



EIROPAS PARLAMENTA UN PADOMES REGULA (EK)
Nr. 1987/2006

2006. gada 20. decembris

par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) izveidi,
darbību un izmantošanu

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

SIS II izveide un vispārējais mērķis

1. Ar šo izveido otrās paaudzes Šengenas Informācijas sistēmu ("SIS II").

2. Saskaņā ar šo regulu SIS II mērķis ir nodrošināt augstu drošības līmeni brīvības, drošības un tiesiskuma telpā, tostarp dalībvalstu teritorijā nodrošināt sabiedrības drošības sabiedriskās kārtības uzturēšanu un saglabāšanu, un piemērot Līguma IV sadaļas noteikumus par personu pārvietošanos to teritorijās, izmantojot šīs sistēmas izplatīto informāciju.

2. pants

Darbības joma

1. Ar šo regulu paredz nosacījumus un kārtību tādu brīdinājumu ievadīšanai un apstrādei SIS II, kas izdoti attiecībā uz trešo valstu valstspiederīgajiem, un papildinformācijas un papildu datu apmaiņai, lai atteiktu ieceļošanu vai uzturēšanos dalībvalstī.

2. Tāpat ar šo regulu paredz noteikumus par SIS II tehnisko uzbūvi, dalībvalstu un 15. pantā minētās pārvaldības iestādes atbildību, vispārēju datu apstrādi, attiecīgo personu tiesībām un atbildību.

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

- a) "brīdinājums" ir datu kopums, ko ievada SIS II un kas kompetentajām iestādēm ļauj identificēt personu, lai konkrēti rīkotos;
- b) "papildinformācija" ir informācija, ko neglabā SIS II, bet kas ir saistīta ar SIS II brīdinājumiem un ar ko apmainās:
 - i) lai dalībvalstis var savstarpēji apspriesties vai informēt cita citu, ievadot brīdinājumu,
 - ii) pēc pozitīvas atbildes saņemšanas, lai varētu attiecīgi rīkoties,
 - iii) ja nav iespējams veikt prasīto rīcību,

▼B

- iv) apsverot SIS II datu kvalitāti,
 - v) apsverot brīdinājumu savietojamību un prioritāti,
 - vi) saistībā ar piekļuves tiesībām;
- c) “papildu dati” ir dati, ko saglabā SIS II un kas saistīti ar SIS II brīdinājumiem un nekavējoties pieejami kompetentajām iestādēm, ja SIS II meklēšanas rezultātā atrod personu, par kuru dati ir ievadīti SIS II;
- d) “trešās valsts valstspiederīgais” ir jebkura persona, kas nav:
- i) ne Eiropas Savienības pilsonis Līguma 17. panta 1. punkta nozīmē;
 - ii) ne arī trešās valsts valstspiederīgais, kuram - saskaņā ar nolīgumiem starp Kopienu un tās dalībvalstīm, no vienas puses, un attiecīgo valsti, no otras puses, ir tādas pašas brīvas pārvietošanās tiesības, kādas ir Eiropas Savienības pilsoņiem;
- e) “personas dati” ir jebkura informācija par identificētu vai identificējamu fizisko personu (“datu subjektu”); identificējama persona ir persona, ko var tieši vai netieši identificēt;
- f) “personas datu apstrāde” (“apstrāde”) ir jebkura darbība vai darbību kopums, kas ar vai bez automatizētiem līdzekļiem veiktas ar personas datiem, kā datu vākšana, reģistrācija, organizēšana, saglabāšana, piemērošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, atklāšana, izmantojot pārsūtīšanu, izplatīšanu vai citādi padarot tos pieejamus, saskaņošana vai savienošana, piekļuves liegšana, dzēšana vai iznīcināšana.

*4. pants***SIS II tehniskā arhitektūra un darbības veidi**

1. SIS II veido:

a) centrālā sistēma (“centrālā SIS II”), ko veido:

— tehniskā nodrošinājuma vienība (“CS-SIS”), kurā ietverta datubāze - “SIS II datubāze”;

— vienota valsts saskarne (“NI-SIS”);

▼B

- b) valsts sistēma katrā dalībvalstī (“N. SIS II”), ko veido valsts datu sistēmas, kuras ir saistītas ar centrālo SIS II. N. SIS II var ietvert datu datni (“valsts eksemplārs”), kas ir pilnīga vai daļēja SIS II datubāzes kopija;
- c) CS-SIS un NI-SIS savstarpējo sakaru infrastruktūra (“sakaru infrastruktūra”), kas nodrošina SIS II datiem atvēlētu kodētu virtuālu tīklu un *SIRENE* biroju savstarpēju datu apmaiņu, kā minēts 7. panta 2. punktā.

2. SIS II datus ievada, atjaunina, dzēš un tajos veic meklēšanu, izmantojot dažādās N. SIS II sistēmas. Valsts eksemplāru dara pieejamu, lai veiktu automatizētu meklēšanu katras dalībvalsts teritorijā, kas lieto tādu eksemplāru. Veikt meklēšanu citu dalībvalstu N. SIS II datu datnēs nav iespējams.

3. CS-SIS, ar ko veic tehniskās uzraudzības un administrācijas uzdevumus, atrodas Strasbūrā (Francijā), un CS-SIS dublējums, kurš spēj nodrošināt visas galvenās CS-SIS funkcijas šīs sistēmas avārijas gadījumā, atrodas *Sankt Johann imPongau* (Austrijā).

4. CS-SIS nodrošina pakalpojumus, kas vajadzīgi, lai ievadītu un apstrādātu SIS II datus, tostarp veiktu meklēšanu SIS II datubāzē. Dalībvalstīm, kas lieto valsts eksemplāru, CS-SIS nodrošina:

- a) valsts eksemplāru tiešsaistes atjaunināšanu;
- b) valsts eksemplāru un SIS II datubāzes sinhronizāciju un saskanību;
- c) kārtību valsts eksemplāru inicializēšanai un rekonstrukcijai.

*5. pants***Izmaksas**

1. Centrālās SIS II un sakaru infrastruktūras izveides, darbības un uzturēšanas izmaksas sedz no Eiropas Savienības vispārējā budžeta.

2. Šīs izmaksas ietver attiecībā uz CS-SIS veikto darbu, kas nodrošina 4. panta 4. punktā minēto pakalpojumu nodrošināšanu.

3. Katras N. SIS II izveides, darbības un uzturēšanas izmaksas sedz no attiecīgās dalībvalsts budžeta.

▼B**II NODAĻA
DALĪBVALSTU ATBILDĪBA****▼M2***6. pants***Valstu sistēmas**

1. Katra dalībvalsts ir atbildīga par savas *N.SIS II* izveidi, ekspluatāciju, uzturēšanu un turpmāku attīstīšanu, kā arī par tās sasaistīšanu ar *NI-SIS*.

2. Katra dalībvalsts ir atbildīga par *SIS II* datu nepārtrauktas pieejamības nodrošināšanu galalietotājiem.

▼B*7. pants***N. SIS II birojs un SIRENE birojs**

1. Katra dalībvalsts norīko iestādi (“N. SIS II birojs”), kam ir galvenā atbildība par attiecīgo N. SIS II. Minētā iestāde ir atbildīga par N. SIS II netraucētu darbību un drošību, nodrošina kompetentu iestāžu piekļuvi SIS un veic pasākumus, kas vajadzīgi, lai nodrošinātu atbilstību šai regulai. Katra dalībvalsts izdod brīdinājumus ar N. SIS II biroja starpniecību.

2. Katra dalībvalsts izraugās iestādi, kas nodrošina visas papildinformācijas apmaiņu (“SIRENE birojs”) saskaņā ar *SIRENE* rokasgrāmatas noteikumiem, kā minēts 8. pantā.

Minētie biroji arī koordinē SIS II ievadītās informācijas kvalitātes pārbaudi. Šajos nolūkos tiem ir piekļuve SIS II apstrādātajiem datiem.

3. Dalībvalstis informē pārvaldības iestādi par attiecīgās valsts N. SIS II biroju un *SIRENE* biroju. Pārvaldības iestāde publicē šo biroju sarakstu kopā ar 31. panta 8. punktā minēto sarakstu.

*8. pants***Papildinformācijas apmaiņa**

1. Papildinformācijas apmaiņu veic saskaņā ar *SIRENE* rokasgrāmatu un izmantojot sakaru infrastruktūru. Ja sakaru infrastruktūra nav pieejama, dalībvalstis var papildinformācijas apmaiņai izmantot citus atbilstīgi nodrošinātus tehniskos līdzekļus.

2. Papildinformāciju izmanto vienīgi nolūkā, kādā tā ir nosūtīta.

▼B

3. Uz dalībvalsts lūgumu sniegt papildinformāciju atbild iespējami īsā laikā.

4. Sīki izstrādātus papildinformācijas apmaiņas noteikumus pieņem saskaņā ar 51. panta 2. punktā minēto procedūru kā “SIRENE rokasgrāmatu”, neskarot instrumentu, ar ko izveido pārvaldības iestādi.

*9. pants***Tehniskā atbilstība**

1. Lai nodrošinātu datu ātru un efektīvu pārsūtīšanu, katra dalībvalsts, izveidojot savu N. SIS II, ievēro protokolus un tehniskās procedūras, kas izveidoti, lai nodrošinātu tās N. SIS II savietojamību ar CS/SIS. Minētos protokolus un tehniskās procedūras izveido saskaņā ar 51. panta 2. punktā minēto procedūru, neskarot instrumentu, ar ko izveido pārvaldības iestādi.

2. Ja dalībvalsts izmanto valsts eksemplāru, tā ar CS-SIS sniegtu pakalpojumu palīdzību nodrošina, ka dati, ko glabā valsts eksemplārā, veicot 4. panta 4. punktā minēto automatisko atjaunināšanu, ir identiski un saskaņoti ar SIS II datubāzi un ka meklēšana attiecīgās valsts eksemplārā sniedz līdzvērtīgu rezultātu SIS II datubāzē veiktai meklēšanai.

