

III

(Tiesību akti, kas pieņemti, piemērojot Līgumu par Eiropas Savienību)

TIESĪBU AKTI, KAS PIEŅEMTI, PIEMĒROJOT LES VI SADAĻU

PADOMES PAMATLĒMUMS 2008/977/TI

(2008. gada 27. novembris)

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

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,

ņemot vērā Eiropas Parlamenta atzinumu ⁽¹⁾,

tā kā:

(1) Eiropas Savienība ir izvirzījusi mērķi uzturēt un attīstīt Eiropas Savienību kā brīvības, drošības un tiesiskuma telpu, kurā dalībvalstu kopīgai rīcībai ir jānodrošina augsta līmeņa drošība, policijas un tiesu iestādēm sadarbojoties krimināllietās.

(2) Kopīga rīcība policijas sadarbības jomā atbilstīgi 30. panta 1. punkta b) apakšpunktam Līgumā par Eiropas Savienību un kopīga rīcība tiesu iestāžu sadarbībā krimināllietās saskaņā ar 31. panta 1. punkta a) apakšpunktu Līgumā par Eiropas Savienību norāda uz vajadzību pēc tādas informācijas apstrādes, uz kuru būtu jāattiecinā atbilstīgi personas datu aizsardzības noteikumi.

(3) Tiesību aktiem, kas attiecas uz VI sadaļu Līgumā par Eiropas Savienību, būtu 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. Abu minēto mērķu sasniegšanu var sekmēt vienoti standarti tādu personas datu apstrādei un aizsardzībai, ko apstrādā, lai novērstu un apkarotu noziedzību.

(4) Hāgas programmā brīvības, drošības un tiesiskuma stiprināšanai Eiropas Savienībā, kuru Eiropadome pieņēma 2004. gada 4. novembrī, ir uzsvērtā vajadzība pēc novatoriskas pieejas tiesībaizsardzības informācijas pārrobežu apmaiņai, stingri ievērojot galvenos nosacījumus datu aizsardzības jomā, un Eiropadome 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 ⁽²⁾.

(5) Apmaiņa ar personas datiem, policijai un tiesu iestādēm sadarbojoties krimināllietās, būtu jāatbalsta ar skaidriem noteikumiem, veicinot kompetento iestāžu savstarpējo uzticēšanos un attiecīgas informācijas aizsardzību, īpaši saskaņā ar informācijas pieejamības principu, kā paredzēts Hāgas programmā, tā, lai nepieļautu nekādu dalībvalstu sadarbības diskrimināciju, pilnībā ievērojot fizisku personu pamattiesības. Pašlaik Eiropas līmenī spēkā esošie tiesību akti nav pietiekami. Eiropas Parlamenta un Padomes Direktīvu 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti ⁽³⁾ nepiemēro personas datu apstrādes darbībām jomās, uz ko neattiecas Kopienas tiesību akti, piemēram, tiesību akti, kuri paredzēti VI sadaļā Līgumā par Eiropas Savienību, un jebkurā gadījumā – apstrādes darbībām, ko veic sakarā ar sabiedrības drošību, aizsardzību, valsts drošību un valsts darbībām krimināltiesību jomā.

⁽¹⁾ OV C 125 E, 22.5.2008., 154. lpp.

⁽²⁾ OV C 198, 12.8.2005., 1. lpp.

⁽³⁾ OV L 281, 23.11.1995., 31. lpp.

- (6) Šis pamatlēmums būtu jāpieņem tikai tiem datiem, ko kompetentas iestādes iegūst vai apstrādā saistībā ar noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu par tiem vai saistībā ar kriminālsodu izpildi. Šim pamatlēmumam būtu jāparedz, ka dalībvalstis valsts līmenī precīzāk nosaka, kādus citus mērķus uzskata par nesaderīgiem ar mērķi, attiecībā uz kuru dati sākotnēji ir iegūti. Parasti turpmāka apstrāde statistikas mērķiem vai vēsturiskas vai zinātniskas pētniecības mērķiem nebūtu jāuzskata par nesaderīgu ar apstrādes sākotnējo mērķi.
- (7) Šā pamatlēmuma darbības joma būtu jāattiecinā tikai uz tādu personas datu apstrādi, kurus pārsūta starp dalībvalstīm vai kurus dara savstarpēji pieejamus. No šā ierobežojuma nebūtu jāizdara nekādi secinājumi par Savienības kompetenci pieņemt tiesību aktus attiecībā uz personas datu vākšanu un apstrādi valsts līmenī vai par šādas Savienības darbības lietderību nākotnē.
- (8) Lai atvieglotu datu apmaiņu Savienībā, dalībvalstu nolūks ir nodrošināt, ka datu aizsardzības standarti, kas sasniegti datu apstrādē valstī, atbilst šajā pamatlēmumā noteiktajiem standartiem. Attiecībā uz valsts datu apstrādi šis pamatlēmums neliedz dalībvalstīm personas datu aizsardzībai noteikt stingrākus drošības pasākumus par šajā pamatlēmumā paredzētajiem.
- (9) Šis pamatlēmums nebūtu jāpieņem personas datiem, kurus dalībvalsts ir saņēmusi šā pamatlēmuma piemērošanas jomā un kuru izcelsme ir šajā dalībvalstī.
- (10) Dalībvalstu tiesību aktu tuvināšanai nekādā ziņā nebūtu jāmazina attiecīgo dalībvalstu nodrošināto datu aizsardzība, bet gan tieši pretēji – tai būtu jācenšas Savienībā nodrošināt augsta līmeņa aizsardzību.
- (11) Ir jāprecizē datu aizsardzības mērķi policijas un tiesu iestāžu darbībā un jāizstrādā noteikumi par personas datu apstrādi, lai nodrošinātu, ka jebkuru informāciju, ar ko varētu apmainīties, apstrādā likumīgi un atbilstīgi pamatprincipiem, kas attiecas uz datu kvalitāti. Tajā pašā laikā nekādi nebūtu jāapdraud policijas, muitas, tiesu iestāžu un citu kompetentu iestāžu likumīgās darbības.
- (12) Datu precizitātes princips jāpieņem, ņemot vērā attiecīgās apstrādes būtību un mērķi. Piemēram, jo īpaši tiesu procesā datu pamatā ir atsevišķu personu subjektīva uztvere, un dažos gadījumos tos nekādi nav iespējams pārbaudīt. Attiecīgi prasība par precizitāti nevar attiekties uz paziņojuma precizitāti, bet vienīgi uz to, ka ir izdarīts konkrēts paziņojums.
- (13) Arhivēšana atsevišķā datu kopumā būtu pieļaujama tikai tad, ja dati vairs nav vajadzīgi un tos neizmanto noziedzīgu nodarījumu novēršanai, izmeklēšanai, atklāšanai un sodīšanai. Arhivēšana atsevišķā datu kopumā būtu pieļaujama arī, ja arhivētos datus glabā datubāzē ar citiem datiem tā, ka tos vairs nevar izmantot noziedzīgu nodarījumu novēršanai, izmeklēšanai, atklāšanai, kriminālvajāšanai par tiem vai kriminālsodu izpildīšanai. Arhivēšanas termiņu piemērotībai vajadzētu būt atkarīgai no arhivēšanas mērķa un datu subjekta likumīgajām interesēm. Ja arhivēšana notiek vēsturiskiem mērķiem, var paredzēt ļoti ilgu termiņu.
- (14) Datus var dzēst arī, iznīcinot datu nesējus.
- (15) Attiecībā uz neprecīziem, nepilniem vai vairs neatjauninātiem datiem, kas pārsūtīti vai darīti pieejami citai dalībvalstij un ko turpmāk apstrādā iestādes, kuras līdzinās tiesu iestādēm, proti, iestādes, kurām ir pilnvaras pieņemt juridiski saistošus lēmumus, tie būtu jālabo, jādzēš vai jāliedz piekļuve tiem saskaņā ar valsts tiesību aktiem.
- (16) Lai personām nodrošinātu augsta līmeņa personas datu aizsardzību, ir vajadzīgi kopēji noteikumi, lai noteiktu to datu likumību un kvalitāti, kurus apstrādājušas kompetentas iestādes citās dalībvalstīs.
- (17) Ir lietderīgi Eiropas līmenī paredzēt nosacījumus, saskaņā ar kuriem kompetentām dalībvalstu iestādēm personas datus, kas saņemti no citām dalībvalstīm, būtu atļauts pārsūtīt vai darīt pieejamus iestādēm un privātām personām dalībvalstīs. Daudzos gadījumos, lai veiktu kriminālvajāšanu vai novērstu tūlītējus un nopietnus draudus sabiedrības drošībai un lai novērstu nopietnu kaitējumu personas tiesībām, tiesībaizsardzības iestādēm, policijai vai muitai ir jāpārsūta personas dati privātām personām, piemēram, izdodot brīdinājumus bankām un kredītiestādēm par vērtspapīru viltojumiem, vai transporta noziedzības jomā, pārsūtot personas datus apdrošināšanas sabiedrībām, lai novērstu zagtu mehānisko transportlīdzekļu nelikumīgu tirdzniecību vai lai uzlabotu nosacījumus nozagto mehānisko transportlīdzekļu atgūšanai no ārvalstīm. Tas nenozīmē policijas vai tiesu pilnvaru nodošanu privātām personām.

