un brīvības,

izņemot gadījumus, kad nepieciešamība aizsargāt datu subjekta intereses vai pamattiesības ir svarīgāka par minētajiem apsvērumiem.

3. Tiesību, kas minētas 1. punktā, īstenošanas atteikumu vai ierobežojumu izklāsta rakstveidā. Ja 1. punktā minēto tiesību īstenošanu atsaka vai ierobežo, personas datu apstrādātājs informē datu subjektu, ka, neierobežojot tiesiskas aizsardzības līdzekļus un valsts kriminālprocesa noteikumus, viņš var iesniegt sūdzību kompetentajai uzraudzības iestādei.

4. Atteikuma iemeslus atbilstoši 2. punktam neatklāj, ja to paziņošana apdraud atteikuma nolūku. Šādā gadījumā personas datu apstrādātājs informē datu subjektu, ka, neierobežojot tiesiskas aizsardzības līdzekļus un valsts kriminālprocesa noteikumus, viņš var iesniegt sūdzību kompetentajai uzraudzības iestādei. Ja datu subjekts iesniedz sūdzību uzraudzības iestādei, tā izskata šo sūdzību. Izskatot sūdzību, uzraudzības iestāde viņu vienīgi informē, vai dati ir apstrādāti pareizi, un, ja nē, vai ir izdarīti jebkādi vajadzīgi labojumi.

22. pants

Informācijas sniegšana trešām personām pēc izlabošanas, dzēšanas vai piekļuves noslēgšanas

Dalībvalstis nosaka atbilstošus tehniskos pasākumus, lai gadījumos, kad personas datu apstrādātājs pēc pieprasījuma slēdz piekļuvi personas datiem, tos izlabo vai dzēš, nodrošinātu šo datu piegādātāju un adresātu saraksta automātisku izveidošanu. Personas datu apstrādātājs nodrošina, lai sarakstā iekļautās personas tiktu informētas par personas datos izdarītajām pārmaiņām.

V NODAĻA
APSTRĀDES KONFIDENCIALITĀTE UN DROŠĪBA

23. pants
Konfidencialitāte

Jebkura persona, darbojoties saskaņā ar personas datu apstrādātāja vai apstrādātāja pilnvarām, ieskaitot pašu apstrādātāju, kam ir piekļuve personu datiem, nedrīkst apstrādāt šos datus citādi, kā pēc personas datu apstrādātāja norādījumiem, ja vien to darīt nepieprasa likums. Visām personām, kuras ir aicinātas sadarboties ar dalībvalsts kompetento iestādi vai strādāt tajā, ir jāievēro stingri konfidencialitātes noteikumi.

24. pants
Drošība

1. Dalībvalstis nosaka, ka personas datu apstrādātājam jāīsteno atbilstoši tehniski un organizatoriski pasākumi, lai aizsargātu personas datus pret nejaušu vai nelikumīgu iznīcināšanu vai nejaušu nozaudēšanu, pārveidošanu, nesankcionētu atklāšanu vai piekļuvi, īpaši, ja apstrāde ietver datu pārraidi elektronisko sakaru tīklā, vai pret to atklāšanu, piešķirot tiešu automatizētu piekļuvi, un pret visām citām nelikumīgām apstrādes formām, īpaši ņemot vērā riskus, kas raksturīgi aizsargājamo datu apstrādei.

   Ņemot vērā tehnisko un organizatorisko pasākumu pašreizējo līmeni un to īstenošanas izmaksas, minētie pasākumi nodrošina raksturīgajiem apstrādes un aizsargājamo datu riskiem atbilstošu drošības pakāpi. Pasākumus uzskata par vajadzīgiem, ja pūles, ko tie rada, nav nesamērīgas salīdzinājumā ar mērķiem, kuru sasniegšanai tie paredzēti attiecībā uz aizsardzību.