*10. pants***Drošība - dalībvalstis**

1. Katra dalībvalsts attiecībā uz N. SIS II pieņem vajadzīgos pasākumus, tostarp drošības plānu, lai:

- a) fiziski aizsargātu datus, tostarp izstrādājot ārkārtas rīcības plānus kritiskās infrastruktūras aizsardzībai;
- b) liegtu nepilnvarotām personām piekļuvi datu apstrādes iekārtām, ko izmanto personas datu apstrādei (piekļuves kontrole);
- c) nodrošinātu to, ka nepilnvarotas personas nelasa, nekopē, negroza vai nedzēš datu nesējus (datu nesēju kontrole);
- d) liegtu datu neatļautu ievadīšanu datubāzē, kā arī liegtu ievadīto personas datu neatļautu lasīšanu, grozīšanu vai dzēšanu (glabāšanas kontrole);

▼ B

- e) nepieļautu to, ka nepilnvarotas personas lieto datu automatizētas apstrādes sistēmu ar datu pārraides ierīču palīdzību (lietošanas kontrole);
- f) nodrošinātu to, ka personām, kam ir pilnvaras lietot automatizētās apstrādes sistēmu, ir pieejami vienīgi tie dati, kuriem tām atļauts piekļūt, un ka šīs personas tiem piekļūst tikai ar individuālām un unikālām lietotāju identitātēm un konfidenciāliem pieejas veidiem (datu pieejamības kontrole);
- g) nodrošinātu to, ka iestādes, kurām ir piekļuves tiesības SIS II vai datu apstrādes iekārtām, izstrādā profilus, raksturojot to personu funkcijas un pienākumus, kuras ir pilnvarotas piekļūt, ievadīt, atjaunot, dzēst un meklēt datus, un pēc 44. panta 1. punktā minēto valstu uzraudzības iestāžu lūguma šos profilus nekavējoties dara tām pieejamus (personālie profili);
- h) nodrošinātu to, ka var pārbaudīt un noteikt, kurām iestādēm personas datus var pārraidīt, izmantojot datu pārraides ierīces (datu pārraides kontrole);
- i) nodrošinātu to, ka vēlāk iespējams pārbaudīt un noteikt, kādi personas dati ir ievadīti automatizētā datu apstrādes sistēmā, kurā brīdī un kura persona tos ir ievadījusi, un kādā nolūkā (ievades kontrole);
- j) nodrošinātu to, ka personas datu pārraides un datu nesēju pārsūtīšanas laikā nav iespējama personas datu neatļauta lasīšana, kopēšana, grozīšana vai dzēšana, to jo īpaši nodrošinot ar attiecīgiem kodēšanas paņēmieniem (pārsūtīšanas kontrole);
- k) uzraudzītu šajā punktā minētos drošības pasākumus un veiktu vajadzīgos organizatoriskos pasākumus saistībā ar iekšējo uzraudzību, lai nodrošinātu atbilstību šai regulai (paškontrole).

2. Dalībvalstis pieņem 1. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz drošību saistībā ar papildinformācijas apmaiņu.

▼ M2*11. pants***Konfidencialitāte – dalībvalstis**

1. Katra dalībvalsts saskaņā ar saviem tiesību aktiem piemēro savus noteikumus par dienesta noslēpumu vai citas līdzvērtīgas prasības attiecībā uz konfidencialitāti visām personām un visām struktūrām, kam jāstrādā ar *SIS II* datiem un papildinformāciju. Šis pienākums ir spēkā arī pēc tam, kad šīs personas vairs neieņem attiecīgo amatu vai netiek nodarbinātas vai kad minēto struktūru darbība ir izbeigta.

▼ M2

2. Ja dalībvalsts jebkuru ar *SIS II* saistītu uzdevumu veikšanai sadarbojas ar ārējiem līgumslēdzējiem, tā rūpīgi uzrauga līgumslēdzēja darbības, lai nodrošinātu atbilstību visiem šīs regulas noteikumiem, jo īpaši attiecībā uz drošību, konfidencialitāti un datu aizsardzību.

3. *N.SIS II* vai jebkuru tehnisko kopiju darbības pārvaldību neuztic privātiem uzņēmumiem vai privātām organizācijām.

▼ B*12. pants***Ierakstu saglabāšana attiecīgajās valstīs**

1. Katra dalībvalsts, kas nelieto valsts eksemplārus, nodrošina, ka katra piekļuve personas datiem un visas personas datu apmaiņas ar CS-SIS ir ierakstītas N. SIS II, lai pārbaudītu, vai meklēšana ir vai nav likumīga, lai uzraudzītu datu apstrādes likumību un pašuzraudzības nolūkos, nodrošinot N. SIS II pareizu darbību, datu integritāti un drošību.

2. Dalībvalstis, kas lieto valsts eksemplārus, nodrošina, ka 1. punktā minētajiem mērķiem reģistrē katru piekļuvi SIS II datiem un visas SIS II datu apmaiņas. Tas neattiecas uz 4. panta 4. punktā minētajiem procesiem.

3. Ierakstos konkrēti uzrāda brīdinājumu vēsturi, datu pārraides datumu un laiku, meklēšanā izmantotos datus, atsauci uz pārraidītajiem datiem un gan kompetentās iestādes, gan par datu apstrādi atbildīgās personas vārdu.

4. Ierakstus lieto vienīgi 1. un 2. punktā minētajā nolūkā un dzēš ne ātrāk kā pēc gada un ne vēlāk kā pēc trim gadiem no to izveides dienas. Ierakstus, kuros ietverta brīdinājumu vēsture, dzēš vienu līdz trīs gadus pēc brīdinājumu dzēšanas.

5. Ierakstus var saglabāt ilgāk, ja tie vajadzīgi uzraudzības procedūrām, kas jau ir iesāktas.

6. Kompetentajām valsts iestādēm, kuru pienākumos ir pārbaudīt, vai meklēšana ir likumīga, uzraudzīt datu apstrādes likumību, veikt pašuzraudzību, nodrošināt N. SIS II pareizu darbību, datu integritāti un drošību, atbilstīgi to kompetencei un pēc to lūguma nodrošina piekļuvi šiem ierakstiem, lai tās varētu pildīt savus pienākumus.

▼ B*13. pants***Pašuzraudzība**

Dalībvalstis nodrošina, ka katra iestādei, kurai ir tiesības piekļūt SIS II, veic pasākumus, lai nodrošinātu atbilstību šai regulai, un vajadzības gadījumā sadarbojas ar valsts uzraudzības iestādi.

*14. pants***Personāla apmācība**

To iestāžu personālu, kam ir tiesības piekļūt SIS II, pienācīgi apmāca par datu drošību un datu aizsardzības noteikumiem, kā arī informē par jebkuru attiecīgi piemērojamu kriminālatbildību un sodiem, pirms tiem piešķir atļauju apstrādāt SIS II uzglabātos datus.

III NODAĻA

PĀRVALDĪBAS IESTĀDES PIENĀKUMI*15. pants***Darbības pārvaldība**

1. Pēc pārejas posma beigām pārvaldības iestāde, ko finansē no Eiropas Savienības vispārējā budžeta, ir atbildīga par centrālās SIS II darbības pārvaldību. Pārvaldības iestāde sadarbībā ar dalībvalstīm nodrošina to, ka centrālās SIS II vajadzībām vienmēr tiek izmantota vislabākā pieejamā tehnoloģija, pamatojoties uz izmaksu un ieguvumu analīzi.

▼ M1

2. Pārvaldības iestāde ir atbildīga par šādiem uzdevumiem, kas saistīti ar komunikāciju infrastruktūru, jo īpaši:

- a) uzraudzību;
- b) drošību;
- c) dalībvalstu un nodrošinātāja attiecību koordinēšanu;
- d) uzdevumiem saistībā ar budžeta izpildi;
- e) iegādi un atjaunināšanu; un
- f) jautājumiem, kas saistīti ar līgumiem.

▼ M2

3.a Pārvaldības iestāde izstrādā un uztur mehānismu un procedūras, lai veiktu CS-SIS datu kvalitātes pārbaudes. Tā regulāri iesniedz ziņojumus dalībvalstīm.

Pārvaldības iestāde regulāri iesniedz Komisijai ziņojumu par problēmām un attiecīgajām dalībvalstīm.

Komisija regulāri ziņo Eiropas Parlamentam un Padomei par datu kvalitātes jautājumiem, kas radušies.

▼ B

4. Pārejas posmā, pirms pārvaldības iestāde sāk pildīt savus pienākumus, Komisija ir atbildīga par centrālās SIS II darbības pārvaldību. Saskaņā ar Padomes Regulu (EK, *Euratom*) Nr. 1605/2002 (2002. gada 25. jūnijs) par finanšu regulu, ko piemēro Eiropas Kopienu vispārējam

▼B

budžetam ⁽¹⁾, Komisija var minēto uzdevumu un uzdevumus saistībā ar budžeta izpildi deleģēt valstu publiskajām struktūrām, kuras atrodas divās dažādās valstīs.

5. Katra 4. punktā minētā valsts publiskā struktūra atbilst šādiem atlases kritērijiem:

- a) iestādei jāpierāda ilgtermiņa pieredze tādas liela mēroga informācijas sistēmas darbības nodrošināšanā, kura veic 4. panta 4. punktā minētās funkcijas;
- b) iestādes personālam ir jābūt būtiskai pieredzei tādas informācijas sistēmas pakalpojumu un drošības prasību jomā, kura pielīdzināma 4. panta 4. punktā minētajām funkcijām;
- c) iestādes personālam ir jābūt pietiekami nokomplektētam, pieredzējušam, kā arī ar atbilstīgām profesionālām un valodas iemaņām, lai strādātu starptautiskas sadarbības vidē, kādu prasa SIS II;
- d) iestādei jābūt pieejamām drošām un īpaši uzbūvētām infrastruktūrām, jo īpaši, lai varētu dublēt un garantēt liela mēroga IT sistēmu nepārtrauktu darbību;

un

- e) iestādes administratīvajai videi ir jābūt tādai, kas ļauj pareizi veikt uzticētos uzdevumus un izvairīties no interešu konfliktiem.

6. Pirms jebkādas 4. punktā minētās deleģēšanas un regulāri pēc tam Komisija informē Eiropas Parlamentu un Padomi par deleģēšanas nosacījumiem, precīzu tās piemērošanas jomu un par struktūrām, kurām deleģēti uzdevumi.

7. Ja Komisija saskaņā ar 4. punktu pārejas posmā deleģē savu atbildību, tā nodrošina, ka, veicot šo deleģēšanu, pilnībā ir ievēroti ierobežojumi, kas paredzēti Līgumā noteiktajā iestāžu sistēmā. Komisija jo īpaši nodrošina, ka šāda deleģēšana nelabvēlīgi neietekmē nevienu ar Kopienas tiesību aktiem saistītu efektīvu kontroles mehānismu – ne Tiesas, ne Revīzijas palātas, ne Eiropas Datu aizsardzības uzraudzītāja kontroles mehānismu.

▼M2

8. Centrālās SIS II darbības pārvaldība ir visi uzdevumi, kas vajadzīgi, lai saskaņā ar šo regulu nodrošinātu centrālās SIS II darbību 24 stundas diennaktī 7 dienas nedēļā, jo īpaši uzturēšanas darbi un tehniski pielāgojumi, kas vajadzīgi sistēmas nevainojamai darbībai. Minētie

⁽¹⁾ OV L 248, 16.9.2002., 1. lpp.

▼ M2

uzdevumi ietver arī centrālās *SIS II* un *N.SIS II* testēšanas pasākumu koordinēšanu, vadību un atbalstīšanu, kas nodrošina, ka centrālā *SIS II* un *N.SIS II* darbojas saskaņā ar tehniskās atbilstības prasībām, kas izklāstītas 9. pantā.