- (18) Šā pamatlēmuma noteikumus par tiesu iestāžu, policijas vai muitas veiktu personas datu pārsūtīšanu privātām personām neattiecinā uz datu atklāšanu privātām personām (piemēram, advokātiem un upuriem) saistībā ar kriminālprocesiem.
- (19) To personas datu turpmākai apstrādei, kurus saņem no kompetentām citu dalībvalstu iestādēm vai kurus tās atklājušas, jo īpaši minēto datu tālākai pārsūtīšanai vai lai darītu tos pieejamus, būtu jāpiemēro kopīgi noteikumi Eiropas līmenī.
- (20) Ja personas datus turpmāk apstrādā pēc tam, kad saņemta piekrišana no dalībvalsts, no kuras dati tika saņemti, katrai dalībvalstij vajadzētu spēt noteikt kārtību šādas piekrišanas sniegšanai, tostarp, piemēram, vispārējas piekrišanas veidā attiecībā uz informācijas kategorijām vai turpmākas apstrādes kategorijām.
- (21) Ja personas datus var turpmāk apstrādāt saistībā ar administratīvām procedūrām, šīs procedūras ietver darbības, ko veic regulējošas vai uzraudzības struktūras.
- (22) Saistībā ar policijas, muitas, tiesas un citu kompetentu iestāžu likumīgām darbībām varētu rasties nepieciešamība nosūtīt datus iestādēm trešās valstīs vai starptautiskām struktūrām, kurām ir pienākums novērst, izmeklēt vai atklāt noziedzīgus nodarījumus vai veikt kriminālvajāšanu par tiem, vai izpildīt kriminālsodus.
- (23) Ja personas datus no dalībvalsts nosūta trešām valstīm vai starptautiskām struktūrām, datiem būtu jānodrošina līdzvērtīgs aizsardzības līmenis.
- (24) Ja personas datus no dalībvalsts nosūta trešām valstīm vai starptautiskām struktūrām, tad principā šādi pārsūtīšanai būtu jānotiek tikai pēc tam, kad dalībvalsts, no kuras dati tika saņemti, ir piekritusi nosūtīšanai. Katrai dalībvalstij būtu jāspēj noteikt kārtību šādi piekrišanai, tostarp, piemēram, vispārējas piekrišanas veidā attiecībā uz informācijas kategorijām vai attiecībā uz konkrētām trešām valstīm.
- (25) Lai tiesībaizsardzības sadarbība būtu efektīva, gadījumos, ja apdraudējums dalībvalsts vai trešās valsts sabiedrības drošībai ir tiešs un ja nav iespējams savlaicīgi saņemt iepriekšēju piekrišanu, kompetentajai iestādei būtu jāspēj pārsūtīt attiecīgos personas datus attiecīgajai trešai valstij bez šādas iepriekšējas piekrišanas. To pašu varētu piemērot gadījumiem, kad skartas kādas citas būtiskas un vienlīdz nozīmīgas dalībvalsts intereses, piemēram, ja varētu būt tūlītēji un nopietni draudi dalībvalsts būtiskajai infrastruktūrai vai ja varētu tikt radīti nopietni traucējumi dalībvalsts finanšu sistēmai.
- (26) Datu subjekti var būt jāinformē par to datu apstrādi, lai garantētu tiem efektīvas tiesiskās aizsardzības iespējas, jo īpaši tad, kad to tiesības ir būtiski aizskartas, veicot datu slepenu ieguvu.
- (27) Dalībvalstīm būtu jānodrošina, ka datu subjektu informē par to, ka personas datus varētu vākt, apstrādāt vai nosūtīt citai dalībvalstij vai tos vāc, apstrādā un nosūta citai dalībvalstij, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus un veiktu kriminālvajāšanu par tiem vai izpildītu kriminālsodus. Kārtību attiecībā uz datu subjekta tiesībām tikt informētam un par izņēmumiem no tās nosaka valsts tiesību aktos. To var veikt vispārēji, piemēram, ar tiesību aktu, vai publicējot apstrādes darbību sarakstu.
- (28) Lai nodrošinātu personas datu aizsardzību, nekaitējot kriminālizmeklēšanas interesēm, ir jānosaka datu subjekta tiesības.
- (29) Dažas dalībvalstis ir nodrošinājušas datu subjekta piekļuves tiesības krimināllietās, izmantojot sistēmu, saskaņā ar ko valsts uzraudzības iestādei, nevis datu subjektam, bez ierobežojumiem ir pieejami visi personas dati, kas attiecas uz datu subjektu, un tā var arī labot, dzēst vai atjaunināt neprecīzus datus. Šādā netiešas piekļuves gadījumā šo dalībvalstu tiesību aktos var arī noteikt, ka valsts uzraudzības iestādes tikai informēs datu subjektu par to, ka ir veikta vajadzīgā pārskatīšana. Tomēr šīs dalībvalstis arī paredz iespējas datu subjektam tieši piekļūt datiem īpašos gadījumos, piemēram, piekļūt sodāmības reģistram, iegūt pašu sodāmības reģistra datu kopijas vai policijas dienestu veiktu nopratināšanu kopijas.
- (30) Ir lietderīgi izveidot kopējus noteikumus par datu apstrādes konfidencialitāti un drošību, kompetentu iestāžu atbildību un tām piemērojamām sankcijām par datu nelikumīgu izmantošanu, kā arī par datu subjektiem pieejamiem tiesiskās aizsardzības līdzekļiem. Tomēr katras dalībvalsts kompetencē ir noteikt atbildības par pārkāpumiem noteikumu būtību, kā arī sankcijas, ko piemēro valsts datu aizsardzības noteikumu pārkāpumiem.
- (31) Šajā pamatlēmumā ir ļauts ņemt vērā principu par sabiedrības tiesībām piekļūt oficiāliem dokumentiem, īstenojot šajā pamatlēmumā paredzētos principus.