2. Attiecībā uz datu automatizētu apstrādi visas dalībvalstis īsteno pasākumus, kas paredzēti, lai:

   (a) liegtu nepiederošām personām pieeju datu apstrādes iekārtām, kuras izmanto personas datu apstrādei (piekļuves kontrole iekārtām);

   (b) novērstu nesankcionētu to nolasīšanu, kopēšanu, sagrozīšanu vai izņemšanu no datu nesējiem (datu nesēju kontrole);

   (c) liegtu datu nesankcionētu ievadīšanu un noglabāto personas datu pārbaudi, grozīšanu vai dzēšanu (uzglabāšanas kontrole);

   (d) liegtu izmantot datu apstrādes automatizētas sistēmas nepilnvarotām personām, izmantojot datu komunikācijas iekārtas (lietotāju kontrole);

   (e) nodrošinātu, ka personām, kas ir pilnvarotas izmantot datu apstrādes automatizētu sistēmu, ir piekļuve tikai tiem datiem, uz ko attiecas viņu piekļuves tiesības (datu piekļuves kontrole);

   (f) nodrošinātu, ka ir iespējams pārbaudīt un noteikt, kurām organizācijām dati ir vai var tikt nosūtīti vai atklāti, izmantojot datu komunikācijas iekārtas (komunikācijas kontrole);

   (g) nodrošinātu, ka pēc tam ir iespējams pārbaudīt un noteikt, kuri personas dati ir ievadīti datu apstrādes automatizētajās sistēmās, kā arī ievadīšanas laiku un ievadītāju (ievades kontrole);

(h) novērstu personas datu nesankcionētu nolasīšanu, kopēšanu, grozīšanu vai dzēšanu personas datu nosūtīšanas laikā vai datu nesēja transportēšanas laikā (transportēšanas kontrole);

(i) nodrošinātu, ka pārtraukuma gadījumā uzstādītās sistēmas var tūlīt atjaunot (atgūšana);

(j) nodrošinātu, ka sistēma funkcionē bez kļūdām, ka par kļūdu parādīšanos darbībās tūlīt ziņo (drošums) un noglabātos datus nevar bojāt sistēmas darbības traucējumu dēļ (integritāte).

3. Dalībvalstis nosaka, ka personas datu apstrādātājam, ja apstrādi veic viņa interesēs, jāizvēlas apstrādātājs, sniedzot pietiekamas garantijas attiecībā uz tehniskās drošības pasākumiem un organizatoriskiem pasākumiem, kas reglamentē veicamo apstrādi, un jānodrošina šo pasākumu izpilde.

4. Apstrāde, kuru veic apstrādātājs, jāreglamentē ar nolīgumu vai tiesību aktu, kurš pakļauj apstrādātāju personas datu apstrādātājam, un jo īpaši paredz, ka:

– apstrādātājs darbojas vienīgi saskaņā ar personas datu apstrādātāja norādījumiem,

– pienākumi, kas izklāstīti 1. un 2. punktā, kā to nosaka tās dalībvalsts, kurā apstrādātājs ir izveidots, tiesību akti, ir saistoši arī apstrādātājam.

5. Lai sniegtu apliecinājumu, nolīguma vai tiesību akta daļām attiecībā uz datu aizsardzību un prasībām, kas attiecas uz 1. punktā minētajiem pasākumiem, jābūt izklāstītām rakstveidā vai kādā citā pielīdzināmā formā.

25. pants
Reģistrs

1. Dalībvalstis nosaka, ka katrs datu apstrādātājs reģistrē datus par jebkādām apstrādes darbībām vai minēto darbību kopumu, kuras paredzētas vienam nolūkam vai vairākiem saistītiem nolūkiem. Reģistrā iekļaujama šāda informācija

(a) personas datu apstrādātāja un viņa pārstāvja, ja tāds ir, nosaukums un adrese;

(b) datu apstrādes nolūks vai nolūki;

(c) datu subjekta kategorijas vai kategoriju apraksts un uz tām attiecināmo datu vai datu kategoriju apraksts;

(d) apstrādes, kurai dati paredzēti, juridiskais pamats;

(e) saņēmēji vai saņēmēju kategorijas, kam datus varētu atklāt;

(f) priekšlikumus par datu pārsūtīšanu trešām valstīm;

(g) vispārējs apraksts, kas ļauj iepriekš novērtēt saskaņā ar 24. pantu veikto pasākumu atbilstību datu apstrādes drošības nodrošināšanai.