▼ B*16. pants***Drošība**

1. Pārvaldības iestāde attiecībā uz centrālo *SIS II* un Komisija attiecībā uz sakaru infrastruktūru pieņem vajadzīgos pasākumus, tostarp drošības plānu, lai:

- a) fiziski aizsargātu datus, tostarp izstrādājot ārkārtas rīcības plānus kritiskās infrastruktūras aizsardzībai;
- b) liegtu nepilnvarotām personām piekļuvi datu apstrādes iekārtām, ko izmanto personas datu apstrādei (piekļuves kontrole);
- c) nodrošinātu to, ka nepilnvarotas personas nelasa, nekopē, negroza vai nedzēš datu nesējus (datu nesēju kontrole);
- d) liegtu datu neatļautu ievadīšanu datubāzē, kā arī liegtu ievadīto personas datu neatļautu lasīšanu, grozīšanu vai dzēšanu (glabāšanas kontrole);
- e) nepieļautu to, ka nepilnvarotas personas lieto datu automatizētas apstrādes sistēmu ar datu pārraides ierīču palīdzību (lietošanas kontrole);
- f) nodrošinātu to, ka personām, kam ir pilnvaras lietot datu automatizētās apstrādes sistēmu, ir pieejami vienīgi tie dati, kuriem tām atļauts piekļūt, un ka šīs personas tiem piekļūst tikai ar individuālām un unikālām lietotāju identitātēm un konfidenciāliem piekļuves veidiem (datu pieejamības kontrole);
- g) izstrādātu profilus, raksturojot to personu funkcijas un pienākumus, kuras ir pilnvarotas piekļūt datiem vai datu apstrādes iekārtām, un pēc 45. pantā minētā Eiropas Datu aizsardzības uzraudzītāja lūguma šos profilus nekavējoties dara tam pieejamus (personālie profili);
- h) nodrošinātu to, ka var pārbaudīt un noteikt, kurām iestādēm personas datus var pārraidīt, izmantojot datu pārraides ierīces (datu pārraides kontrole);

▼B

- i) nodrošinātu to, ka vēlāk iespējams pārbaudīt un noteikt, kādi personas dati ir ievadīti automatizētā datu apstrādes sistēmā, kurā brīdī un kura persona tos ir ievadījusi (ievades kontrole);
 - j) nodrošinātu to, ka personas datu pārraides un datu nesēju pārsūtīšanas laikā nav iespējama datu neatļauta lasīšana, kopēšana, grozīšana vai dzēšana, jo īpaši ar attiecīgiem kodēšanas paņēmieniem (pārsūtīšanas kontrole);
 - k) uzraudzītu šajā punktā minētos drošības pasākumus un veiktu vajadzīgos organizatoriskos pasākumus saistībā ar iekšējo uzraudzību, lai nodrošinātu atbilstību šai regulai (paškontrole).
2. Pārvaldības iestāde veic 1. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz drošību saistībā ar papildinformācijas apmaiņu, izmantojot sakaru infrastruktūru.

*17. pants***Konfidencialitāte - pārvaldības iestāde**

1. Neskarot Eiropas Kopienų Civildienesta noteikumu 17. pantu, pārvaldības iestāde piemēro pienācīgus noteikumus par dienesta noslēpumu vai citas līdzvērtīgas prasības attiecībā uz konfidencialitāti visam iestādes personālam, kam jāstrādā ar SIS II datiem, atbilstīgi standartiem, kas pielīdzināmi šīs regulas 11. pantā paredzētajiem. Šis pienākums ir spēkā arī pēc tam, kad šīs personas vairs neieņem attiecīgo amatu vai netiek nodarbinātas vai kad šo struktūru darbība ir izbeigta.

2. Pārvaldības iestāde veic 1. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz konfidencialitāti saistībā ar papildinformācijas apmaiņu, izmantojot sakaru infrastruktūru.

▼M2

3. Ja pārvaldības iestāde jebkuru ar *SIS II* saistītu uzdevumu veikšanai sadarbojas ar ārējiem līgumslēdzējiem, tā rūpīgi uzrauga līgumslēdzēja darbības, lai nodrošinātu atbilstību visiem šīs regulas noteikumiem, jo īpaši attiecībā uz drošību, konfidencialitāti un datu aizsardzību.

4. *CS-SIS* darbības pārvaldību neztic privātiem uzņēmumiem vai privātām organizācijām.

▼B*18. pants***Reģistrēšana centrālā līmenī**

1. Pārvaldības iestāde nodrošina, ka 12. panta 1. un 2. punktā minētajiem mērķiem reģistrē katru piekļuvi *CS-SIS* saglabātajiem personas datiem un visas minēto datu apmaiņas.

▼B

2. Ierakstos konkrēti uzrāda brīdinājumu vēsturi, datu pārraides datumu un laiku, meklēšanā izmantotos datus, atsauci uz pārraidītajiem datiem, kā arī par datu apstrādi atbildīgās iestādes nosaukumu.

3. Ierakstus lieto vienīgi 1. punktā paredzētajā nolūkā un dzēš ne ātrāk kā pēc gada un ne vēlāk kā pēc trim gadiem no to izveides dienas. Ierakstus, kuros ietverta brīdinājumu vēsture, dzēš vienu līdz trīs gadus pēc brīdinājumu dzēšanas.

4. Ierakstus var saglabāt ilgāk, ja tie vajadzīgi uzraudzības procedūrām, kas jau ir iesāktas.

5. Kompetentajām iestādēm, kuru pienākumos ir pārbaudīt, vai meklēšana ir likumīga, uzraudzīt datu apstrādes likumību, veikt pašuzraudzību, nodrošināt CS-SIS pareizu darbību, datu integritāti un drošību, atbilstīgi to kompetencei un pēc to lūguma ir nodrošināta piekļuve šiem ierakstiem, lai tās varētu pildīt savus pienākumus.

*19. pants***Informācijas kampaņa**

Komisija sadarbībā ar valstu uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju līdz ar SIS II darbības sākšanu veic arī informācijas kampaņu, lai sabiedrību informētu par tās mērķiem, glabātajiem datiem, iestādēm, kam ir piekļuves tiesības, un personu tiesībām. Pārvaldības iestāde pēc tās izveides sadarbībā ar valsts uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju šādas kampaņas regulāri atkārti. Dalībvalstis sadarbībā ar savām valsts uzraudzības iestādēm izstrādā un īsteno vajadzīgo politiku, lai informētu savus iedzīvotājus par SIS II kopumā.

IV NODAĻA

BRĪDINĀJUMI PAR TREŠO VALSTU VALSTSPIEDERĪGAJIEM, LAI ATTEIKTU IECEĻOŠANU UN UZTURĒŠANOS*20. pants***Datu kategorijas**

1. Neskarot 8. panta 1. punktu vai šīs regulas noteikumus par papildu datu saglabāšanu, SIS II ir ietverti tikai to kategoriju dati, ko ir iesniegusi katra dalībvalsts un kas ir vajadzīgi 24. pantā noteiktajiem nolūkiem.

2. Informācija par personām, attiecībā uz kurām brīdinājums ir izdots, ir ne vairāk kā šādi dati:

▼ B

- a) uzvārds(-i) un vārds(-i), vārds(-i) piedzimstot un iepriekš lietoti vārdi un pseidonīmi, ko var ievadīt atsevišķi;
- b) īpašas fiziskās pazīmes, kas ir objektīvas un nemainīgas;
- c) dzimšanas vieta un datums;
- d) dzimums;
- e) fotogrāfijas;
- f) pirkstu nospiedumi;
- g) valstspiederība(s);
- h) norāde, vai attiecīgā persona ir bruņota, varmācīga vai izbēgusi;
- i) brīdinājuma iemesls;
- j) brīdinājuma izdevēja iestāde;
- k) norāde uz lēmumu, kas ir brīdinājuma pamatā;

▼ M2

- ka) nodarījuma veids;

▼ B

- l) veicamā rīcība;
- m) saite(s) ar citiem brīdinājumiem, kas izdoti SIS II saskaņā ar 37. pantu.

3. Tehniskos noteikumus, kas vajadzīgi, lai 2. punktā minētos datus ievadītu, atjauninātu un dzēstu un lai tajos veiktu meklēšanu, izstrādā saskaņā ar 51. panta 2. punktā minēto procedūru, neskarot instrumentu, ar ko izveido pārvaldības iestādi.

4. Tehniskie noteikumi, kas vajadzīgi, lai veiktu 2. punktā minēto datu meklēšanu, ir līdzīgi noteikumiem par meklēšanu CS-SIS, valstu eksemplāros un 31. panta 2. punktā minētajās tehniskajās kopijās.

*21. pants***Proporcionalitāte**

Pirms brīdinājuma izdošanas dalībvalstis nosaka, vai gadījums ir atbilstīgs, piemērots un pietiekami svarīgs, lai brīdinājums būtu jāievada SIS II.

▼ M2

Ja 24. panta 2. punktā minētais lēmums atteikt iecelšanu un uzturēšanos ir saistīts ar teroristu nodarījumu, konkrēto gadījumu uzskata par

▼ **M2**

atbilstīgu, piemērotu un pietiekami svarīgu, lai būtu brīdinājums *SIS II*. Sabiedriskās vai valsts drošības apsvērumu dēļ dalībvalstis var izņēmuma kārtā atturēties ievadīt brīdinājumu, ja tas varētu traucēt oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras.

22. pants

Īpaši noteikumi ievadīšanai, pārbaudei vai meklēšanai, izmantojot fotogrāfijas un pirkstu nospiedumus

1. Fotogrāfijas un pirkstu nospiedumus ievada tikai pēc īpašas kvalitātes pārbaudes, lai apstiprinātu, ka tie atbilst minimālajiem datu kvalitātes standartiem. Īpašās kvalitātes pārbaudes specifikāciju nosaka saskaņā ar 51. panta 2. punktā minēto procedūru.

2. Ja *SIS II* brīdinājumā ir pieejamas fotogrāfijas un pirkstu nospiedumu dati, tos izmanto, lai apstiprinātu tādas personas identitāti, kura atrasta *SIS II* burtparu meklēšanas rezultātā.

3. Lai identificētu personu, visos gadījumos var veikt meklēšanu pirkstu nospiedumu datos. Tomēr, ja personas identitāti nevar noskaidrot, izmantojot citus līdzekļus, personas identifikācijas nolūkos veic meklēšanu pirkstu nospiedumu datos. Minētajam nolūkam centrālā *SIS II* ietver automatizētu pirkstu nospiedumu identifikācijas sistēmu (*AFIS*).

4. Pirkstu nospiedumu datos *SIS II* saistībā ar brīdinājumiem, kuri ievadīti saskaņā ar 24. un 26. pantu, var meklēt arī, izmantojot pilnus vai nepilnus pirkstu nospiedumu komplektus, kas konstatēti izmeklējamu smagu noziegumu vai teroristu nodarījumu izdarīšanas vietās, ja ar augstu varbūtības pakāpi var konstatēt, ka minētie nospiedumu komplekti pieder nodarījuma izdarītājam un ar noteikumu, ka meklēšanu veic vienlaikus dalībvalsts attiecīgajās valstu pirkstu nospiedumu datubāzēs.