- (32) Ja jāaizsargā personas dati saistībā ar apstrādi, kas apjoma vai veida dēļ rada īpašu risku attiecībā uz datu subjekta pamattiesībām un pamatbrīvībām, piemēram, apstrāde, izmantojot jaunas tehnoloģijas, mehānismus vai procedūras, ir lietderīgi nodrošināt, ka pirms tās kartotēkas sistēmas izveides, kuras mērķis ir šo datu apstrāde, konsultējas ar kompetentajām valsts uzraudzības iestādēm.
- (33) Tādu uzraudzības iestāžu izveide dalībvalstīs, kuras pilda funkcijas pilnīgi neatkarīgi, ir būtiska aizsardzības sastāvdaļa attiecībā uz personas datiem, ko apstrādā, sadarbojoties dalībvalstu policijas un tiesu iestādēm.
- (34) Uzraudzības iestādēm, kas dalībvalstīs jau izveidotas saskaņā ar Direktīvu 95/46/EK, būtu jāspēj veikt arī valsts uzraudzības iestāžu funkcijas, kas jānosaka saskaņā ar šo pamatlēmumu.
- (35) Minēto iestāžu rīcībā vajadzētu būt to pienākumu veikšanai nepieciešamajiem līdzekļiem, tostarp pilnvarām veikt izmeklēšanu un iejaukties, jo īpaši personu sūdzību gadījumos, un pilnvarām iesaistīties tiesvedībā. Šīm uzraudzības iestādēm būtu jāpalīdz nodrošināt datu apstrādes pārskatāmību dalībvalstīs, kuru jurisdikcijā ir attiecīgās iestādes. Tomēr šo iestāžu pilnvarām nevajadzētu būt pretrunā īpašajiem noteikumiem, kas paredzēti kriminālprocesā, un tām nebūtu jāietekmē tiesu neatkarība.
- (36) Līguma par Eiropas Savienību 47. pantā paredzēts, ka neviens no Līguma noteikumiem neierobežo Eiropas Kopienų 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 Direktīvā 95/46/EK, Eiropas Parlamenta un Padomes Regulā (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un organizācijās un par šādu datu brīvu apriti⁽¹⁾ un Eiropas Parlamenta un Padomes Direktīvā 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju)⁽²⁾.
- (37) Šis pamatlēmums neskar noteikumus, kas attiecas uz nelikumīgu piekļuvi datiem, kā paredzēts Padomes Pamatlēmumā 2005/222/TI (2005. gada 24. februāris) par uzbrukumiem informācijas sistēmām⁽³⁾.
- (38) Šis pamatlēmums neskar dalībvalstu vai Savienības spēkā esošās saistības un pienākumus, kas izriet no divpusējiem un/vai daudzpusējiem nolīgumiem ar trešām valstīm. Turpmākos nolīgumos būtu jāievēro noteikumi par datu apmaiņu ar trešām valstīm.
- (39) Vairākos tiesību aktos, kas pieņemti, pamatojoties uz Līguma par Eiropas Savienību VI sadaļu, ir īpaši noteikumi par to personas datu aizsardzību, ar kuriem notiek apmaiņa saskaņā ar šiem tiesību aktiem vai ko citādi apstrādā. Dažos gadījumos šie noteikumi ir pilnīgs un saskaņots noteikumu kopums, kas attiecas uz visiem attiecīgiem datu aizsardzības aspektiem (datu kvalitātes principi, datu drošības noteikumi, datu subjektu tiesību un garantiju reglamentācija, pārraudzības un atbildības organizācija), un tajos šie jautājumi ir reglamentēti sīkāk nekā šajā pamatlēmumā. Šim pamatlēmumam nebūtu jāskar minēto aktu attiecīgo datu aizsardzības noteikumu kopums, jo īpaši tie noteikumi, kuros reglamentē Eiropola, Eurojust, Šengenas Informācijas sistēmas (SIS) un Muitas informācijas sistēmas (CIS) darbību, kā arī tie, kas ievieš dalībvalstu iestāžu tiešu piekļuvi citu dalībvalstu konkrētu datu sistēmām. Tas pats attiecas arī uz datu aizsardzības noteikumiem, kas reglamentē automatizētu DNS profilu, pirkstu nospiedumu datu un valsts transportlīdzekļu reģistrācijas datu pārsūtīšanu starp dalībvalstīm saskaņā ar Padomes Lēmumu 2008/615/TI (2008. gada 23. jūnijs) par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu un pārrobežu noziedzību⁽⁴⁾.
- (40) Citos gadījumos aktu, kas pieņemti, pamatojoties uz Līguma par Eiropas Savienību VI sadaļu, datu aizsardzības noteikumu darbības joma ir ierobežotāka. Bieži tajos dalībvalstīm, kas no citām dalībvalstīm saņem informāciju, kurā ir personas dati, ir paredzēti īpaši nosacījumi par nolūkiem, kuros datus var izmantot, bet uz citiem datu aizsardzības aspektiem attiecina Eiropas Padomes 1981. gada 28. janvāra Konvenciju par personu aizsardzību attiecībā uz personas datu automatizētu apstrādi vai valsts tiesību aktus. Ja minēto aktu noteikumi, kuros paredzēti nosacījumi saņēmējām dalībvalstīm par personas datu izmantošanu vai turpmāku pārsūtīšanu, ir stingrāki nekā tie, kas ietverti attiecīgos šā pamatlēmuma noteikumos, pirmajiem minētajiem noteikumiem būtu jāpaliek spēkā. Tomēr visiem citiem aspektiem būtu jāpieņem šajā pamatlēmumā paredzētie noteikumi.
- (41) Šis pamatlēmums neskar Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automatizētu apstrādi, minētās konvencijas 2001. gada 8. novembra papildprotokolu vai Eiropas Padomes konvencijas par tiesu iestāžu sadarbību krimināllietās.

⁽¹⁾ OV L 8, 12.1.2001., 1. lpp.

⁽²⁾ OV L 201, 31.7.2002., 37. lpp.

⁽³⁾ OV L 69, 16.3.2005., 67. lpp.

⁽⁴⁾ OV L 210, 6.8.2008., 1. lpp.