2. Dalībvalstis precizē nosacījumus un kārtību, kādā 1. punktā minētā informācija jāpaziņo uzraudzības iestādei.

26. pants
Iepriekšēja pārbaude

1. Dalībvalstis nosaka datu apstrādes darbības, kuras iespējami var radīt zināmu risku datu subjektu tiesībām un brīvībām, un kontrolē, lai šīs apstrādes darbības pirms to uzsākšanas tiktu pārbaudītas.

2. Minētās iepriekšējās pārbaudes pēc paziņojuma saņemšanas no personas datu apstrādātāja veic uzraudzības iestāde vai datu aizsardzības amatpersona, kurai šaubu gadījumā jākonsultējas ar uzraudzības iestādi.

3. Dalībvalstis arī var veikt šādas pārbaudes valsts parlamenta pasākuma vai pasākuma, kas balstās uz tādu tiesību aktu, kurš nosaka apstrādes raksturu un paredz atbilstošas garantijas, sagatavošanas kontekstā.

VI NODAĻA
TIESISKĀS AIZSARDZĪBAS LĪDZEKĻI UN ATBILDĪBA

27. pants
Aizsardzības līdzekļi

Neierobežojot nevienu administratīva rakstura līdzekli, kuru var, *inter alia*, noteikt 30. pantā minētajai uzraudzības iestādei pirms vēršanās tiesas iestādē, dalībvalstis nodrošina katras personas tiesības uz tiesiskas aizsardzības līdzekli par jebkuru tiesību, ko šai personai atbilstoši šim pamatlēmumam garantē minētajai datu apstrādei piemērojamais valsts likums, pārkāpumu.

28. pants
Atbildība

1. Dalībvalstis nosaka, ka jebkurai personai, kam nodarīts kaitējums sakarā ar datu nelikumīgu apstrādi vai jebkādas rīcības dēļ, kas nav savienojama ar valsts noteikumiem, kas pieņemti saskaņā ar šo pamatlēmumu, ir tiesības saņemt no personas datu apstrādātāja kompensāciju par nodarīto kaitējumu. Personas datu apstrādātāju var pilnībā vai daļēji atbrīvot no šīs atbildības, ja tas pierāda, ka nav atbildīgs par notikumu, kurš izraisījis kaitējumu.

2. Tomēr kompetentā iestāde, kas ir saņēmusi personas datus no citas dalībvalsts kompetentās iestādes, ir atbildīga par kaitējumu, kas radies cietušajai personai neprecīzu vai novecojušu datu izmantošanas dēļ. Tā nevar atteikties no šīs atbildības, pamatojoties uz to, ka tā ir saņēmusi neprecīzus vai novecojušus datus no citas iestādes. Ja nosaka atlīdzību par kaitējumu, ko piespriež saņēmējai iestādei tāpēc, ka tā ir izmantojusi neprecīzus datus, kurus tai pārsūtījusi vai atklājusi citas dalībvalsts kompetentā iestāde, minētā iestāde pilnībā atlīdzina saņēmējai iestādei summu, kas izmaksāta par kaitējumu.

29. pants
Sankcijas

1. Dalībvalstis pieņem atbilstošus pasākumus, lai nodrošinātu šā pamatlēmuma noteikumu ieviešanu pilnībā, un jo īpaši nosaka efektīvas, samērīgas un preventīvas

sankcijas, kuras jāuzliek gadījumā, ja tiek pārkāpti saskaņā ar šo pamatlēmumu pieņemtie noteikumi.

2. Dalībvalstis nosaka efektīvas, samērīgas un preventīvas krimināl sankcijas par tīši izdarītiem nodarījumiem, kas saistīti ar nopietniem nosacījumu, kas pieņemti atbilstoši šim pamatlēmumam, pārkāpumiem, īpaši to nosacījumu, kas vērsti uz apstrādes konfidencialitātes un drošības nodrošināšanu.

