

## Šengenas Informācijas sistēma II — rokasgrāmata par piekļuves tiesību izmantošanu Kopsavilkums

Personām, kuru dati tiek vākti, glabāti vai citādi apstrādāti otrās paaudzes Šengenas Informācijas sistēmā (turpmāk "SIS II"), ir tiesības uz piekļuvi, neprecīzu datu labošanu un nelikumīgi glabātu datu dzēšanu<sup>1</sup>. Šajā rokasgrāmatā ir aprakstīti šo tiesību izmantošanas veidi.

### I. Īsa informācija par otrās paaudzes Šengenas Informācijas sistēmu (SIS II)

SIS II ir liela mēroga IT sistēma, kas izveidota, lai atsvērtu iekšējās robežkontroles atcelšanu Šengenas teritorijā, un paredzēta, lai nodrošinātu augstu drošības līmeni Eiropas Savienības brīvības, drošības un tiesiskuma telpā, tostarp nodrošinātu sabiedrības drošības un sabiedriskās kārtības uzturēšanu un garantētu drošību dalībvalstu teritorijās. SIS II ir ieviesta visās Eiropas Savienības dalībvalstīs, izņemot Kipru, Horvātiju un Īriju<sup>2</sup>, kā arī četrās asociētajās valstīs: Islandē, Norvēģijā, Šveicē un Lihtenšteinā.

SIS II ir informācijas sistēma, kas valstu tiesībsardzības, tiesu un administratīvajām iestādēm ļauj veikt konkrētus uzdevumus, apmainoties ar svarīgu informāciju. Eiropas aģentūrām EIROPOLAM un EUROJUST arī ir ierobežotas piekļuves tiesības šai sistēmai.

#### *Apstrādātās informācijas kategorijas*

SIS II centralizē divas plašas informācijas kategorijas brīdinājumu veidā, pirmkārt, par *personām*, kuras meklē, lai arestētu, ir pazudušas, cenšas atrast, lai tās varētu palīdzēt tiesas procesā, diskrētām pārbaudēm vai īpašām pārbaudēm, vai par trešo valstu pilsoņiem, kuriem atteikta ieejošana Šengenas zonā, un, otrkārt, par *priekšmetiem*, piemēram, transportlīdzekļiem, ceļošanas dokumentiem, kredītkartēm, konfiskācijai vai izmantošanai par pierādījumiem krimināllietās, vai diskrētām pārbaudēm vai īpašām pārbaudēm.

#### *Juridiskais pamats*

Atkarībā no brīdinājuma veida SIS II regulē vai nu Eiropas Parlamenta un Padomes 2006. gada 20. decembra Regula (EK) 1987/2006 par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) izveidi, darbību un izmantošanu attiecībā uz brīdinājuma procedūrām, uz ko attiecas Eiropas Kopienų dibināšanas līguma IV sadaļa — agrākais pirmais pīlārs (turpmāk "SIS II Regula"), vai Padomes 2007. gada 12. jūnija Lēmums 2007/533/TI par otrās paaudzes Šengenas informācijas sistēmas (SIS II) izveidi, darbību un izmantošanu, kas attiecas uz procedūrām, uz ko attiecas Līguma par Eiropas Savienību VI sadaļa — agrākais trešais pīlārs (turpmāk "SIS II Lēmums").

#### *Apstrādāto personas datu kategorijas*

Ja brīdinājums attiecas uz personu, informācijai vienmēr jāietver vārds, uzvārds un jebkādi pseidonīmi, dzimums, norāde uz lēmumu, kas ir brīdinājuma pamatā, un veicamie pasākumi. Brīdinājumā jāietver arī informācija par jebkādam īpašām fiziskām pazīmēm, kas ir

<sup>1</sup> Šīs tiesības ir piešķirtas ar 41. pantu 2006. gada 20. decembra Regulā (EK) Nr. 1987/2006 par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) izveidi, darbību un izmantošanu un 58. pantu Padomes 2007. gada 12. jūnija Lēmumā 2007/533/TI par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) izveidi, darbību un izmantošanu.