(42) Ņemot vērā to, ka šā pamatlēmuma mērķi – proti, paredzēt kopējus noteikumus attiecībā uz to personas datu aizsardzību, kurus apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās, – nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, un to, ka minētās rīcības mēroga un iedarbības dēļ minēto mērķi var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma 5. pantā noteikto subsidiaritātes principu un atsaucoties uz 2. pantu Līgumā par Eiropas Savienību. Saskaņā ar Eiropas Kopienas dibināšanas līguma 5. pantā noteikto proporcionalitātes principu šajā pamatlēmumā paredz vienīgi tos pasākumus, kas ir vajadzīgi šā mērķa sasniegšanai.

(43) 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 ⁽¹⁾.

(44) Īrija piedalās šajā lēmumā saskaņā ar 5. pantu Protokolā par Šengenas *acquis* iekļaušanu Eiropas Savienības sistēmā, 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 ⁽²⁾.

(45) Attiecībā uz Islandi un Norvēģiju šis lēmums papildina Šengenas *acquis* nosacījumus, kā tas paredzēts nolīgumā, ko noslēgusi Eiropas Savienības Padome, Islandes Republika un Norvēģijas Karaliste par šo valstu iesaistīšanos Šengenas *acquis* īstenošanā, piemērošanā un izstrādē ⁽³⁾, un tas pieder pie jomas, kas minēta 1. panta H un I punktā Padomes Lēmumā 1999/437/EK ⁽⁴⁾ par dažiem pasākumiem, lai piemērotu minēto nolīgumu.

(46) Attiecībā uz Šveici šis pamatlēmums papildina 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 ⁽⁵⁾, un tas pieder pie jomas, kas minēta 1. panta H un I

punktā Lēmumā 1999/437/EK par dažiem pasākumiem, lai piemērotu minēto nolīgumu, un kas lasāma saistībā ar 3. pantu Padomes Lēmumā 2008/149/TI ⁽⁶⁾ par minētā nolīguma noslēgšanu Eiropas Savienības vārdā.

(47) Attiecībā uz Lihtenšteinu šis pamatlēmums papildina Šengenas *acquis* nosacījumus, kā tas paredzēts Protokolā, ko parakstījusi Eiropas Savienība, Eiropas Kopiena, Šveices Konfederācija un Lihtenšteinas Firstiste par Lihtenšteinas Firstistes pievienošanu Nolīgumam, ko noslēgusi Eiropas Savienība, Eiropas Kopiena un Šveices Konfederācija par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un izstrādē, un tas pieder pie jomas, kas minēta 1. panta H un I punktā Lēmumā 1999/437/EK, kas lasāma saistībā ar 3. pantu Padomes Lēmumā 2008/262/TI ⁽⁷⁾ par minētā protokola parakstīšanu Eiropas Savienības vārdā.

(48) Šajā pamatlēmumā ir ievērotas pamattiesības un principi, kas jo īpaši atzīti Eiropas Savienības Pamattiesību hartā ⁽⁸⁾. Šā pamatlēmuma mērķis ir nodrošināt to, ka pilnībā ievēro tās tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību, kas atspoguļotas hartas 7. un 8. pantā,

IR PIEŅĒMUSI ŠO PAMATLĒMUMU.

1. pants

Mērķis un darbības joma

1. Šā pamatlēmuma mērķis ir nodrošināt augsta līmeņa aizsardzību fizisku personu pamattiesībām un pamatbrīvībām, jo īpaši to tiesībām uz privāto dzīvi, attiecībā uz personas datu apstrādi, kas notiek saskaņā ar Līguma par Eiropas Savienību VI sadaļā paredzēto policijas un tiesu iestāžu sadarbību krimināllietās, vienlaikus nodrošinot augsta līmeņa sabiedrības drošību.

2. Dalībvalstis saskaņā ar šo pamatlēmumu aizsargā fizisku personu pamattiesības un pamatbrīvības, jo īpaši to tiesības uz privāto dzīvi, gadījumos, kad saistībā ar noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu par tiem vai saistībā ar kriminālsodu izpildi personas datus:

a) nosūta vai dara pieejamus vai tie ir nosūtīti vai darīti pieejami starp dalībvalstīm;

⁽¹⁾ OV L 131, 1.6.2000., 43. lpp.

⁽²⁾ OV L 64, 7.3.2002., 20. lpp.

⁽³⁾ OV L 176, 10.7.1999., 36. lpp.

⁽⁴⁾ OV L 176, 10.7.1999., 31. lpp.

⁽⁵⁾ OV L 53, 27.2.2008., 52. lpp.

⁽⁶⁾ OV L 53, 27.2.2008., 50. lpp.

⁽⁷⁾ OV L 83, 26.3.2008., 5. lpp.

⁽⁸⁾ OV C 303, 14.12.2007., 1. lpp.

b) nosūta vai dara pieejamus vai tie ir nosūtīti vai darīti pieejami no dalībvalstīm – iestādēm un informācijas sistēmām, kas izveidotas, pamatojoties uz Līguma par Eiropas Savienību VI sadaļu, vai

c) nosūta vai dara pieejamus vai tie ir nosūtīti vai darīti pieejami no iestādēm vai informācijas sistēmām, kas izveidotas, pamatojoties uz Līgumu par Eiropas Savienību vai Eiropas Kopienas dibināšanas līgumu, – dalībvalstu kompetentām iestādēm.

3. Šis pamatlēmums attiecas uz personas datu apstrādi, kas pilnībā vai daļēji veikta ar automatizētiem līdzekļiem, un uz tādu personas datu apstrādi, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem.

4. Šis pamatlēmums neskar būtiskas valsts drošības intereses un īpašas izlūkošanas darbības valsts drošības jomā.

5. Šis pamatlēmums neliedz dalībvalstīm valsts līmenī apstrādāt vai vākt personas datu aizsardzībai noteikt stingrākus drošības pasākumus par šajā pamatlēmumā paredzētajiem.

2. pants

Definīcijas

Šajā pamatlēmumā:

a) “personas dati” ir jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisku personu, (turpmāk “datu subjekts”); identificējama persona ir tāda, ko tieši vai netieši var identificēt, jo īpaši – norādot personas kodu vai vienu vai vairākus šai personai raksturīgus fiziskas, fizioloģiskas, garīgas, saimnieciskas, kultūras vai sociālas identitātes faktoros;

b) “personas datu apstrāde” un “apstrāde” ir jebkura ar personas datiem veikta darbība vai darbību kopums ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, glabāšana, piemērošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, atklāšana, izmantojot pārsūtīšanu, izplatīšanu vai, citādi atklājot tos, saskaņošana vai savienošana, piekļuves liegšana, dzēšana vai iznīcināšana;

c) “piekļuves liegšana” ir uzglabātu personas datu iezīmēšana, paredzot ierobežot to apstrādi nākotnē;

d) “personas datu kartotēka” un “kartotēka” ir jebkurš sakārtots personas datu kopums, kurā tādi dati ir pieejami saskaņā ar īpašiem kritērijiem – centralizētiem, decentralizētiem vai izkliedētiem, pamatojoties uz funkcionālu vai ģeogrāfisku motivāciju;