VII NODAĻA
UZRAUDZĪBAS IESTĀDE UN DARBA GRUPA PERSONU AIZSARDZĪBAI ATTIECĪBĀ UZ PERSONAS DATU APSTRĀDI

30. pants
Uzraudzības iestāde

1. Visas dalībvalstis nosaka, ka viena vai vairākas valsts iestādes ir atbildīgas par noteikumu, ko dalībvalstis pieņēmušas saskaņā ar šo pamatlēmumu, piemērošanas kontroli tās teritorijā. Šīs iestādes tām uzticēto pienākumu izpildē darbojas pilnīgi neatkarīgi.

2. Visas dalībvalstis nosaka, ka, izstrādājot administratīva rakstura pasākumus vai noteikumus attiecībā uz personas tiesību un brīvību aizsardzību saistībā ar personas datu apstrādi noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un krimināl vajāšanas mērķiem, apspriežas ar uzraudzības iestādēm.

3. Katrai iestādei ir piešķirtas:

   – izmeklēšanas pilnvaras, piemēram, pilnvaras piekļūt datiem, kuri veido apstrādes darbību priekšmetu, un pilnvaras ievākt visu informāciju, kas ir vajadzīga tās uzraudzības pienākumu izpildei;

   – efektīvas iejaukšanās pilnvaras, piemēram, pilnvaras sniegt atzinumus pirms datu apstrādes darbību veikšanas atbilstoši 26. pantam un pilnvaras nodrošināt minēto atzinumu atbilstīgu nodošanu atklātībai, pilnvaras likt noslēgt piekļuvi datiem, dzēst vai iznīcināt datus, noteikt pagaidu vai galīgu aizliegumu datu apstrādei, brīdināt vai izteikt aizrādījumu personas datu apstrādātājam vai pilnvaras nodot jautājumu izskatīšanai valstu parlamentiem vai citām politiskām institūcijām;

   – pilnvaras uzsākt procesuālas darbības, ja pārkāpti valstu noteikumi, kas pieņemti saskaņā ar šo pamatlēmumu, vai darīt zināmus šos pārkāpumus tiesu iestādēm.

   Uzraudzības iestādes lēmumus, kuri dod tiesības uz sūdzību procedūru, var pārsūdzēt tiesā.

4. Visas uzraudzības iestādes uzklausa jebkuras personas iesniegtu prasību, kas saistīta ar šīs personas tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi. Ieinteresēto personu informē par prasības rezultātu.

5. Visas uzraudzības iestādes regulāros starplaikos sagatavo ziņojumu par savu darbību. Ziņojumu publisko.

6. Visas uzraudzības iestādes neatkarīgi no tā, kādas valsts tiesības tiktu piemērotas konkrētajai datu apstrādei, ir kompetentas savas dalībvalsts teritorijā pašas realizēt

tām saskaņā ar 3. punktu piešķirtās pilnvaras. Citas dalībvalsts iestāde var lūgt visām uzraudzības iestādēm realizēt to pilnvaras.

7. Uzraudzības iestādes sadarbojas cita ar citu, kā arī ar uzraudzības organizācijām, kuras izveidotas atbilstoši VI sadaļai Līgumā par Eiropas Savienību, un ar Eiropas datu aizsardzības uzraudzītāju, ciktāl tas nepieciešams to pienākumu izpildei, jo īpaši, apmainoties ar visu lietderīgo informāciju.

8. Dalībvalstis nosaka, ka uz uzraudzības iestādes locekļiem un personālu pat pēc viņu nodarbinātības izbeigšanās attiecas profesionālā noslēpuma pienākums attiecībā uz konfidenciālo informāciju, kura viņiem ir pieejama.

9. Uzraudzības iestādes pilnvaras neierobežo tiesu varas neatkarību, un lēmums, kuru pieņem šī iestāde, neierobežo tiesu iestādes likumīgo uzdevumu izpildi kriminālprocesā.