<sup>2</sup> Informācija par situāciju 2015. gada jūlijā. Bulgārijai un Rumānijai joprojām ir iekšējās robežas, lai gan tās izmanto SIS. Apvienotajai Karalistei ir piekļuve SIS, bet ne attiecībā uz brīdinājumiem saistībā ar aizliegumu ieejot Šengenas teritorijā.

objektīvas un nemainīgas, ja tādas ir pieejamas, dzimšanas vieta un datums, fotogrāfijas, pirkstu nospiedumi, valstspiederība(-as); norāde, vai attiecīgā persona ir bruņota, varmācīga vai izbēgusi; brīdinājuma iemesls; brīdinājuma izdevēja iestāde; saiknes ar citiem brīdinājumiem, kas izdoti SIS II saskaņā ar SIS II Regulas 37. pantu vai SIS II Lēmuma 52. pantu.

### *Sistēmas tehniskā uzbūve*

SIS II veido: 1) centrālā sistēma ("centrālā SIS II"), 2) valsts sistēma katrā dalībvalstī ("N. SIS II"), kas ir saistīta ar centrālo SIS II, un 3) centrālās sistēmas un valstu sistēmu savstarpējo sakaru infrastruktūra, kas nodrošina SIS II datiem atvēlētu kodētu virtuālu tīklu un datu apmaiņu starp iestādēm, kuras ir atbildīgas par papildinformācijas apmaiņu (SIRENE birojs)<sup>3</sup>.

## **II. Personām, kuru dati tiek apstrādāti SIS II, piešķirtās tiesības**

Saskaņā ar datu aizsardzības principiem visām personām, kuru dati tiek apstrādāti SIS II, ar SIS II Regulu un SIS II Lēmumu ir piešķirtas īpašas tiesības<sup>4</sup>, kas tiks analizētas turpmāk. Ikviens, izmantojot šīs tiesības, var vērsties kompetentajās iestādēs tādā valstī pēc savas izvēles, kurā darbojas SIS II. Šāda izvēle ir iespējama, jo visu valstu datubāzes (N.SIS II) ir identiskas centrālās sistēmas datubāzei<sup>5</sup>. Tādējādi šīs tiesības var izmantot jebkurā valstī, kur darbojas SIS II, neatkarīgi no tā, kura dalībvalsts ir izdevusi brīdinājumu.

Kad persona īsteno savas piekļuves tiesības, kā arī tiesības labot neprecīzus datus un dzēst nelikumīgi glabātus datus, kompetentajām iestādēm ir jāsniedz atbilde stingri noteiktā termiņā. Tātad persona ir jāinformē, tiklīdz iespējams, bet jebkurā gadījumā ne vēlāk kā 60 dienu laikā pēc dienas, kad persona iesniegusi pieteikumu piekļuves saņemšanai, vai agrāk, ja to paredz attiecīgās valsts tiesību akti.<sup>6</sup> 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 arī par pasākumiem, kas veikti, īstenojot personas tiesības attiecībā uz datu labošanu un dzēšanu.<sup>7</sup>

### ***Tiesības uz piekļuvi***

Tiesības uz piekļuvi ir iespēja ikvienam, kurš to lūdz, saskaņā ar valsts tiesību aktiem uzzināt informāciju, kas attiecas uz šo personu un glabājas datnē. Tas ir datu aizsardzības pamatprincips, kas datu subjektiem ļauj īstenot kontroli pār personas datiem, ko glabā trešās puses. Šīs tiesības ir skaidri noteiktas SIS II Regulas 41. pantā un SIS II Lēmuma 58. pantā.

Tiesības uz piekļuvi īsteno saskaņā ar tās dalībvalsts tiesību aktiem, kurai ir iesniegts lūgums. Dažādās valstīs ir atšķirīgas procedūras un noteikumi par datu paziņošanu pieteikuma iesniedzējam. Ja dalībvalsts saņem lūgumu piekļūt brīdinājumam, ko tā nav izdevusi, šai

---

<sup>3</sup> SIS II dati tiek ievadīti, atjaunināti, dzēsti un meklēti ar dažādu valstu sistēmu palīdzību. Centrālā sistēma, kas veic tehniskās uzraudzības un administrācijas uzdevumus, atrodas Strasbūrā (Francijā). Tā sniedz SIS datu ievades un apstrādes pakalpojumus. Sistēmas dublējums, kas spēj nodrošināt visas galvenās centrālās sistēmas funkcijas šīs sistēmas avārijas gadījumā, atrodas Zalcburgā (Austrijā). Katra dalībvalsts ir atbildīga par savas valsts sistēmas izveidi, darbību un uzturēšanu, kā arī par tās pievienošanu centrālajai sistēmai. Dalībvalsts norīko iestādi — valsts SIS II biroju ("N. SIS II birojs"), kam ir galvenā atbildība par attiecīgo valsts SIS II projektu. Minētā iestāde ir atbildīga par attiecīgās valsts sistēmas netraucētu darbību un drošību.