e) “datu apstrādātājs” ir jebkura struktūra, kas apstrādā personas datus atbildīgā personas datu apstrādātāja uzdevumā;

f) “datu saņēmējs” ir jebkura struktūra, kurai izpauž datus;

g) “datu subjekta piekrišana” ir jebkura labprātīga attiecīgās personas vēlmju konkrēta un apzināta norāde, ar ko datu subjekts apliecina piekrišanu uz viņu attiecināmu personas datu apstrādei;

h) “kompetentas iestādes” ir aģentūras un struktūras, kas izveidotas ar tiesību aktiem, ko Padome pieņēmusi atbilstīgi Līguma par Eiropas Savienību VI sadaļai, kā arī dalībvalstu policijas, muitas, tiesu un citas kompetentas iestādes, kuras ar valsts tiesību aktiem ir pilnvarotas apstrādāt personas datus šā pamatlēmuma darbības jomā;

i) “personas datu apstrādātājs” ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai jebkura cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus;

j) “atsauču atzīmēšana” ir atzīmju veikšana uz uzglabātiem personas datiem bez nolūka ierobežot to apstrādi nākotnē;

k) “datu padarīšana par anonīmiem” ir datu tāda pārveidošana, lai atsevišķas norādes par personīgiem vai materiāliem apstākļiem vairs nevar piedēvēt identificētai vai identificējamai fiziskai personai, vai arī šāda piedēvēšana ir saistīta ar nesamērīgu laika, izmaksu un darba ieguldījumu.

3. pants

Likumības, samērīguma un mērķa principi

1. Kompetentās iestādes var vākt personas datus tikai konkrētiem, precīzi formulētiem un likumīgiem mērķiem saistībā ar to pienākumiem, un tos var apstrādāt tikai tam mērķim, kuram dati ir iegūti. Datu apstrāde ir likumīga, adekvāta un atbilstīga, un tā nav pārmērīgā apjomā saistībā ar mērķiem, kuriem dati ir iegūti.

2. Datu turpmāka apstrāde citiem mērķiem ir pieļaujama, ja ievēroti šādi nosacījumi:

a) tāda apstrāde nav nesaderīga ar mērķiem, kuriem dati ir iegūti;

b) kompetentās iestādes ir pilnvarotas apstrādāt šādus datus citiem mērķiem saskaņā ar spēkā esošajiem tiesību aktiem; un

c) datu apstrāde ir vajadzīga un proporcionāla minēto citu mērķu sasniegšanai.

Turklāt kompetentās iestādes var nosūtīt personas datus turpmāk apstrādāt vēstures, statistikas vai zinātniskiem mērķiem, ja dalībvalstis nosaka piemērotas garantijas, piemēram, par datu padarīšanu par anonīmiem.

4. pants

Labošana, dzēšana un piekļuves liegšana

1. Personas datus labo, ja tie nav precīzi, un, ja tas ir iespējams un vajadzīgs, tos papildina vai atjaunina.

2. Personas dati ir jādzēš vai jāpadara anonīmi, ja tie vairs nav vajadzīgi mērķiem, kuriem tie ir likumīgi iegūti vai likumīgi turpmāk apstrādāti. Šis noteikums neskar šo datu arhivēšanu atsevišķā datu kopā piemērotā termiņā saskaņā ar valsts tiesību aktiem.

3. Personas datus nedzēš, bet liedz piekļuvi šiem datiem, ja ir pamatots iemesls uzskatīt, ka dzēšana var ietekmēt datu subjekta likumīgas intereses. Datus, kuriem liegta piekļuve, apstrādā tikai mērķim, sakarā ar kuru tie netika dzēsti.

4. Ja personas dati ir ietverti juridiskā lēmumā vai reģistrā, kas saistīts ar juridiska lēmuma izdošanu, labošana, dzēšana vai piekļuves liegšanu veic saskaņā ar valsts noteikumiem par tiesvedību.

5. pants

Dzēšanas un pārbaudes termiņu noteikšana

Personas datu dzēšanai vai regulārai pārbaudei, vai arvien ir vajadzība datus uzglabāt, nosaka piemērotus termiņus. Šo termiņu ievērošanu nodrošina ar procedūru pasākumiem.

6. pants

Īpašu kategoriju datu apstrāde

Tādu personas datu apstrāde, kuri atklāj rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisku vai filozofisku pārliecību, dalību arodbiedrībās, kā arī uz veselību vai seksuālo dzīvi attiecināmu datu apstrāde ir pieļaujama tikai tad, ja tas ir absolūti vajadzīgs un ja valsts tiesību aktos ir paredzētas piemērotas garantijas.

7. pants

Automatizēti individuāli lēmumi

Lēmums, kas izraisa nelabvēlīgas tiesiskas sekas datu subjektam vai būtiski to ietekmē un ko pieņem, pamatojoties vienīgi uz tādu datu automatizētu apstrādi, kas paredzēti, lai novērtētu konkrētus individuālos aspektus, kas attiecas uz datu subjektu, ir atļaujams tikai tad, ja tas ir atļauts ar likumu, kurā paredzētas arī garantijas datu subjekta likumīgo interešu aizstāvībai.

8. pants

Pārsūtīto vai atklāto datu kvalitātes pārbaude

1. Kompetentās iestādes veic visus piemērotos pasākumus, lai nodrošinātu to, ka personas datus, kas ir neprecīzi, nepilnīgi vai

vairs nav aktuāli, nepārsūta vai neatklāj citām personām. Tādēļ kompetentās iestādes, cik iespējams, pirms personas datu nosūtīšanas vai atklāšanas pārbauda personas datu kvalitāti. Veicot datu pārsūtīšanu, ja iespējams, katreiz pievieno informāciju, kas ļauj datu saņēmējai dalībvalstij izvērtēt datu precizitātes, pilnības, aktualitātes un ticamības pakāpi. Ja personas dati pārsūtīti bez iepriekšēja lūguma, saņēmēja iestāde tūlīt izvērtē, vai dati ir vajadzīgi mērķiem, kādiem tie sūtīti.

2. Ja konstatē, ka ir nosūtīti nepareizi dati vai dati ir pārsūtīti nelikumīgi, par to nekavējoties informē datu saņēmēju. Dati ir nekavējoties jālabo, jādzēš vai jāliedz tiem piekļuve saskaņā ar 4. pantu.

9. pants

Termiņi

1. Datu nosūtītāja iestāde, nosūtot vai atklājot datus, saskaņā ar valsts tiesību aktiem un atbilstīgi 4. un 5. pantam var norādīt termiņus datu glabāšanai, pēc kuru beigām arī saņēmējam dati ir jādzēš vai jāliedz tiem piekļuve, vai jāpārbauda, vai tie arvien ir vajadzīgi. Šo prasību var neievērot, ja šo termiņu beigās dati ir vajadzīgi notiekošai noziedzīgu nodarījumu izmeklēšanai, kriminālvajāšanai par tiem vai kriminālspriedumu izpildei.