31. pants

Darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem

1. Ar šo tiek izveidota darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem, še turpmāk „darba grupa”. Tai ir padomdevējas statuss, un tā darbojas neatkarīgi.

2. Darba grupā ietilpst uzraudzības iestādes vai iestāžu, kuras norīkojusi katra dalībvalsts, pārstāvis, Eiropas datu aizsardzības uzraudzītāja pārstāvis un Komisijas pārstāvis.

   Katru darba grupas locekli norīko viņa pārstāvētā institūcija, iestāde vai iestādes. Ja dalībvalsts ir izraudzījusies vairāk nekā vienu uzraudzības iestādi, tās izvirza kopēju pārstāvi.

   Kopējo uzraudzības iestāžu, kas izveidotas atbilstoši VI sadaļai Līgumā par Eiropas Savienību, priekšsēdētājiem ir tiesības piedalīties vai būt pārstāvētiem darba grupas sanāksmēs. Uzraudzības iestādei vai iestādēm, kuras norīko Islande, Norvēģija un Šveice, ir tiesības būt pārstāvētām darba grupas sanāksmēs, ciktāl tās attiecas uz Šengenas *acquis* jautājumiem.

3. Darba grupa pieņem lēmumus ar dalībvalstu uzraudzības iestāžu pārstāvju vienkāršu balsu vairākumu.

4. Darba grupa ievēl tās priekšsēdētāju. Priekšsēdētāja amata pilnvaru laiks ir divi gadi. Viņu var ievēlēt atkārtoti.

5. Darba grupas sekretariātu nodrošina Komisija.

6. Darba grupa pieņem savu reglamentu.

7. Darba grupa izskata jautājumus, kurus tās darba kārtībai nosaka priekšsēdētājs vai nu pēc savas iniciatīvas, vai pēc uzraudzības iestāžu pārstāvja, Komisijas, Eiropas datu aizsardzības uzraudzītāja vai kopīgo uzraudzības iestāžu priekšsēdētāju pieprasījuma.

32. pants

Uzdevumi

1. Darba grupa

(a) izskata jebkuru jautājumu, kas attiecas uz valsts pasākumu, kuri pieņemti saskaņā ar šo pamatlēmumu, piemērošanu, lai veicinātu šādu pasākumu vienādu piemērošanu;

(b) sniedz atzinumu par aizsardzības līmeni dalībvalstīs un trešās valstīs un starptautiskās organizācijās jo īpaši, lai nodrošinātu, ka trešām valstīm un starptautiskām organizācijām, kuras nodrošina pietiekamu datu aizsardzības līmeni, personu datus pārsūta atbilstoši 15. punktam šajā pamatlēmumā;

(c) sniedz padomus Komisijai un dalībvalstīm par jebkuru ierosinātu šā pamatlēmuma grozījumu, jebkuriem papildu vai īpašiem pasākumiem, lai aizsargātu fizisku personu tiesības un brīvības attiecībā uz personas datu apstrādi noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem, un jebkuriem citiem ierosinātiem pasākumiem, kas ietekmē minētās tiesības un brīvības.

2. Ja darba grupa konstatē, ka starp dalībvalstu likumiem vai praksi rodas atšķirības, kuras var ietekmēt personu līdzvērtīgu aizsardzību attiecībā uz personas datu apstrādi Eiropas Savienībā, tā informē Padomi un Komisiju.

3. Darba grupa pēc savas iniciatīvas vai pēc Komisijas vai Padomes iniciatīvas var sniegt ieteikumus par visiem jautājumiem, kas saistīti ar personu aizsardzību attiecībā uz personas datu apstrādi Eiropas Savienībā noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem.

4. Darba grupas atzinumus un ieteikumus nosūta Padomei, Komisijai un Eiropas Parlamentam, un 16. pantā minētajai komitejai.

5. Pamatojoties uz dalībvalstu sniegto informāciju, Komisija informē darba grupu par darbību, ko tā uzsākusi, atbildot uz šīs grupas atzinumiem un ieteikumiem. Komisija to dara ar ziņojumu, kuru nosūta arī Eiropas Parlamentam un Padomei. Ziņojumu dara zināmu atklātībai. Dalībvalstis informē darba grupu par jebkuru darbību, ko tās uzsāk atbilstoši 1. punktam.