▼ **B**

23. pants

Prasība ievadīt brīdinājumu

1. Brīdinājumu nevar ievadīt, ja nav 20. panta 2. punkta a), d), k) un l) apakšpunktā minēto datu.

2. Ievada arī visus pārējos 20. panta 2. punktā minētos datus, tiklīdz tie ir pieejami.

24. pants

Nosacījumi brīdinājumu izdošanai, lai atteiktu ieceļošanu vai uzturēšanos

1. Datus par trešo valstu valstspiederīgajiem, par kuriem izdots brīdinājums, lai atteiktu ieceļošanu vai uzturēšanos, ievada, pamatojoties uz attiecīgās valsts brīdinājumu, kas izriet no kompetento administratīvo iestāžu vai tiesu lēmuma, kurš pieņemts saskaņā ar attiecīgās valsts tiesību aktos paredzētajiem procedūras noteikumiem. Šo lēmumu var pieņemt, tikai pamatojoties uz īpašu novērtējumu. Pārsūdzības attiecībā uz šiem lēmumiem iesniedz saskaņā ar attiecīgās valsts tiesību aktiem.

▼ **B**

2. Brīdinājumu izdod, ja 1. punktā minētā lēmuma pamatā ir draudi sabiedriskajai kārtībai vai sabiedrības drošībai, vai valsts drošībai, kurus var radīt attiecīgā trešās valsts valstspiederīgā atrašanās dalībvalsts teritorijā. Šāda situācija pastāv jo īpaši attiecībā uz:

- a) trešās valsts valstspiederīgo, kurš kādā dalībvalstī notiesāts par noziedzīgu nodarījumu, par ko paredzētais sods ir saistīts ar brīvības atņemšanu uz vismaz vienu gadu;
- b) trešās valsts valstspiederīgo, par kuru ir pamatots iemesls uzskatīt, ka viņš ir izdarījis smagu noziedzīgu nodarījumu, vai par kuru ir skaidras norādes par viņa nodomu izdarīt šādu noziedzīgu nodarījumu kādas dalībvalsts teritorijā.

3. Brīdinājumu var izdot arī tad, ja 1. punktā minētā lēmuma pamatā ir fakts, ka trešās valsts valstspiederīgajam ir piemērots jebkāds pasākums, kas saistīts ar izraidīšanu vai ieceļošanas atteikumu un kas nav atcelts vai atlikts, ietverot vai papildus piemērojot ieceļošanas aizliegumu vai, attiecīgā gadījumā, uzturēšanās aizliegumu, kas pamatots ar to, ka nav ievēroti attiecīgās valsts noteikumi par trešo valstu valstspiederīgo ieceļošanu vai uzturēšanos.

4. Šo pantu nepiemēro 26. pantā minētajām personām.

5. Trīs gadus pēc 55. panta 2. punktā minētās dienas Komisija pārskata šā panta piemērošanu. Pamatojoties uz minēto pārskatīšanu, Komisija, izmantojot iniciatīvas tiesības atbilstīgi Līgumam, iesniedz vajadzīgos priekšlikumus šā panta grozījumiem, lai panāktu brīdinājumu izdošanas kritēriju lielāku saskaņotību.

25. pants

Nosacījumi brīdinājumu ievadīšanai par trešo valstu valstspiederīgajiem, kuriem ir tiesības brīvi pārvietoties Kopienā

1. Brīdinājums attiecībā uz trešās valsts valstspiederīgo, kuram ir tiesības brīvi pārvietoties Kopienā, kā noteikts Eiropas Parlamenta un Padomes Direktīvā 2004/38/EK (2004. gada 29. aprīlis) par Savienības pilsoņu un viņu ģimenes locekļu tiesībām brīvi pārvietoties un uzturēties dalībvalstu teritorijā ⁽¹⁾, ir saskaņā ar noteikumiem, kas pieņemti, īstenojot minēto direktīvu.

2. Ja attiecībā uz trešās valsts valstspiederīgo, kuram ir tiesības brīvi pārvietoties Kopienā, ir saņemta pozitīva atbilde par brīdinājumu, kas ievadīts saskaņā ar 24. pantu, tad dalībvalsts, kas izpilda brīdinājumu, tūlīt konsultējas ar ievadītāju dalībvalsti, izmantojot savu *SIRENE* biroju un saskaņā ar *SIRENE* rokasgrāmatas noteikumiem, lai nekavējoties lemtu par veicamo rīcību.

⁽¹⁾ OV L 158, 30.4.2004., 77. lpp.

▼ **M2**

26. pants

Nosacījumi brīdinājumu ievadīšanai par trešo valstu valstspiederīgajiem, uz kuriem attiecas ierobežojoši pasākumi

1. Brīdinājumus par trešo valstu valstspiederīgajiem, uz kuriem attiecas ierobežojošs pasākums, kas saskaņā ar Padomes pieņemtajiem tiesību aktiem paredzēts, lai nepieļautu ieceļošanu dalībvalstu teritorijā vai tranzītu caur to, tostarp pasākumi, ar ko īsteno Apvienoto Nāciju Organizācijas Drošības padomes noteiktu ceļošanas aizliegumu, ievada *SIS II* nolūkā atteikt ieceļošanu un uzturēšanos tiktāl, ciktāl ir nodrošināta atbilstība datu kvalitātes prasībām.

2. Brīdinājumus ievada, atjaunina un dzēš tās dalībvalsts kompetentā iestāde, kura pasākuma pieņemšanas laikā ir Eiropas Savienības Padomes prezidentvalsts. Ja minētajai dalībvalstij nav piekļuves *SIS II* vai brīdinājumiem, kas ievadīti saskaņā ar šo regulu, atbildību uzņemas dalībvalsts, kas būs nākamā prezidentvalsts un kam ir piekļuve *SIS II*, tostarp piekļuve brīdinājumiem, kas ievadīti saskaņā ar šo regulu.

Dalībvalstis ievieš procedūras, kas vajadzīgas, lai ievadītu, atjauninātu un dzēstu šādus brīdinājumus.

▼ **B**

27. pants

Iestādes, kurām ir tiesības piekļūt brīdinājumiem

1. Piekļuve *SIS II* ievadītajiem datiem un tiesības veikt tiešu meklēšanu šajos datos vai *SIS II* datu eksemplārā ir vienīgi iestādēm, kas ir atbildīgas par trešo valstu valstspiederīgo identifikāciju, lai veiktu:

- a) robežkontroli saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 562/2006 (2006. gada 15. marts), ar kuru ievieš Kopienas Kodeksu par noteikumiem, kas reglamentē personu pārvietošanos pār robežām (Šengenas Robežu kodekss) ⁽¹⁾;
- b) citas attiecīgajā dalībvalstī veiktās policijas un muitas pārbaudes un lai norīkotās iestādes koordinētu šādas pārbaudes.

2. Tomēr tiesības piekļūt *SIS II* ievadītajiem datiem un tiesības veikt tiešu meklēšanu šajos datos var būt arī attiecīgās valsts tiesu iestādēm - tostarp tām, kuras ir atbildīgas par valsts apsūdzības celšanu krimināllietās un par tiesas izmeklēšanu pirms apsūdzības izvirzīšanas - pildot attiecīgās valsts tiesību aktos paredzētos uzdevumus, kā arī šādu iestāžu darbības koordinēšanas iestādēm.

3. Turklāt tiesības piekļūt *SIS II* ievadītajiem datiem un datiem, kuri attiecas uz dokumentiem saistībā ar personām un kuri ievadīti saskaņā ar ► **C1** Lēmuma 2007/533/TI ◀ 38. panta 2. punkta d) un e) apakšpunktū, un tiesības veikt tiešu meklēšanu šajos datos var izmantot iestādes, kas atbild par vīzu izsniegšanu, centrālās iestādes, kuras atbild par vīzu pieteikumu izskatīšanu, un iestādes, kas atbild par uzturēšanās atļauju

⁽¹⁾ OV L 105, 13.4.2006., 1. lpp.

▼ B

izsniegšanu un par tādu tiesību aktu administrēšanu, kuri attiecas uz trešo valstu valstspiederīgajiem, sakarā ar Kopienas *acquis* piemērošanu, kas attiecas uz personu pārvietošanos. Šo iestāžu piekļuvi datiem reglamentē katras dalībvalsts tiesību akti.

4. Šajā pantā minētās iestādes iekļauj 31. panta 8. punktā minētajā sarakstā.

▼ M2*27.a pants***Eiropola piekļuve SIS II datiem**

1. Eiropas Savienības Aģentūrai tiesībaizsardzības sadarbībai (Eiropolam), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/794 ⁽¹⁾, ja tas vajadzīgs tās pilnvaru izpildei, ir tiesības piekļūt *SIS II* datiem un meklēt tajos. Eiropols var arī veikt papildinformācijas apmaiņu un vēl lūgt sniegt papildinformāciju saskaņā ar *SIRENE* rokasgrāmatas noteikumiem.

2. Ja Eiropola veiktā meklēšanā konstatē, ka *SIS II* ir brīdinājums, Eiropols informē izdevēju dalībvalsti, ar komunikācijas infrastruktūras palīdzību veicot papildinformācijas apmaiņu un rīkojoties saskaņā ar *SIRENE* rokasgrāmatā paredzētajiem noteikumiem. Kamēr Eiropols vēl nevar izmantot papildinformācijas apmaiņai paredzētās funkcijas, tas informē izdevējas dalībvalstis, izmantojot kanālus, kas definēti Regulā (ES) 2016/794.

3. Eiropols papildinformāciju, ko tam sniegušas dalībvalstis, var apstrādāt salīdzināšanas ar tā datubāzēm un operatīvās analīzes projektiem nolūkā, kuras mērķis ir identificēt saiknes vai citu svarīgu saistību un veikt stratēģisko, tematisko vai operatīvo analīzi, kas minēta Regulas (ES) 2016/794 18. panta 2. punkta a), b) un c) apakšpunktā. Eiropols jebkādu papildinformācijas apstrādi šā panta nolūkā veic saskaņā ar minēto regulu.

4. *SIS II* meklēšanā vai papildinformācijas apstrādē iegūtās informācijas izmantošanai Eiropolam ir vajadzīga izdevējas dalībvalsts piekrišana. Ja dalībvalsts atļauj izmantot šādu informāciju, Eiropola darbības ar to reglamentē Regula (ES) 2016/794. Eiropols šādu informāciju sniedz trešām valstīm un trešām struktūrām vienīgi ar izdevējas dalībvalsts piekrišanu un pilnībā ievērojot Savienības tiesību aktus datu aizsardzības jomā.