2. Ja nosūtītāja iestāde nav noteikusi termiņu saskaņā ar 1. punktu, piemēro saskaņā ar 4. un 5. pantu noteiktos termiņus datu glabāšanai, kas paredzēti saņēmējas dalībvalsts tiesību aktos.

10. pants

Reģistrēšana un dokumentēšana

1. Katru personas datu nosūtīšanas reizi reģistrē un dokumentē, lai pārbaudītu datu apstrādes likumību, veiktu pašuzraudzību un nodrošinātu datu integritāti un drošību.

2. Reģistrus un dokumentāciju, kas sagatavota saskaņā ar šā panta 1. punktu, pēc lūguma iesniedz datu aizsardzības uzraudzības iestādei datu aizsardzības kontrolei. Kompetentā uzraudzības iestāde šo informāciju izmanto vienīgi datu aizsardzības kontroles nolūkā un lai nodrošinātu datu pareizu apstrādi, kā arī datu integritāti un drošību.

11. pants

Citas valsts nosūtītu vai atklātu personas datu apstrāde

Personas datus, ko nosūtījušas vai atklājušas kompetentās citu dalībvalstu iestādes, saskaņā ar 3. panta 2. punkta prasībām drīkst turpmāk apstrādāt citiem mērķiem nekā tiem, kuriem tie sākotnēji tika nosūtīti vai atklāti, vienīgi tad, ja tas ir vajadzīgs šādiem mērķiem:

- a) lai novērstu, izmeklētu, atklātu tādu noziedzīgu nodarījumu un veiktu tā kriminālvajāšanu vai izpildītu kriminālsodu, kurš nav tas pats noziedzīgs darījums vai kriminālsods, par kuru dati ir nosūtīti vai atklāti;
- b) cita veida tiesvedībai vai administratīvām procedūrām, kas tieši saistītas ar noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu par tiem vai kriminālsodu izpildi;
- c) lai novērstu tūlītējus un nopietnus draudus sabiedrības drošībai, vai
- d) jebkādam citam mērķim vienīgi ar nosūtītājas dalībvalsts iepriekšēju piekrišanu vai ar datu subjekta piekrišanu, kas dota saskaņā ar valsts tiesību aktiem.
- b) saņēmēja iestāde trešā valstī vai saņēmēja starptautiska struktūra ir atbildīga par noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai kriminālvajāšanu par tiem vai par kriminālsodu izpildi;
- c) dalībvalsts, no kuras dati iegūti, ir devusi piekrišanu datu nodošanai atbilstīgi tās valsts tiesību aktiem, un
- d) trešā valsts vai starptautiska struktūra nodrošina piemērotu aizsardzības līmeni paredzētajai datu apstrādei.
2. Datu pārsūtīšana bez iepriekšējas piekrišanas saskaņā ar 1. punkta c) apakšpunktu ir atļaujama vienīgi gadījumos, kad datu pārsūtīšana ir svarīga, lai novērstu tūlītējus un nopietnus draudus dalībvalsts vai trešās valsts sabiedrības drošībai vai dalībvalsts būtiskām interesēm, un iepriekšēju piekrišanu nevar spējēt iegūt. Nekavējoties tiek informēta iestāde, kura dod šādu piekrišanu.

Turklāt kompetentās iestādes var nosūtīt personas datus turpmāk apstrādāt vēstures, statistikas vai zinātniskiem mērķiem, ja dalībvalstis nosaka piemērotas garantijas, piemēram, par datu padarīšanu par anonīmiem.

12. pants

Atbilstība valsts apstrādes ierobežojumiem

1. Ja atbilstīgi sūtītāja dalībvalsts tiesību aktiem īpašos gadījumos īpašus apstrādes ierobežojumus piemēro datu apmaiņai starp šīs dalībvalsts kompetentajām iestādēm, datu nosūtītāja iestāde norāda saņēmējam uz šādiem ierobežojumiem. Saņēmējs nodrošina, ka šie apstrādes ierobežojumi ir ievēroti.

2. Piemērojot 1. punktu, dalībvalstis uz datu nodošanu citām dalībvalstīm vai aģentūrām vai struktūrām, kas izveidotas saskaņā ar Līguma par Eiropas Savienību VI sadaļu, neattiecinā citus ierobežojumus, izņemot ierobežojumus, ko piemēro līdzīgai datu nodošanai valsts iekšzemē.

13. pants

Pārsūtīšana kompetentām iestādēm trešās valstīs vai starptautiskām struktūrām

1. Dalībvalstis nosaka, ka citas dalībvalsts kompetentās iestādes nosūtītās vai atklātos datus var pārsūtīt trešām valstīm vai starptautiskām struktūrām vienīgi tad, ja:

- a) tas ir nepieciešams, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus un saistībā ar tiem veiktu kriminālvajāšanu vai izpildītu kriminālsodus;

3. Atkāpjoties no 1. punkta d) apakšpunkta prasībām, personas datus var pārsūtīt, ja:

- a) tas ir noteikts datus pārsūtošās dalībvalsts tiesību aktos saistībā ar:

i) datu subjekta likumīgām īpašām interesēm vai

ii) likumīgām prioritārām interesēm, jo īpaši – svarīgām sabiedriskām interesēm, vai

- b) trešā valsts vai saņēmēja starptautiska struktūra nodrošina piemērotus drošības pasākumus, ko dalībvalsts saskaņā ar saviem valsts tiesību aktiem uzskata par piemērotiem.

4. 1. punkta d) apakšpunktā minēto aizsardzības līmeņa piemērotību novērtē, ņemot vērā visus ar datu pārsūtīšanas darbību vai datu pārsūtīšanas darbību kopumu cieši saistītos apstākļus. Jo īpaši ņem vērā datu veidu, ierosinātās apstrādes darbības vai darbību mērķi un ilgumu, izcelsmes valsti un valsti vai starptautisku struktūru, kas ir datu galamērķis, attiecīgajā trešā valstī vai starptautiskā struktūrā spēkā esošās gan vispārējās, gan nozaru tiesību normas un profesionālos noteikumus un drošības pasākumus, kas tajā jāievēro.

14. pants

Pārsūtīšana privātām personām dalībvalstīs

1. Dalībvalstis nosaka, ka citas dalībvalsts kompetentās iestādes nosūtītās vai atklātos personas datus privātām personām var pārsūtīt vienīgi turpmāk minētos gadījumos:

- a) tās dalībvalsts kompetentā iestāde, no kuras dati ir iegūti, ir piekritusi datu pārsūtīšanai atbilstīgi tās valsts tiesību aktiem;
- b) datu subjekta legītīmas intereses neliedz datus pārsūtīt, un
- c) īpašos gadījumos kompetentajai iestādei, kas pārsūta datus privātai personai, pārsūtīšana ir vajadzīga:
 - i) lai pildītu tai likumīgi uzlikto pienākumu;
 - ii) lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus un veiktu kriminālvajāšanu saistībā ar tiem vai izpildītu kriminālsodus;
 - iii) lai novērstu tūlītējus un nopietnus draudus sabiedrības drošībai vai
 - iv) lai novērstu privātpersonu tiesību būtisku aizskaršanu.

2. Kompetenta iestāde, kas pārsūta datus privātai personai, informē šo personu par to, kādiem mērķiem šos datus drīkst izmantot.