6. Darba grupa izstrādā gada ziņojumu par situāciju attiecībā uz fizisku personu aizsardzību saistībā ar personas datu apstrādi kriminālnoziegumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem Eiropas Savienībā un trešās valstīs, kuru tā nosūta Komisijai, Eiropas Parlamentam un Padomei. Ziņojumu dara zināmu atklātībai.

VIII NODAĻA
Nobeiguma noteikumi

33. pants
Grozījums Šengenas Konvencijā

Jautājumos, uz ko attiecas Līgums par Eiropas Savienību, šis pamatlēmums aizstāj 126. un 130. pantu Šengenas Konvencijā.

34. pants
Saistība ar citiem tiesību aktiem, kas attiecas uz personas datu apstrādi un aizsardzību

1. Šis pamatlēmums aizstāj 23. pantu Konvencijā par Eiropas Savienības dalībvalstu savstarpējo palīdzību kriminālllietās.

2. Ikvienu atsauci uz Eiropas Padomes 1981. gada 28. janvāra Konvenciju Personu aizsardzībai attiecībā uz personisko datu automātisko apstrādi (Nr. 108) uzskata par atsauci uz šo pamatlēmumu.

35. pants
Īstenošana

1. Dalībvalstis veic vajadzīgos pasākumus, lai līdz 2006. gada 31. decembrim panāktu atbilstību šim pamatlēmumam.

2. Līdz tai pašai dienai dalībvalstis nosūta Padomes Ģenerālsekretariātam un Komisijai to nosacījumu tekstu, ar kuriem saistības, kuras tām uzliek šis pamatlēmums, transponē valstu tiesību aktos, kā arī informāciju par 29. pantā minētās uzraudzības iestādes vai iestāžu norīkošanu. Pamatojoties uz šo informāciju un uz Komisijas rakstisku ziņojumu, Padome līdz 2007. gada 31. decembrim novērtē, kā dalībvalstis ir veikušas pasākumus, kas vajadzīgi, lai panāktu atbilstību šim pamatlēmumam.

36. pants
Stāšanās spēkā

Šīs lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē,

Padomes vārdā —
priekšsēdētājs

PIELIKUMS

TIESĪBU AKTA FINANŠU PĀRSKATS

Politikas joma(-as): Tieslietas un iekšlietas

Darbība(-as): 1806 – Patiesas brīvības, drošības un tiesiskuma telpas kriminālllietās un civillietās izveidošana

PASĀKUMA NOSAUKUMS: PRIEKŠLIKUMS PADOMES PAMATLĒMUMAM PAR PERSONAS DATU, KO APSTRĀDĀ, SADARBOJOTIES POLICIJAS UN TIESU IESTĀDĒM, AIZSARDZĪBU

1. BUDŽETA POZĪCIJA(-S):

Nepiemēro

2. KOPĒJIE RĀDĪTĀJI

2.1. Kopējais piešķīrums pasākumam (B daļa): miljonos euro saistību izpildei

Nepiemēro

2.2. Piemērošanas periods:

sākot ar 2006. gadu

2.3. Kopējā daudzgadu izdevumu tāme

(a) Saistību apropriāciju/maksājumu apropriāciju (finanšu intervences) plāns *(skatīt 6.1.1. punktu)*

miljonos euro *(līdz 3 zīmēm aiz komata)*

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Kopā
Saistības							
Maksājumi							

(b) Tehniskās un administratīvās palīdzības un atbalsta izdevumi *(skatīt 6.1.2. punktu)*

Saistības							
Maksājumi							

Starpsumma a+b							
Saistības							
Maksājumi							

(c) Cilvēkresursu un citu administratīvo izmaksu kopējā finansiālā ietekme*(skatīt 7.2. un 7.3. punktu)*