⁽¹⁾ Eiropas Parlamenta un Padomes Regula (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI (OV L 135, 24.5.2016., 53. lpp.).

▼ M2

5. Eiropols:
- a) neskarot 4. un 6. punktu, nepievieno *SIS II* daļas un nepārsūta tur esošos datus, kuriem tas var piekļūt, nevienai datu vākšanas un apstrādes sistēmai, ko ekspluatē Eiropols vai kas tiek ekspluatētas Eiropolā, kā arī neveic nekādu *SIS II* daļu lejupielādi vai citādu kopēšanu;
 - b) neatkarīgi no Regulas (ES) 2016/794 31. panta 1. punkta dzēš papildinformāciju, kas satur personas datus, ne vēlāk kā vienu gadu pēc saistītā brīdinājuma dzēšanas. Atkāpjoties no šā noteikuma, ja Eiropolam tā datubāzēs vai operatīvās analīzes projektos ir informācija par gadījumu, uz kuru attiecas papildinformācija, lai Eiropols varētu veikt savus uzdevumus, Eiropols – vajadzības gadījumā – izņēmuma kārtā var turpināt glabāt papildinformāciju. Eiropols informē izdevēju un izpildītāju dalībvalsti par šādas papildinformācijas turpinātu glabāšanu un sniedz tam pamatojumu;
 - c) tiesības piekļūt *SIS II* datiem, tostarp papildinformācijai, nodrošina vienīgi īpaši pilnvaroti Eiropola darbinieki, kuriem piekļuve šādiem datiem nepieciešama viņu pienākumu pildīšanai;
 - d) pieņem un piemēro pasākumus ar mērķi nodrošināt drošību, konfidencialitāti un pašuzraudzību saskaņā ar 10., 11. un 13. pantu;
 - e) nodrošina, ka darbinieki, kam ir tiesības apstrādāt *SIS II* datus, tiek pienācīgi apmācīti un saņem informāciju saskaņā ar 14. panta 1. punktu; un
 - f) neskarot Regulu (ES) 2016/794, ļauj Eiropas Datu aizsardzības uzraudzītājam uzraudzīt un pārskatīt Eiropola darbības, ko tas veic, īstenojot tiesības piekļūt *SIS II* datiem un meklēt tajos, un to, kā tas veic papildinformācijas apmaiņu un apstrādi.
6. Eiropols datus no *SIS II* kopē vienīgi tehniskos nolūkos, ja šāda kopēšana ir vajadzīga, lai pienācīgi pilnvaroti Eiropola darbinieki varētu veikt tiešu meklēšanu šajos datos. Šādām kopijām piemēro šo regulu. Tehnisko kopiju izmanto vienīgi tam, lai saglabātu *SIS II* datus, kamēr tajos notiek meklēšana. Tiklīdz meklēšana ir pabeigta, datus dzēš. Šādu izmantošanu neuzskata par *SIS II* datu nelikumīgu lejupielādi vai kopēšanu. Eiropols nekopē brīdinājumu datus vai papildu datus, ko izdevušas dalībvalstis, vai no *CS-SIS II* citās Eiropola sistēmās.
7. Lai pārbaudītu datu apstrādes likumību, veiktu pašuzraudzību un nodrošinātu datu pienācīgu drošību un integritāti, Eiropols saglabā reģistra ierakstus par katru piekļuvi un meklēšanu *SIS II* saskaņā ar 12. panta noteikumiem. Šādus reģistra ierakstus un dokumentus neuzskata par *SIS II* daļu nelikumīgu lejupielādi vai kopēšanu.

▼ M2

8. Dalībvalstis papildinformācijas apmaiņas ceļā informē Eiropolu par jebkādu informācijas atbilstīgu saistību ar brīdinājumiem, kas saistīti ar teroristu nodarījumiem. Izņēmuma kārtā dalībvalstis var neinformēt Eiropolu, ja tas apdraudētu patlaban notiekošu izmeklēšanu, kādas personas drošību vai ja tas būtu pretrunā izdevējas dalībvalsts būtiskām drošības interesēm.

9. Šā panta 8. punktu piemēro no dienas, kad Eiropols var saņemt papildinformāciju saskaņā ar 1. punktu.

27.b pants

Piekluve *SIS II* datiem, ko piešķir Eiropas Robežu un krasta apsardzes vienībām, tāda personāla vienībām, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, un migrācijas pārvaldības atbalsta vienībām

1. Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2016/1624 ⁽¹⁾ 40. panta 8. punktu minētās regulas 2. panta 8) un 9) punktā minēto vienību dalībniekiem atbilstīgi to pilnvarām un ar noteikumu, ka tie ir pilnvaroti veikt pārbaudes saskaņā ar šīs regulas 27. panta 1. punktu un tiem ir nodrošināta prasītā apmācība saskaņā ar šīs regulas 14. pantu, ir tiesības piekļūt *SIS II* datiem un meklēt tajos, ciktāl tas ir nepieciešams viņu pienākumu pildīšanai un ciktāl to prasa konkrētās operācijas operatīvais plāns. Pieklūvi *SIS II* datiem neattiecina uz citiem vienības dalībniekiem.

2. Šā panta 1. punktā minētie vienību dalībnieki īsteno tiesības piekļūt *SIS II* datiem un meklēt tajos saskaņā ar 1. punktu, izmantojot tehnisko saskarni. Tehnisko saskarni izveido un uztur Eiropas Robežu un krasta apsardzes aģentūra un tā ļauj nodrošināt tiešu savienojumu ar centrālo *SIS II*.

3. Ja šā panta 1. punktā minētā vienību dalībnieka veiktā meklēšanā tiek konstatēts brīdinājums *SIS II*, par to informē izdevēju dalībvalsti. Saskaņā ar Regulas (ES) 2016/1624 40. pantu vienību dalībnieki saistībā ar brīdinājumu *SIS II* rīkojas tikai saskaņā ar uzņēmējas dalībvalsts, kurā tie darbojas, robežsargu vai ar atgriešanu saistītu uzdevumu izpildē iesaistīto darbinieku norādījumiem un parasti tikai viņu klātbūtnē. Uzņēmēja dalībvalsts var vienību dalībniekus pilnvarot rīkoties tās vārdā.

4. Lai pārbaudītu datu apstrādes likumību, veiktu pašuzraudzību un nodrošinātu datu pienācīgu drošību un integritāti, Eiropas Robežu un krasta apsardzes aģentūra saglabā reģistra ierakstus par katru pieklūvi un meklēšanu *SIS II* saskaņā ar 12. panta noteikumiem.

⁽¹⁾ Eiropas Parlamenta un Padomes Regula (ES) 2016/1624 (2016. gada 14. septembris) par Eiropas Robežu un krasta apsardzi un ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) 2016/399 un ar ko atceļ Eiropas Parlamenta un Padomes Regulu (EK) Nr. 863/2007, Padomes Regulu (EK) Nr. 2007/2004 un Padomes Lēmumu 2005/267/EK (OV L 251, 16.9.2016., 1. lpp.).

▼ **M2**

5. Eiropas Robežu un krasta apsardzes aģentūra pieņem un piemēro pasākumus ar mērķi nodrošināt drošību, konfidencialitāti un pašuzraudzību saskaņā ar 10., 11. un 13. pantu un nodrošina, ka šā panta 1. punktā minētās vienības piemēro minētos pasākumus.

6. Neko šajā pantā neinterpretē kā tādu, kas ietekmētu Regulas (ES) 2016/1624 noteikumus par datu aizsardzību vai Eiropas Robežu un krasta apsardzes aģentūras atbildību par jebkādu neatļautu vai nepareizu datu apstrādi, ko tā veic.

7. Neskarot 2. punktu, nevienu *SIS II* daļu nepievieno nevienai datu vākšanas un apstrādes sistēmai, ko ekspluatē 1. punktā minētās vienības vai Eiropas Robežu un krasta apsardzes aģentūra, un *SIS II* datus, kuriem minētajām vienībām ir piekļuve, nenosūta nevienai šādi sistēmai. *SIS II* daļas netiek lejupielādētas vai kopētas. Reģistra ierakstu par piekļuvi un meklēšanu saglabāšanu neuzskata par *SIS II* datu nelikumīgu lejupielādi vai kopēšanu.

8. Eiropas Robežu un krasta apsardzes aģentūra ļauj Eiropas Datu aizsardzības uzraudzītājam uzraudzīt un pārskatīt šajā pantā minēto vienību darbības, ko tās veic, īstenojot savas tiesības piekļūt *SIS II* datiem un meklēt tajos. Tas neskar turpmākos noteikumus Eiropas Parlamenta un Padomes Regulā (ES) 2018/1725 ⁽¹⁾.

▼ **B***28. pants***Piekļuves ierobežojumi**

Lietotāji drīkst piekļūt vienīgi tiem datiem, kas ir vajadzīgi attiecīgo lietotāju uzdevumu izpildei.

*29. pants***Brīdinājumu saglabāšanas laiks**

1. Saskaņā ar šo regulu *SIS II* ievadītos brīdinājumus saglabā vienīgi tik ilgi, cik vajadzīgs, lai sasniegtu mērķus, kādiem tie ievadīti.

2. Dalībvalsts, kas izdod šādu brīdinājumu, trīs gados pēc tā ievadīšanas *SIS II* izvērtē vajadzību to saglabāt.

3. Ikviena dalībvalsts vajadzības gadījumā saskaņā ar saviem tiesību aktiem nosaka īsākus izvērtēšanas termiņus.

4. Izvērtēšanas termiņā brīdinājuma izdevēja dalībvalsts pēc visaptveroša individuāla novērtējuma, ko dokumentē, var pieņemt lēmumu brīdinājumu saglabāt ilgāk, ja tas ir vajadzīgs nolūkos, kuru dēļ brīdinājums izdots. Šādā gadījumā 2. punkts attiecas arī uz termiņa pagarinājumu. Par brīdinājuma termiņa pagarināšanu paziņo CS-SIS.

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

▼B

5. Brīdinājumus automātiski dzēš, tiklīdz beidzas 2. punktā minētais izvērtēšanas termiņš, izņemot gadījumu, kad brīdinājuma izdevēja dalībvalsts saskaņā ar 4. punktu ir paziņojusi CS-SIS par brīdinājuma termiņa pagarināšanu. CS-SIS četrus mēnešus iepriekš automātiski informē dalībvalstis par paredzamo datu dzēšanu sistēmā.

6. Dalībvalstis glabā statistiku par to brīdinājumu skaitu, kuru saglabāšanas termiņš ir pagarināts saskaņā ar 4.punktu.

*30. pants***Pilsonības iegūšana un brīdinājumi**

Brīdinājumus par personu, kas ieguvusi tādas valsts pilsonību, kuras pilsoņiem ir tiesības brīvi pārvietoties Kopienā, dzēš, tiklīdz brīdinājuma izdevēja dalībvalsts uzzina vai tiek informēta saskaņā ar 34. pantu, ka attiecīgā persona ieguvusi šādu pilsonību.