15. pants

Kompetentās iestādes informēšana pēc tās lūguma

Datu saņēmējs pēc tās kompetentās iestādes lūguma, kura nosūtījusi vai atklājusi personas datus, to informē par attiecīgo datu apstrādi.

16. pants

Datu subjekta informēšana

1. Dalībvalstis saskaņā ar attiecīgās valsts tiesību aktiem nodrošina, ka datu subjekts ir informēts par to, ka kompetentās iestādes vāc vai apstrādā personas datus.
2. Ja personas dati ir pārsūtīti vai atklāti starp dalībvalstīm, katra dalībvalsts saskaņā ar tās tiesību aktu noteikumiem, kas minēti 1. punktā, var lūgt, lai otrā dalībvalsts neinformētu datu subjektu. Šādā gadījumā pēdējā minētā dalībvalsts neinformē datu subjektu, ja nav saņemta otrās dalībvalsts iepriekšējā piekrišana.

17. pants

Piekļuves tiesības

1. Katram datu subjektam ir tiesības pēc lūguma iesniegšanas samērīgos termiņos bez ierobežojumiem, kā arī bez pārmērīgas kavēšanas vai izmaksām saņemt:
 - 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.

2. Dalībvalstis var pieņemt tiesību aktus, ierobežojot piekļuvi informācijai saskaņā ar šā panta 1. punktu a) apakšpunktu, ja šāds ierobežojums, ņemot vērā attiecīgās personas likumīgās intereses, ir vajadzīgs un samērīgs šādiem mērķiem:

- a) lai izvairītos no oficiālas vai tiesiskas izmeklēšanas vai procedūru kavēšanas;
- b) lai izvairītos no noziedzīgu nodarījumu novēršanas, izmeklēšanas un atklāšanas un kriminālvajāšanas kavēšanas;
- c) lai aizsargātu sabiedrības drošību;
- d) lai aizsargātu valsts drošību;
- e) lai aizsargātu datu subjektu citu personu tiesības un brīvības.

3. Par atteikumu vai ierobežošanu piekļūt informācijai datu subjektam paziņo rakstiski. Vienlaicīgi tam paziņo faktiskos vai tiesiskos iemeslus, kas ir lēmuma pamatā. Tādu paziņošanu var neveikt, ja ir pamatojums saskaņā ar šā panta 2. punkta a) līdz e) apakšpunktu. Visos šajos gadījumos datu subjekts ir jāinformē par to, ka tas kompetentajai valsts uzraudzības iestādei, tiesas iestādei vai tiesai var iesniegt sūdzību.

18. pants

Tiesības uz datu labošanu, dzēšanu vai piekļuves liegšanu tiem

1. Datu subjektam ir tiesības sagaidīt, lai personas datu apstrādātājs pildītu šajā pamatlēmumā noteiktos pienākumus saistībā ar 4., 8. un 9. pantu attiecībā uz personas datu labošanu, dzēšanu vai piekļuves liegšanu tiem. Dalībvalstis nosaka, vai datu subjekts minētās tiesības īsteno tieši attiecībā uz personas datu apstrādātāju vai ar kompetentās valsts uzraudzības iestādes starpniecību. Ja personas datu apstrādātājs liedz datus labot, dzēst vai liegt piekļuvi tiem, atteikums ir jānosūta rakstiskā veidā datu subjektam, kam jābūt informētam par valsts tiesību aktos noteiktajām iespējām iesniegt sūdzību vai iesniegt pārsūdzību tiesā. Izskatot sūdzību vai pārsūdzību tiesā, datu subjektu informē, vai personas datu apstrādātājs ir rīkojies pareizi. Dalībvalstis var arī noteikt, ka kompetentajai valsts uzraudzības iestādei jāinformē datu subjekts par to, ka ir veikta pārskatīšana.

2. Ja datu subjekts apgalvo, ka dati ir neprecīzi, un ja nevar noteikt, vai tie ir vai nav precīzi, veic attiecīgo datu atsauču iezīmēšanu.

19. pants

Tiesības saņemt kompensāciju

1. Jebkurai personai, kurai nodarīts kaitējums sakarā ar datu nelikumīgu apstrādi vai jebkādas rīcības dēļ, kas nav savienojama ar valsts noteikumiem, kuri pieņemti šā pamatlēmuma īstenošanai, ir tiesības saņemt no personas datu apstrādātāja vai citas saskaņā ar valsts tiesību aktiem kompetentās iestādes kompensāciju par nodarīto kaitējumu.

2. Ja datus ir nosūtījusi dalībvalsts kompetenta iestāde, saņēmējs saistībā ar savu atbildību pret cietušo pusi saskaņā ar valsts tiesību aktiem nevar atsaukties uz to, ka nosūtītie dati bijuši neprecīzi. Ja saņēmējs izmaksā kompensāciju par kaitējumu, ko izraisījusi neprecīzi nosūtīto datu izmantošana, datus nosūtījusi kompetentā iestāde pilnībā atlīdzina saņēmējam izmaksātās kompensācijas summu, ņemot vērā jebkādu iespējamo saņēmēja vainu.

20. pants

Tiesiskās aizsardzības līdzekļi

Neskarot nevienu administratīvu līdzekli, ko var izmantot pirms vērsšanās tiesā, datu subjektam ir jābūt nodrošinātām tiesībām vērsties tiesā par jebkuru tādu tiesību pārkāpumu, kas attiecinājams personai garantētas valsts tiesību aktos.

21. pants

Datu apstrādes konfidencialitāte

1. Jebkura persona, kam ir piekļuve personas datiem, uz kuriem attiecas šis pamatlēmums, var apstrādāt šos datus tikai tad, ja šī persona ir piederīga kompetentajai iestādei vai darbojas tās uzdevumā, ja vien šai personai tas nav jādara saskaņā ar tiesību aktu prasību.

2. Personām, kas strādā dalībvalsts kompetentās iestādes labā, ir saistoši visi datu aizsardzības noteikumi, ko piemēro attiecīgajai kompetentajai iestādei.

22. pants

Datu apstrādes drošība

1. Dalībvalstis nosaka, ka kompetentajām iestādēm ir jāīsteno atbilstīgi tehniski un organizatoriski pasākumi, lai aizsargātu personas datus pret nejaušu vai nelikumīgu iznīcināšanu vai

nejaušu nozaudēšanu, nesankcionētu pārveidošanu, nesankcionētu atklāšanu vai piekļuvi tiem, īpaši, ja apstrāde ietver datu pārraidi elektronisko sakaru tīklā, vai pret to atklāšanu, piešķirot tiešu automatizētu piekļuvi, un pret visām citām nelikumīgām apstrādes formām. Turklāt īpaši jāņem vērā riski, kas raksturīgi aizsargājamo datu apstrādei. Ņemot vērā pašreizējā līmeņa tehniskos un organizatoriskos pasākumus un to īstenošanas izmaksas, minētie pasākumi nodrošina raksturīgajiem apstrādes un aizsargājamo datu riskiem atbilstošu drošības pakāpi.