Saistības/maksājumi	0,389	0,389	0,389	0,389	0,389	0,389	2,334

KOPĀ a+b+c							
Saistības							
Maksājumi							

2.4. Atbilstība finanšu programmas izstrādei un finanšu perspektīvai

Nepiemēro

2.5. Finansiālā ietekme uz ieņēmumiem:

Priekšlikumam nav finansiālu seku

3. BUDŽETA RĀDĪTĀJI

Izdevumu veids		Jauns	EBTA iemaksa	Kandidātvalstu iemaksas	Pozīcija finanšu perspektīvā
Neoblig.	Nedif.	Nepiemēro	Nepiemēro	Nepiemēro	Nr. Nepiemēro

4. JURIDISKAIS PAMATS

LES 30. pants, 31. pants un 34. panta 2. punkta b) apakšpunkts

5. APRAKSTS UN PAMATOJUMS

5.1. Kopienas intervences nepieciešamība

5.1.1. Izvirzītie mērķi

Ierosinātais pamatlēmums nosaka kopējus standartus attiecībā uz personas datu, ko apstrādā kompetentas iestādes VI sadaļā Līgumā par Eiropas Savienību (policijas un tiesu iestāžu sadarbība krimināllietās) minēto darbību kontekstā, aizsardzību. Neatkarīgas uzraudzības iestādes uzrauga valstu noteikumu piemērošanu dalībvalstīs atbilstoši šim pamatlēmumam. ES līmenī tiek izveidota darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem, še turpmāk „darba grupa". Darba grupā ietilpst uzraudzības iestādes vai iestāžu, kuras norīkojusi katra dalībvalsts, pārstāvis, Eiropas datu aizsardzības uzraudzītāja pārstāvis un Komisijas pārstāvis. Darba grupa izskata jebkuru jautājumu, kas attiecas uz valsts pasākumu piemērošanu, kuri pieņemti saskaņā ar šo pamatlēmumu, lai veicinātu minēto pasākumu vienādu piemērošanu. Tā sniedz atzinumus par datu aizsardzības līmeni dalībvalstīs un trešās valstīs un konsultē Komisiju un dalībvalstis par jebkuriem ierosinātiem šā pamatlēmuma grozījumiem, kā arī par jebkuriem papildu vai īpašiem pasākumiem pamattiesību aizsardzībai.

Turklāt atbilstoši 16. pantam pamatlēmumā komiteja, kas sastāv no dalībvalstu pārstāvjiem un kuras priekšsēdētājs ir Komisijas pārstāvis, kur tas ir nepieciešams, palīdz Komisijai novērtēt datu aizsardzības līmeni trešā valstī.

5.1.2. Pasākumi, kas veikti saistībā ar ex ante vērtēšanu

Notika apspriešanās ar dalībvalstu, kā arī ar Islandes, Norvēģijas un Šveices valdību un neatkarīgo uzraudzības iestāžu, Datu aizsardzības uzraudzītāja, Eiropola un Eurojust pārstāvjiem. Jo īpaši, ņemot vērā atšķirīgos viedokļus, Komisija ierosina izveidot iepriekš minēto darba grupu. Lai aprēķinātu iespējamās izmaksas, ko radītu šis pasākums, Komisija pārbaudīja izmaksas (komandējumu izmaksas, sekretariāta atbalsts sanāksmju sagatavošanai un organizēšanai), kuras pašlaik ir darba grupai, kas izveidota atbilstoši 29. pantam Direktīvā 95/46/EK.

5.2. Paredzētā rīcība un budžeta intervences pasākumi

Iepriekš minētā darba grupa, iespējams, rīkos regulāras sanāksmes, kas paredzētas piecas reizes gadā. Komiteja, kas minēta 16. pantā, vajadzības gadījumā sanāks kopā tik bieži, cik nepieciešams, iespējams, arī piecas reizes gadā. Izdevumi būs jāatlīdzina par vienu dalībnieku no katras dalībvalsts un no katras Šengenas valsts (Islande, Norvēģija). Daļēju orientāciju var saņemt no grupām, kas izveidotas saskaņā ar 29. un 31. pantu Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvā par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

5.3. Īstenošanas metodes

Visas sapulces jāorganizē un jāvada Komisijai. Komisijai jānodrošina sekretāru pakalpojumi iepriekš minētajai darba grupai un komitejai un jāsagatavo/jāorganizē to sanāksmes.