V NODAĻA

VISPĀRĪGIE DATU APSTRĀDES NOTEIKUMI*31. pants***SIS II datu apstrāde**

1. Dalībvalstis 20. pantā minētos datus var apstrādāt, lai atteiktu iecelošanu vai uzturēšanos savā teritorijā.

2. Datus var kopēt vienīgi tehniskos nolūkos, ja šāda kopēšana ir vajadzīga, lai 27. pantā minētās iestādes varētu veikt tiešu meklēšanu šajos datos. Uz šādām kopijām attiecas šī regula. Vienas dalībvalsts izdotus brīdinājumus nedrīkst pārkopēt no šīs valsts N. SIS II uz citām valsts datu datnēm.

3. Šā panta 2. punktā minētās tehniskās kopijas, kuru rezultātā veidojas datubāze, kas nav tiešaistē, drīkst saglabāt laiku, ka nav ilgāks par 48 stundām. Ārkārtas situācijās šo laiku var pagarināt līdz ārkārtas situācijas beigām.

Neskarot šā punkta pirmo daļu, tehniskās kopijas, kuru rezultātā veidojas datubāze, kas nav tiešaistē un ko izmanto vīzu izsniegšanas iestādes, vairs nav atļautas vienu gadu pēc tam, kad attiecīgā iestāde ir sekmīgi pievienojusies Kopienas Vīzu informācijas sistēmas sakaru infrastruktūrai, kas paredzama turpmākā regulā par Vīzu informācijas sistēmu (VIS) un par datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām; tas neattiecas uz kopijām, kas veidotas lietošanai ārkārtas situācijās pēc tam, kad tikls nav bijis pieejams vairāk nekā 24 stundas.

Dalībvalstis uztur šādu kopiju pastāvīgi atjauninātu uzskaitījumu, šo uzskaitījumu dara pieejamu attiecīgās valsts uzraudzības iestādei un nodrošina, ka attiecībā uz šīm kopijām piemēro šo regulu, jo īpaši tās 10. pantu.

▼B

4. Piekļuvi šādiem datiem atļauj vienīgi saskaņā ar 27. pantā minēto attiecīgo valstu iestāžu kompetenci un vienīgi attiecīgi pilnvarotam personālam.

5. Datus nedrīkst izmantot administratīviem nolūkiem. Izņēmuma kārtā datus, kas ievadīti saskaņā ar šo regulu, savu uzdevumu pildīšanai var lietot 27. panta 3. punktā minētās iestādes saskaņā ar katras dalībvalsts tiesību aktiem.

6. Saskaņā ar šīs regulas 24. pantu ievadītos datus un datus, kuri attiecas uz dokumentiem saistībā ar personām un kuri ievadīti saskaņā ar ►C1 Lēmuma 2007/533/TI ◀ 38. panta 2. punkta d) un e) apakšpunktu, saskaņā ar katras dalībvalsts tiesību aktiem var izmantot šīs regulas 27. panta 3. punkta nolūkos.

7. Datu izmantošanu, kura neatbilst 1. līdz 6. punktam, uzskata par nelikumīgu izmantošanu atbilstīgi katras dalībvalsts tiesību aktiem.

8. Katra dalībvalsts nosūta pārvaldības iestādei to kompetento iestāžu sarakstu, kurām saskaņā ar šo regulu ir atļauts tieši veikt meklēšanu SIS II ievadītajos datos, kā arī jebkuras izmaiņas minētajā sarakstā. Minētajā sarakstā attiecībā uz katru iestādi norāda, kuros datos un kādos nolūkos tās drīkst veikt meklēšanu. Pārvaldības iestāde nodrošina saraksta gadskārtēju publicēšanu *Eiropas Savienības Oficiālajā Vēstnesī*.

9. Ja vien Kopienas tiesību aktos nav paredzēti īpaši noteikumi, tad attiecīgās valsts N. SIS II ievadītajiem datiem piemēro attiecīgās dalībvalsts tiesību aktus.

*32. pants***SIS II dati un valstu datnes**

1. Šīs regulas 31. panta 2. punkts neskar dalībvalsts tiesības savās datnēs saglabāt SIS II datus, saistībā ar kuriem tās teritorijā ir veiktas darbības. Tādus datus valstu datnēs saglabā ne ilgāk kā trīs gadus, izņemot gadījumus, kad attiecīgās valsts īpašos tiesību aktos nav paredzēts ilgāks saglabāšanas termiņš.

2. Šīs regulas 31. panta 2. punkts neskar dalībvalstu tiesības savās datnēs saglabāt datus par konkrētu brīdinājumu, ko šī dalībvalsts ir izdevusi SIS II.

*33. pants***Informācija brīdinājuma neizpildes gadījumā**

Ja pieprasīto rīcību nevar veikt, brīdinājuma saņēmēja dalībvalsts nekaļējoties informē brīdinājuma izdevēju dalībvalsti.

▼B*34. pants***SIS II apstrādāto datu kvalitāte**

1. Brīdinājuma izdevēja dalībvalsts ir atbildīga par to, lai dati būtu precīzi, nebūtu novecojuši un būtu likumīgi ievadīti SIS II.
2. Vienīgi brīdinājuma izdevēja dalībvalsts ir tiesīga grozīt, papildināt, labot, atjaunināt vai dzēst ievadītos datus.
3. Ja dalībvalstij, kura nav brīdinājuma izdevēja dalībvalsts, ir pierādījumi par to, ka datos ir faktu kļūda vai ka dati saglabāti nelikumīgi, tad attiecīgā valsts iespējami drīz, bet ne vēlāk kā desmit dienās pēc tam, kad tai kļuvis zināms minētais pierādījums, apmainoties ar papildinformāciju, par to informē brīdinājuma izdevēja dalībvalsti. Brīdinājuma izdevēja dalībvalsts pārbauda šo informāciju un vajadzības gadījumā attiecīgo ierakstu nekavējoties labo vai dzēš.
4. Ja dalībvalstis divos mēnešos nespēj vienoties, tad dalībvalsts, kura nav izdevusi brīdinājumu, jautājumu nodod Eiropas Datu aizsardzības uzraudzītājam, kas kopā ar attiecīgajām valstu uzraudzības iestādēm darbojas kā starpnieks.
5. Dalībvalstis apmainās ar papildinformāciju, ja persona iesniedz pretenziju, ka nav tā persona, par kuru izdots brīdinājums. Ja pārbaudē konstatē, ka tās tiešām ir divas dažādas personas, pretenzijas iesniedzēju informē par 36. pantā minētajiem noteikumiem.
6. Ja par kādu personu SIS II jau ir ievadīts brīdinājums, tad dalībvalsts, kura datubāzē ievada jaunu brīdinājumu, par brīdinājuma ievadīšanu vienojas ar dalībvalsti, kas ievadījusi pirmo brīdinājumu. Vienošanās notiek, veicot papildinformācijas apmaiņu.

*35. pants***Personu ar līdzīgām īpašībām atšķiršana**

Ja, ievadot jaunu brīdinājumu, konstatē, ka SIS II jau ir dati par personu ar tādu pašu identitātes apraksta elementu, piemēro šādu procedūru:

- a) *SIRENE* birojs sazinās ar lūguma iesniedzēju iestādi, lai noskaidrotu, vai brīdinājums attiecas uz vienu un to pašu personu;

▼B

- b) ja dažādu avotu pārbaudē atklājas, ka jaunā brīdinājuma subjekts un persona, kas jau norādīta SIS II, patiešām ir viena un tā pati persona, *SIRENE* birojs piemēro 34. panta 6. punktā minēto procedūru vairāku brīdinājumu ievadīšanai. Ja pārbaudē atklājas, ka tās ir divas dažādas personas, *SIRENE* birojs apstiprina lūgumu ievadīt otro brīdinājumu, pievienojot vajadzīgos elementus, lai novērstu nepareizu identifikāciju.

*36. pants***Papildu dati, ko izmanto attiecībā uz ļaunprātīgi izmantotu identitāti**

1. Ja personu, uz kuru faktiski attiecas brīdinājums, var sajaukt ar personu, kuras identitāte ir izmantota ļaunprātīgi, brīdinājuma ievadītāja dalībvalsts ar minētās personas skaidri izteiktu piekrišanu brīdinājumam pievieno datus par pēdējo minēto personu, lai izvairītos no nepareizas identifikācijas negatīvām sekām.

2. Datus par personu, kuras identitāte ir izmantota ļaunprātīgi, izmanto vienīgi šādos nolūkos:

- a) lai ļautu kompetentajai iestādei atšķirt personu, kuras identitāte ir izmantota ļaunprātīgi, no personas, uz kuru faktiski attiecas brīdinājums;
- b) lai personai, kuras identitāte ir izmantota ļaunprātīgi, ļautu konstatēt, ka tās identitāte ir izmantota ļaunprātīgi, un pierādīt savu īsto identitāti.

3. Šā panta nolūkiem SIS II drīkst ievadīt un turpmāk apstrādāt vienīgi šādus personas datus:

- a) uzvārds(-i) un vārds(-i), vārds(-i) piedzimstot un iepriekš lietoti vārdi un pseidonīmi, ko var ievadīt atsevišķi;
- b) īpašas fiziskas pazīmes, kas ir objektīvas un nemainīgas;
- c) dzimšanas vieta un datums;
- d) dzimums;
- e) fotogrāfijas;
- f) pirkstu nospiedumi;
- g) valstspiederība(s);
- h) personas dokumenta(-u) numurs(-i) un izdošanas datums(-i).

▼B

4. Tehniskus noteikumus, kas vajadzīgi 3. punktā minēto datu ievadīšanai un turpmākai apstrādei, paredz saskaņā ar 51. panta 2. punktā minēto procedūru, neskarot instrumentu, ar ko izveido pārvaldības iestādi.

5. Šā panta 3. punktā minētos datus dzēs vienlaikus ar attiecīgo brīdinājumu vai agrāk, ja attiecīgā persona to lūdz.

6. Šā panta 3. punktā minētajiem datiem var piekļūt vienīgi iestādes, kurām ir tiesības piekļūt attiecīgajam brīdinājumam. Minētās iestādes to var darīt vienīgi tādēļ, lai novērstu nepareizu identifikāciju.

*37. pants***Brīdinājumu sasaiste**

1. Jebkura dalībvalsts var veikt to brīdinājumu sasaisti, kurus tā ievada SIS II. Šāda sasaiste nodrošina divu vai vairāk brīdinājumu savstarpēju saistību.

2. Sasaistes izveidošana neietekmē nedz konkrētas darbības, kas jāveic saskaņā ar katru no sasaistītajiem brīdinājumiem, nedz katra saistītā brīdinājuma saglabāšanas termiņu.

3. Sasaistes izveidošana neietekmē šajā regulā paredzētās piekļuves tiesības. Iestādēm, kurām nav tiesību piekļūt noteiktu kategoriju brīdinājumiem, nav iespējas skatīt sasaisti ar brīdinājumu, kuram tām nav piekļuves.