2. Datu automatizētā apstrādē 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 datu nesankcionētu nolasīšanu, kopēšanu, sagrozīšanu vai izņemšanu no datu nesējiem (datu nesēju kontrole);
- c) liegtu datu neatļautu ievadīšanu datubāzē, kā arī liegtu ievadīto personas datu neatļautu lasīšanu, grozīšanu vai dzēšanu (glabāšanas 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 kuriem attiecas viņu piekļuves tiesības (datu piekļuves kontrole);
- f) nodrošinātu, ka ir iespējams pārbaudīt un noteikt, kurām organizācijām dati ir vai var tikt pārsūtīti vai atklāti, izmantojot datu komunikācijas iekārtas (komunikācijas kontrole);
- g) nodrošinātu, ka pēc tam ir iespējams pārbaudīt un noteikt, kādi 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 pārsūtīšanas laikā vai datu nesēja transportēšanas laikā (transportēšanas kontrole);
- i) nodrošinātu, ka traucējumu gadījumā uzstādītās sistēmas var atjaunot (atgūšana);
- j) nodrošinātu, ka sistēma funkcionē tā, ka par kļūdu parādīšanos darbībā ziņo (drošums) un saglabātie dati nevar tikt sabojāti sistēmas darbības traucējumu dēļ (integritāte).

3. Dalībvalstis nosaka, ka par datu apstrādātāju var noteikt tikai tādas personas, kas garantē, ka tās atbilst šā panta 1. punktā prasītajiem tehniskajiem organizatoriskajiem pasākumiem un ievēro 21. panta norādījumus. Kompetentā iestāde šajā sakarā veic datu apstrādātāja uzraudzību.

4. Datu apstrādātājs var apstrādāt personas datus, vienīgi pamatojoties uz tiesību aktu vai rakstisku līgumu.

23. pants

Iepriekšējas konsultācijas

Dalībvalstis nodrošina, ka pirms personas datu apstrādes, ko ietver jaunā veidojamā kartotēkā, konsultējas ar kompetentajām valsts uzraudzības iestādēm gadījumos, ja:

- a) apstrādā īpašu kategoriju datus, kas minēti 6. pantā; vai
- b) datu apstrādes veids, jo īpaši izmantojot jaunas tehnoloģijas, mehānismus vai procedūras, rada citādu veidu īpašu risku attiecībā uz datu subjekta pamattiesībām un pamatbrīvībām, jo īpaši attiecībā uz tā privātuma aizsardzību.

24. pants

Sankcijas

Dalībvalstis pieņem attiecīgus pasākumus, lai nodrošinātu šā pamatlēmuma ieviešanu pilnībā, un jo īpaši nosaka efektīvas, samērīgas un preventīvas sankcijas, kas jāuzliek gadījumā, ja ir pārkāpti saskaņā ar šo pamatlēmumu pieņemti noteikumi.

25. pants

Valsts uzraudzības iestādes

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

2. Katrai uzraudzības iestādei jo īpaši ir piešķirtas:

- a) izmeklēšanas pilnvaras, piemēram, pilnvaras piekļūt datiem, kurus apstrādā, un pilnvaras ievākt visu informāciju, kas ir vajadzīga tās pārraudzības pienākumu izpildei;
- b) efektīvas iejaukšanās pilnvaras, piemēram, pilnvaras sniegt atzinumus pirms datu apstrādes darbību veikšanas un pilnvaras nodrošināt minēto atzinumu atbilstīgu nodošanu atklātībai, pilnvaras likt liegt 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 iestādēm;

- c) 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.

3. Jebkura persona jebkurai uzraudzības iestādei var iesniegt prasību, kas saistīta ar šīs personas tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi. Ieinteresēto personu informē par prasības rezultātu.

4. Dalībvalstis nosaka, ka uzraudzības iestādei piederīgajām personām un tās personām ir saistoši attiecīgajai kompetentajai iestādei piemērojamie datu aizsardzības noteikumi par dienesta noslēpumu attiecībā uz konfidenciālu informāciju, kas viņiem ir pieejama, pat pēc viņu nodarbinātības laika izbeigšanās.

26. pants

Saistība ar nolīgumiem ar trešām valstīm

Šis pamatlēmums neskar dalībvalstu vai Savienības saistības un pienākumus, kas izriet no divpusējiem un/vai daudzpusējiem nolīgumiem ar trešām valstīm, kuri ir spēkā šā pamatlēmuma pieņemšanas laikā.

Piemērojot šos nolīgumus, no dalībvalsts saņemtu personu datu pārsūtīšanu trešai valstij veic, ievērojot attiecīgi 13. panta 1. punkta c) apakšpunktu vai 2. punktu.

27. pants

Izvērtēšana

1. Dalībvalstis līdz 2013. gada 27. novembrim ziņo Komisijai par valsts pasākumiem, kas veikti, lai nodrošinātu pilnīgu šā pamatlēmuma ievērošanu, un jo īpaši to noteikumu ievērošanu, kas jāievēro, vācot datus. Komisija īpaši pārbauda, kāda šiem noteikumiem ir ietekme ir uz šā pamatlēmuma darbības jomu, kā noteikts 1. panta 2. punktā.

2. Komisija viena gada laikā ziņo Eiropas Parlamentam un Padomei par 1. punktā minētā izvērtējuma rezultātiem, un pievieno ziņojumam jebkādas piemērotas priekšlikumus šā pamatlēmuma grozījumiem.

28. pants

Saistība ar iepriekš pieņemtajiem Savienības aktiem

Ja tiesību aktos, kas pieņemti saskaņā ar Līguma par Eiropas Savienību VI sadaļu, pirms stājas spēkā pamatlēmums, un kas reglamentē personas datu apmaiņu starp dalībvalstīm vai dalībvalstu izraudzīto iestāžu piekļuvi saskaņā ar Eiropas Kopienas dibināšanas līguma izveidotajām informācijas sistēmām, ir paredzēti īpaši noteikumi par saņēmējas dalībvalsts veiktu personas datu izmantošanu, šiem noteikumiem ir lielāks juridisks spēks nekā šā pamatlēmuma noteikumiem par to datu izmantošanu, kuri saņemti no citas dalībvalsts vai kurus tā darījusi pieejamus.

29. pants

Īstenošanas noteikumi

1. Dalībvalstis līdz 2010. gada 27. novembrim veic vajadzīgos pasākumus, lai nodrošinātu atbilstību šim pamatlēmumam.
2. Līdz minētajai dienai dalībvalstis nosūta Padomes Ģenerālsekretariātam un Komisijai tos noteikumus, ar kuriem saistības,

kuras tām uzliek šis pamatlēmums, transponē valstu tiesību aktos, kā arī informāciju par 25. pantā minēto uzraudzības iestādi vai iestādēm. Pamatojoties uz Komisijas ziņojumu, kas sastādīts, izmantojot šo informāciju, Padome līdz 2011. gada 27. novembrim izvērtē, kā dalībvalstis ir nodrošinājušas atbilstību šim pamatlēmumam.

30. pants

Stāšanās spēkā

Šis pamatlēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2008. gada 27. novembrī

Padomes vārdā —
priekšsēdētāja
M. ALLIOT-MARIE