6. FINANSIĀLĀ IETEKME

6.1. Kopējā finansiālā ietekme uz B daļu - (visā plānošanas periodā)

6.1.1. Finanšu intervence

Nepiemēro

6.1.2. Tehniskās un administratīvās palīdzības un atbalsta izdevumi un IT izdevumi (saistību apropriācijas)

Nepiemēro

6.2. Izmaksu aprēķins B daļā paredzētajam pasākumam (visā plānošanas periodā)

Nepiemēro

7. IETEKME UZ PERSONĀLA UN ADMINISTRATĪVAJIEM IZDEVUMIEM

Ietekmi uz personāla un administratīvajiem izdevumiem segs vadošā ģenerāldirektorāta līdzekļu piešķiršanas kontekstā ikgadējo resursu sadalījuma procedūras kontekstā.

Amatu sadalījums ir atkarīgs arī no funkciju un resursu sadalījuma 2007.-2013. gada finanšu perspektīvu kontekstā.

7.1. Ietekme uz cilvēkresursiem

Amatu veidi	Darbinieki, kas norīkojami pasākuma vadībā, izmantojot pašreizējos un/vai papildu resursus	Kopā	Uzdevumu, kas izriet no pasākuma, apraksts

		Pastāvīgo amatu skaits	Pagaidu amatu skaits		
Ierēdņi vai pagaidu darbinieki	A B C	0,25 A 0,50 B 1,00 C		0,25A 0,50B 1,00C	Sniedz sekretariāta atbalstu, sagatavo darba grupas un komitejas sanāksmes
Citi cilvēkresursi					
Kopā					

7.2. Cilvēkresursu kopējā finansiālā ietekme

Cilvēkresursu veids	Summa (EUR)	Aprēķina metode *
Ierēdņi Pagaidu darbinieki	1. gads: 189 000	1 X 108 000 0,5 X 108 000 0,25 X 108 000 = 189 000
Citi cilvēkresursi (norādīt budžeta pozīciju)		
Kopā	189 000	

Summā iekļauti kopējie izdevumi divpadsmit mēnešu laikā.

7.3. Citi administratīvie izdevumi, kas saistīti ar pasākumu

Budžeta pozīcija (numurs un pozīcija)	Summa (EUR)	Aprēķina metode
Kopējais piešķīrums (sadaļa A7) A0701 – Komandējumi A07030 – Sanāksmes A07031 – Obligātās komitejas A07032 – Komitejas, kas nav obligātas A07040 – Konferences A0705 – Pētījumi un konsultācijas Citi izdevumi (precizēt)	200 000	10 sanāksmes* 27 * 740 euro
Informācijas sistēmas (A-5001/A-4300)		
Citi izdevumi - A daļa (precizēt)		
Kopā	200 000	

Summā iekļauti kopējie izdevumi divpadsmit mēnešu laikā.
Norādīt komitejas veidu un grupu, kurai tā pieder.

I	Kopsumma gadā (7.2. + 7.3.)	EUR 389 000
II	Pasākuma ilgums	
III	Pasākuma kopējās izmaksas (I x II)	

8. IZPILDES UZRAUDZĪBA UN VĒRTĒJUMS

8.1. Izpildes uzraudzība

Darba grupa un komiteja noteiks reglamentu, tostarp konfidencialitātes noteikumus. Eiropas Parlamentu informēs līdzīgi kā norādīts 7. pantā Padomes Lēmumā 99/468/EK (1999. gada 28. jūnijs), ar ko nosaka Komisijai piešķirto ieviešanas pilnvaru īstenošanas kārtību (OV L 184, 17.7.1999., 23. lpp.).

8.2. Plānotā novērtējuma pasākumi un norise

Nepiemēro

9. PASĀKUMI PRET KRĀPŠANU

Nepiemēro

XXX