4. Dalībvalsts veic brīdinājumu sasaisti vienīgi tad, ja ir skaidra operatīva vajadzība.

5. Dalībvalsts var veikt brīdinājumu sasaisti saskaņā ar saviem tiesību aktiem ar nosacījumu, ka ir ievēroti šajā pantā izklāstītie principi.

6. Ja dalībvalsts uzskata, ka citas dalībvalsts veikta brīdinājumu sasaiste ir pretrunā tās tiesību aktiem vai starptautiskām saistībām, tā var veikt vajadzīgos pasākumus, lai nodrošinātu, ka sasaistei nevar piekļūt no attiecīgās valsts teritorijas vai arī ka tai nevar piekļūt šīs valsts iestādes, kuras atrodas ārpus tās teritorijas.

7. Tehniskos noteikumus par brīdinājumu sasaisti pieņem saskaņā ar 51. panta 2. punktā minēto procedūru, neskarot instrumentu, ar ko izveido pārvaldības iestādi.

▼B*38. pants***Papildinformācijas nolūks un saglabāšanas termiņš**

1. Lai atbalstītu papildinformācijas apmaiņu, dalībvalstis saglabā atsauci uz lēmumiem, pamatojoties uz kuriem *SIRENE* birojs ir ievadījis brīdinājumu.

2. Personas datus, kas *SIRENE* biroja datnēs glabājas pēc informācijas apmaiņas, saglabā vienīgi tik ilgi, cik vajadzīgs, lai sasniegtu mērķus, kādiem attiecīgie dati sniegti. Tos noteikti dzēs ne vēlāk kā vienu gadu pēc tam, kad no SIS II ir dzēsts attiecīgais brīdinājums.

3. Šā panta 2. punkts neskar dalībvalsts tiesības savās datnēs saglabāt datus, kas attiecas uz konkrētu šīs dalībvalsts izdotu brīdinājumu vai uz brīdinājumu, saistībā ar kuru tās teritorijā ir veikta darbība. Laiku, cik ilgi ir atļauts datnēs glabāt šādus datus, reglamentē attiecīgās valsts tiesību akti.

*39. pants***Personas datu nodošana trešām personām**

Datus, kas atbilstīgi šai regulai apstrādāti SIS II, nenodod un nedara pieejamus trešām valstīm vai starptautiskām organizācijām.

VI NODAĻA

DATU AIZSARDZĪBA*40. pants***Īpašu kategoriju datu apstrāde**

Ir aizliegts apstrādāt to kategoriju datus, kuras uzskaitītas Direktīvas 95/46/EK 8. panta 1. punktā.

*41. pants***Tiesības uz piekļuvi, neprecīzu datu labošanu un nelikumīgi glabātu datu dzēšanu**

1. Personu tiesības piekļūt datiem, kas uz šīm personām attiecas un kas ir ievadīti SIS II saskaņā ar šo regulu, īsteno saskaņā ar tās dalībvalsts tiesību aktiem, kurā attiecīgās personas atsauca uz minētajām tiesībām.

▼B

2. Ja attiecīgas valsts tiesību akti to paredz, valsts uzraudzības iestāde pieņem lēmumu par to, vai un kādā kārtībā informācija ir jādara zināma.
3. Dalībvalsts, kas nav brīdinājuma izdevēja dalībvalsts, informāciju par šādiem datiem var darīt zināmu vienīgi tad, ja tā iepriekš ir devusi iespēju brīdinājuma izdevējai dalībvalstij darīt zināmu savu nostāju. To dara, apmainoties ar papildinformāciju.
4. Datu subjektam informāciju nedara zināmu, ja tas ir noteikti nepieciešams, pildot likumīgu pienākumu sakarā ar brīdinājumu vai sargājot trešo personu tiesības un brīvības.
5. Ikvienai personai ir tiesības uz to, ka tiek dzēsti uz šo personu attiecīgi dati, kuros ir faktu kļūda vai kuri saglabāti nelikumīgi.
6. Attiecīgo personu informē, tiklīdz iespējams, bet jebkurā gadījumā ne vēlāk kā 60 dienās pēc dienas, kad persona iesniegusi pieteikumu piekļuves saņemšanai, vai agrāk, ja to paredz attiecīgās valsts tiesību akti.
7. Tiklīdz iespējams, bet jebkurā gadījumā ne vēlāk kā trīs mēnešus pēc dienas, kad persona iesniegusi pieteikumu par datu labošanu vai dzēšanu, vai agrāk, ja to paredz attiecīgās valsts tiesību akti, attiecīgo personu informē par pasākumiem, kas veikti, īstenojot personas tiesības attiecībā uz datu labošanu un dzēšanu

*42. pants***Tiesības uz informāciju**

1. Trešo valstu valstspiederīgos, par ko saskaņā ar šo regulu izdots brīdinājums, informē saskaņā ar Direktīvas 95/46/EK 10. un 11. pantu. Šo informāciju sniedz rakstiski, pievienojot kopiju lēmumam, kas ir brīdinājuma pamatā, kā minēts 24. panta 1. punktā, vai atsauci uz minēto lēmumu.
2. Šo informāciju noteikti nesniedz:
 - a) ja:
 - i) no attiecīgā trešās valsts valstspiederīgā nav iegūti personas dati;
 - un
 - ii) informācijas sniegšana nav iespējama, vai tā ir saistīta ar nesamērīgu piepūli;
- b) ja attiecīgajam trešās valsts valstspiederīgajam jau ir šī informācija;

▼B

- c) ja attiecīgās valsts tiesību aktos ir atļauti ierobežojumi tiesībām uz informāciju, jo īpaši nolūkā garantēt valsts drošību, aizsardzību, sabiedrības drošību, kā arī nolūkā novērst, izmeklēt un atklāt noziedzīgus nodarījumus, un sodīt par tiem.

*43. pants***Tiesiskās aizsardzības līdzekļi**

1. Ikviens persona var vērsties tiesā vai saskaņā ar attiecīgās dalībvalsts tiesību aktiem kompetentā iestādē, lai sadarā ar brīdinājumu, kas attiecas uz konkrēto personu, iegūtu piekļuvi informācijai, labotu, dzēstu vai iegūtu to vai saņemtu kompensāciju.
2. Neskarot 48. pantu, dalībvalstis savstarpēji apņemas īstenot galīgos lēmumus, ko pieņem tiesa vai 1. punktā minētās iestādes.
3. Komisija ►C1 līdz 2009. gada 17. janvārim ◀ izvērtē šajā pantā paredzētos noteikumus par tiesiskās aizsardzības līdzekļiem.

*44. pants***N. SIS II uzraudzība**

1. Katrā dalībvalstī norīkotā iestāde vai iestādes, kam piešķirtas Direktīvas 95/46/EK 28. pantā minētās pilnvaras, ("attiecīgās valsts uzraudzības iestāde") neatkarīgi uzrauga, cik likumīgi SIS II notiek personas datu apstrāde attiecīgās valsts teritorijā un to nosūtīšana no attiecīgās valsts teritorijas, kā arī papildinformācijas apmaiņa un turpmākā apstrāde.
2. Attiecīgās valsts uzraudzības iestāde nodrošina, ka vismaz reizi četros gados tiek veikta attiecīgās valsts N. SIS II veikto datu apstrādes operāciju revīzija saskaņā ar starptautiskiem revīzijas standartiem.
3. Dalībvalstis nodrošina, ka to valstu uzraudzības iestādēm ir pietiekami resursi, lai pildītu ar šo regulu noteiktos uzdevumus.

*45. pants***Pārvaldības iestādes uzraudzība**

1. Eiropas Datu aizsardzības uzraudzītājs pārbauda, vai pārvaldības iestāde veic personas datu apstrādi saskaņā ar šo regulu. Attiecīgi

▼B

piemēro Regulas (EK) Nr. 45/2001 46. un 47. pantā minētos pienākumus un pilnvaras.

2. Eiropas Datu aizsardzības uzraudzītājs nodrošina, ka vismaz reizi četros gados tiek veikta pārvaldības iestādes veikto personas datu apstrādes operāciju revīzija saskaņā ar starptautiskiem revīzijas standartiem. Šādas revīzijas ziņojumu nosūta Eiropas Parlamentam, Padomei, pārvaldības iestādei, Komisijai un valstu uzraudzības iestādēm. Pirms ziņojuma pieņemšanas pārvaldības iestādei dod iespēju izteikt savus apsvērumus.

*46. pants***Sadarbība starp valstu uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju**

1. Attiecīgo valstu uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs, rīkojoties saskaņā ar savām attiecīgajām pilnvarām, aktīvi sadarbojas, pildot savus pienākumus, un nodrošina koordinētu SIS II uzraudzību.

2. Attiecīgo valstu uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs, rīkojoties saskaņā ar savām attiecīgajām pilnvarām, apmainās ar svarīgu informāciju, palīdz cits citam veikt revīzijas un pārbaudes, izskata šīs regulas interpretācijas vai piemērošanas grūtības, analizē problēmas, ko rada neatkarīga uzraudzība vai datu subjektu tiesību īstenošana, sagatavo saskaņotus priekšlikumus, meklējot kopīgus risinājumus visām problēmām, un pēc vajadzības palīdz apzināt datu aizsardzības tiesības.

3. Šai nolūkā attiecīgo valstu uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs tiekas vismaz divreiz gadā. Šādu sanāksmju un ar tām saistītu pakalpojumu izmaksas sedz Eiropas Datu aizsardzības uzraudzītājs. Pirmajā sanāksmē pieņem reglamentu. Pēc vajadzības kopīgi izstrādā pārējās darba metodes. Eiropas Parlamentam, Padomei, Komisijai un pārvaldības iestādei reizi divos gados nosūta kopīgu darbības pārskatu.

*47. pants***Datu aizsardzība pārejas posmā**

Ja pārejas posmā Komisija tai uzticētos pienākumus deleģē citai struktūrai saskaņā ar 15. panta 4. punktu, tā nodrošina, lai Eiropas Datu aizsardzības uzraudzītājam būtu tiesības un iespējas pilnībā veikt uzticētos uzdevumus, tostarp veikt pārbaudes uz vietas un īstenot visas citas pilnvaras, kas Eiropas Datu aizsardzības uzraudzītājam uzticētas ar Regulas (EK) Nr. 45/2001 47. pantu.



VII NODAĻA
ATBILDĪBA UN SANKCIJAS

48. pants

Atbildība

1. Katra dalībvalsts saskaņā ar saviem tiesību aktiem ir atbildīga par jebkuru kaitējumu personai, kas radies, izmantojot N. SIS II. Tas attiecas arī uz kaitējumu, ko radījusi brīdinājuma izdevēja dalībvalsts, ja tā ievadījusi datus ar faktu kļūdām vai datus saglabājusi nelikumīgi.