<sup>4</sup> Skatīt jo īpaši SIS II Regulas 41. pantu un SIS II Lēmuma 58. pantu.

<sup>5</sup> Skatīt SIS II Regulas un Lēmuma 4. panta 1. punkta b) apakšpunktu.

<sup>6</sup> Skatīt SIS II Regulas 41. panta 6. punktu un SIS II Lēmuma 58. panta 6. punktu.

<sup>7</sup> Skatīt SIS II Regulas 41. panta 7. punktu un SIS II Lēmuma 58. panta 7. punktu.

valstij ir jādod iespēja brīdinājuma izdevējai dalībvalstij darīt zināmu savu nostāju par iespēju izpaust datus pieteikuma iesniedzējam<sup>8</sup>. Informāciju nedara zināmu datu subjektam, ja tā ir noteikti nepieciešama, pildot juridisku pienākumu sakarā ar brīdinājumu vai aizsargājot citu cilvēku tiesības un brīvības.

Patlaban ir divu veidu sistēmas, kas regulē tiesības uz piekļuvi datiem, ko apstrādā tiesībaizsardzības iestādes, un kas tādējādi ir piemērojamas SIS datiem. Dažās dalībvalstīs tiesības uz piekļuvi ir tiesas, bet citās — netiešas.

**Tiešas** piekļuves gadījumā attiecīgā persona tieši iesniedz pieteikumu iestādēm, kuras apstrādā datus (policija, žandarmērija, muita utt.). Ja to atļauj valsts tiesību akti, pieteikuma iesniedzējam var nosūtīt informāciju, kas attiecas uz viņu.

**Netiešas** piekļuves gadījumā persona nosūta savu lūgumu piekļūt informācijai tās valsts datu aizsardzības iestādei, kurai ir iesniegts lūgums. Datu aizsardzības iestāde veic nepieciešamās pārbaudes, lai izskatītu lūgumu, un atbild pieteikuma iesniedzējam.

#### ***Tiesības labot un dzēst datus***

Tiesības uz piekļuvi papildina tiesības panākt, ka tiek laboti personas dati, kuros ir faktu kļūda vai kuri ir nepilnīgi, un tiesības lūgt tos dzēst, ja tie ir nelikumīgi glabāti (SIS II Regulas 41. panta 5. punkts un SIS II Lēmuma 58. panta 5. punkts).

Saskaņā ar Šengenas tiesisko regulējumu tikai tā valsts, kura izdevusi brīdinājumu SIS II, var to labot vai dzēst (skatīt SIS II Regulas 34. panta 2. punktu un SIS II Lēmuma 49. panta 2. punktu). Ja lūgums ir iesniegts dalībvalstī, kura nav izdevusi brīdinājumu, attiecīgo dalībvalstu kompetentās iestādes sadarbojas, lai izskatītu pieteikumu, apmainoties ar informāciju un veicot nepieciešamās pārbaudes. Pieteikuma iesniedzējam ir jāsniedz pamatojums lūgumam labot vai dzēst datus un jāsavāc visa svarīgā informācija, kas to pamato.

#### ***Tiesiskās aizsardzības līdzekļi — tiesības sūdzēties datu aizsardzības iestādē vai ierosināt tiesvedību***

SIS II Regulas 43. pantā un SIS II Lēmuma 59. pantā ir noteikti tiesiskās aizsardzības līdzekļi, kas pieejami personām, ja to lūgums nav bijis izpildīts. Ikviena persona var vērsties tiesā vai saskaņā ar attiecīgās dalībvalsts tiesību aktiem vērsties kompetentā iestādē, lai sakarā ar brīdinājumu, kas attiecas uz konkrēto personu, iegūtu piekļuvi informācijai, labotu, dzēstu vai iegūtu to vai saņemtu kompensāciju.

Ja ir jāizskata sūdzība ar pārrobežu elementu, valstu datu aizsardzības iestādēm ir jāsadarbojas, lai garantētu datu subjektu tiesību īstenošanu.

---

<sup>8</sup> Skatīt SIS II Regulas 41. panta 3. punktu un SIS II Lēmuma 58. panta 3. punktu.