2. Ja dalībvalsts, pret kuru ceļ prasību, nav brīdinājuma izdevēja dalībvalsts, tad brīdinājuma izdevējai dalībvalstij pēc pieprasījuma ir jāatmaksā naudas summas, kas izmaksātas kā kompensācija, ja vien dalībvalsts, kura lūdz kompensāciju, nav pārkāpusi šo regulu, izmantojot datus.

3. Ja tas, ka dalībvalsts neievēro šīs regulas uzliktos pienākumus, rada kaitējumu SIS II, kaitējumā vainojamo dalībvalsti sauc pie atbildības par kaitējumu, ja vien un ciktāl pārvaldības iestāde vai cita dalībvalsts, kas piedalās SIS II, nav veikusi(-šas) pienācīgus pasākumus, lai novērstu kaitējumu vai mazinātu tā ietekmi.

49. pants

Sankcijas

Dalībvalstis nodrošina, ka par SIS II datu ļaunprātīgu izmantošanu vai jebkuru papildinformācijas apmaiņu, kas ir pretrunā šai regulai, piemēro efektīvas, samērīgas un preventīvas sankcijas saskaņā ar attiecīgās valsts tiesību aktiem.

VIII NODAĻA
NOBEIGUMA NOTEIKUMI

50. pants

Uzraudzība un statistika

1. Pārvaldības iestāde nodrošina to procedūru ieviešanu, ar kuru palīdzību uzrauga SIS II darbības atbilstību sistēmas izveides mērķiem saistībā ar darbības efektivitāti, izmaksu lietderīgumu, drošību un pakalpojumu kvalitāti.

2. Tehniskās uzturēšanas, ziņošanas un statistikas nolūkos pārvaldības iestādei ir piekļuve vajadzīgajai informācijai, kas attiecas uz apstrādes darbībām, kuras veic centrālā SIS II.

3. Katru gadu pārvaldības iestāde publicē statistiku, norādot ierakstu skaitu pa brīdinājumu kategorijām, saņemto pozitīvu atbilžu skaitu pa

▼B

brīdinājumu kategorijām un piekļuves gadījumu skaitu kopsummā, kā arī pa dalībvalstīm.

4. Divus gadus pēc SIS II darbības sākšanas un pēc tam reizi divos gados pārvaldības iestāde iesniedz Eiropas Parlamentam un Padomei ziņojumu par centrālās SIS II tehnisko darbību un sakaru infrastruktūru, tostarp tās drošību un papildinformācijas divpusēju un daudzpusēju apmaiņu starp dalībvalstīm.

5. Trīs gadus pēc SIS II darbības sākšanas un pēc tam reizi četros gados Komisija sagatavo vispārēju izvērtējumu par papildinformācijas divpusēju un daudzpusēju apmaiņu starp centrālo SIS II un dalībvalstīm. Šajā vispārējā novērtējumā iekļauj sasniegto rezultātu analīzi salīdzinājumā ar mērķiem, izvērtējumu par to, vai pamatojums joprojām ir spēkā, par šīs regulas piemērošanu saistībā ar centrālo SIS II, centrālās SIS II drošību un turpmāko darbību iespējamo ietekmi. Komisija izvērtējumu nosūta Eiropas Parlamentam un Padomei.

6. Dalībvalstis iesniedz pārvaldības iestādei un Komisijai informāciju, kas vajadzīga, lai izstrādātu 3., 4. un 5. punktā minētos ziņojumus.

7. Pārvaldības iestāde iesniedz Komisijai informāciju, kas vajadzīga, lai izstrādātu 4. punktā minētos vispārējos novērtējumus.

8. Pārejas posmā, pirms pārvaldības iestāde sāk pildīt savus pienākumus, Komisija ir atbildīga par 3. un 4. punktā minēto ziņojumu sagatavošanu un iesniegšanu.

*51. pants***Komiteja**

1. Komisijai palīdz komiteja.
2. Ja ir atsauce uz šo punktu, piemēro Lēmuma 1999/468/EK 5. un 7. pantu, ņemot vērā tā 8. pantu.

Lēmuma 1999/468/EK 5. panta 6. punktā paredzētais termiņš ir trīs mēneši.

3. Komiteja pilda savas funkcijas no šīs regulas spēkā stāšanās dienas.

*52. pants***Grozījumi Šengenas acquis noteikumos**

1. Saistībā ar jautājumiem, uz kuriem attiecas Līgums, no 55. panta 2. punktā minētās dienas šī regula aizstāj Šengenas Konvencijas 92. līdz 119. pantu, izņemot tās 102.A pantu.

▼B

2. No 55. panta 2. punktā minētās dienas šī regula aizstāj arī turpmāk norādītos Šengenas *acquis* noteikumus, ar kuriem īsteno minētos pantus ⁽¹⁾:

- a) Izpildu komitejas Lēmums (1993. gada 14. decembris) par finanšu regulu par Šengenas Informācijas sistēmas (C. SIS) ierīkošanas un darbības izmaksām (*SCH/Com-ex (93) 16*);
- b) Izpildu komitejas Lēmums (1997. gada 7. oktobris) par Šengenas Informācijas sistēmas attīstību (*SCH/Com-ex (97) 24*);
- c) Izpildu komitejas Lēmums (1997. gada 15. decembris), ar ko groza finanšu regulu par centrālo Šengenas Informācijas sistēmu (*SCH/Com-ex (97) 35*);
- d) Izpildu komitejas Lēmums (1998. gada 21. aprīlis) par centrālo Šengenas Informācijas sistēmu ar 15/18 saiknēm (*SCH/Com-ex (98) 11*);
- e) Izpildu komitejas Lēmums (1999. gada 28. aprīlis) par centrālās Šengenas Informācijas sistēmas uzstādīšanas izmaksām (*SCH/Com-ex (99) 4*);
- f) Izpildu komitejas Lēmums (1999. gada 28. aprīlis) par *SIRENE* rokasgrāmatas atjaunināšanu (*SCH/Com-ex (99) 5*);
- g) Izpildu komitejas Deklarācija (1996. gada 18. aprīlis), ar ko nosaka ārvalstnieka jēdzienu (*SCH/Com-ex (96) decl. 5*);
- h) Izpildu komitejas Deklarācija (1999. gada 28. aprīlis) par SIS struktūru (*SCH/Com-ex (99) decl. 2 rev.*);
- i) Izpildu komitejas Lēmums (1997. gada 7. oktobris) par Norvēģijas un Islandes iemaksām Centrālās Šengenas informācijas sistēmas ierīkošanai un darbībai (*SCH/Com-ex (97) 18*).

3. Saistībā ar jautājumiem, uz kuriem attiecas Līgums, atsaucies uz aizstātajiem Šengenas Konvencijas pantiem un attiecīgajiem Šengenas *acquis* noteikumiem, ar ko īsteno minētos pantus, uzskata par atsaucēm uz šo regulu.

53. pants

Atcelšana

No 55. panta 2. punktā minētās dienas tiek atcelta Regula (EK) Nr. 378/2004, Regula (EK) Nr. 871/2004, Lēmums 2005/451/TI, Lēmums 2005/728/TI un Lēmums 2006/628/EK.

⁽¹⁾ OV L 239, 22.9.2000., 439. lpp.

▼B*54. pants***Pārejas posms un budžets**

1. Brīdinājumus pārnes no SIS 1+ uz SIS II. Prioritāti piešķirot brīdinājumiem par personām, dalībvalstis nodrošina, ka to brīdinājumu saturs, kurus pārnes no SIS 1+ uz SIS II, pēc iespējas ātrāk un ne vēlāk kā trīs gados no 55. panta 2. punktā minētās dienas atbilst šai regulai. Šajā pārejas posmā to brīdinājumu saturam, kurus pārnes no SIS 1+ uz SIS II, dalībvalstis var turpināt piemērot Šengenas Konvencijas 94. un 96. pantu, ievērojot šādus noteikumus:

- a) ja brīdinājumu, kas pārņemts no SIS 1+ uz SIS II, groza, papildina, labo vai atjaunina, dalībvalstis nodrošina, ka brīdinājums atbilst šai regulai no brīža, kad to groza, papildina, labo vai atjaunina;
- b) ja ir atsauce uz brīdinājumu, kas pārņemts no SIS 1+ uz SIS II, dalībvalstis nekavējoties izskata šāda brīdinājuma atbilstību šai regulai, tomēr tā, lai nekavētu darbības, kas jāveic, pamatojoties uz šo brīdinājumu.

2. Saskaņā ar 55. panta 2. punktu noteiktajā dienā tā budžeta atlikumu, kas apstiprināts saskaņā ar Šengenas Konvencijas 119. pantu, atmaksā dalībvalstīm. Atmaksājāmās summas aprēķina, pamatojoties uz dalībvalstu iemaksām, kā noteikts Izpildu komitejas Lēmumā (1993. gada 14. decembris) par finanšu regulu par Šengenas Informācijas sistēmas (C. SIS) ierīkošanas un darbības izmaksām.

3. Šīs regulas 15. panta 4. punktā minētajā pārejas posmā šajā regulā esošās atsauces uz pārvaldības iestādi uzskata par atsaucēm uz Komisiju.

*55. pants***Stāšanās spēkā, piemērojamība un pāreja**

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

2. Dalībvalstīm, kas piedalās SIS 1+, to piemēro no dienas, ko nosaka Padome ar to Padomes locekļu vienprātīgu lēmumu, kuri pārstāv to dalībvalstu valdības, kas piedalās SIS 1+.

▼B

3. Šā panta 2. punktā minētās dienas nosaka, kad:
- a) ir pieņemti vajadzīgie īstenošanas pasākumi;
 - b) visas dalībvalstis, kas pilnībā piedalās SIS 1+, Komisijai ir paziņojušas, ka tās veikušas tehniskos un tiesiskos pasākumus, kas vajadzīgi SIS II datu apstrādei un papildinformācijas apmaiņai;
 - c) Komisija ir paziņojusi, ka sekmīgi pabeigta visaptveroša SIS II pārbaude, ko veic Komisija kopā ar dalībvalstīm, un Padomes sagatavošanas struktūras ir apstiprinājušas iesniegtos pārbaudes rezultātus. Ar šo apstiprināšanu apliecina, ka SIS II darbības līmenis ir vismaz līdzvērtīgs SIS 1+ panāktajam darbības līmenim;
 - d) Komisija ir veikusi vajadzīgos tehniskos pasākumus, lai centrālo SIS II varētu pieslēgt attiecīgo dalībvalstu N. SIS II.
4. Komisija informē Eiropas Parlamentu par tās pārbaudes rezultātiem, kas veikta saskaņā ar 3. punkta c) apakšpunktu.
5. Lēmumu, ko Padome pieņem saskaņā ar 2. punktu, publicē *Eiropas Savienības Oficiālajā Vēstnesī*.
- Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs saskaņā ar Eiropas Kopienas dibināšanas līgumu.