EIROPAS
KOMISIJA

Briselē, 21.12.2016.
COM(2016) 883 final

2016/0409 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par Šengenas Informācijas sistēmas (SIS) izveidi, darbību un izmantošanu policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās, ar ko groza Regulu (ES) Nr. 515/2014 un atceļ Regulu (EK) Nr. 1986/2006, Padomes Lēmumu 2007/533/TI un Komisijas Lēmumu 2010/261/ES

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Pēdējo divu gadu laikā Eiropas Savienība ir strādājusi, lai vienlaikus risinātu dažādas problēmas tādās jomās kā migrācijas pārvaldība, ES ārējo robežu integrēta robežu pārvaldība un cīņa pret terorismu un pārrobežu noziedzību. Efektīva informācijas apmaiņa dalībvalstu starpā un starp dalībvalstīm un attiecīgajām ES aģentūrām ir būtiska, lai nodrošinātu noturīgu šo problēmu risinājumu un veidotu efektīvu un reālu drošības savienību.

Šengenas informācijas sistēma (SIS) ir vispiemērotākais līdzeklis efektīvai sadarbībai starp imigrācijas, policijas, muitas un tiesu iestādēm Eiropas Savienībā un Šengenas asociētajās valstīs. Dalībvalstu kompetentajām iestādēm, piemēram, policijai, robežsardzei un muitas amatpersonām ir jābūt piekļuvei augstas kvalitātes informācijai par personām vai priekšmetiem, kurus tie pārbauda, ar skaidrām norādēm par to, kas jādara katrā atsevišķā gadījumā. Šī lielapjoma informācijas sistēma ir Šengenas sadarbības pamatā un tai ir būtiska loma cilvēku brīvas pārvietošanās atvieglināšanā Šengenas zonā. Tā ļauj kompetentajām iestādēm ievadīt un iegūt datus par meklētām personām, personām, kurām, iespējams, nav tiesību ieceļot vai uzturēties ES, pazudušām personām, jo īpaši bērniem, kā arī par priekšmetiem, kas var būt nozagti, nelikumīgi piesavināti vai pazaudēti. SIS ne tikai satur informāciju par noteiktu personu vai priekšmetu, bet arī skaidras norādes kompetentajām iestādēm par to, kā rīkoties, kad attiecīgā persona vai priekšmets ir atrasts.

Komisija 2016. gadā, trīs gadus pēc SIS otrās paaudzes sistēmas darbības sākšanas, veica tās vispusīgu novērtējumu[1]. Šis novērtējums liecina, ka SIS darbība ir panākumiem bagāta. Valstu kompetentās iestādes 2015. gadā gandrīz 2,9 miljardus reižu salīdzināja personas un priekšmetus ar datiem, kas glabājas SIS, un apmainījās ar vairāk nekā 1,8 miljoniem papildinformācijas vienību. Tomēr, kā paziņots 2017. gada Komisijas darba programmā, pamatojoties uz līdz šim gūto pozitīvo pieredzi, sistēmas efektivitāte un lietderība būtu vēl vairāk jāstiprina. Šajā nolūkā Komisija iesniedz pirmo trīs priekšlikumu paketi, lai, pamatojoties uz novērtējuma rezultātiem, uzlabotu un paplašinātu SIS izmantošanu, vienlaicīgi turpinot darbu, lai pašreizējās un nākotnē iecerētās tiesībaizsardzības un robežu pārvaldības sistēmas kļūtu vēl savietojamākas, ņemot vērā augsta līmeņa ekspertu grupas informācijas sistēmu un sadarbspējas jautājumos veikumu.

Šie priekšlikumi attiecas uz sistēmas izmantošanu a) robežu pārvaldībai, b) policijas un tiesu iestāžu sadarbībai krimināllietās un c) tādu trešo valstu valstspiederīgo atgriešanai, kuri uzturas nelikumīgi. Pirmie divi priekšlikumi kopā veido SIS izveides, darbības un izmantošanas juridisko pamatu. Priekšlikums par SIS izmantošanu tādu trešo valstu valstspiederīgo atgriešanai, kuri uzturas nelikumīgi, papildina priekšlikumu par robežu

[1] Ziņojums Eiropas Parlamentam un Padomei par otrās paaudzes Šengenas Informācijas sistēmu (SIS II) saskaņā ar Regulas (EK) Nr. 1987/2006 24. panta 5. punktu, 43. panta 5. punktu un 50. panta 5. punktu un Lēmuma 2007/533/TI 59. panta 3. punktu un 66. panta 5. punktu un pievienotais Komisijas dienestu darba dokuments. (OV...).

pārvaldību un pilnveido tajā iekļautos noteikumus. Ar to izveido jaunu brīdinājumu kategoriju un uzlabo Direktīvas 2008/115/EK[2] īstenošanu un uzraudzību.

Ņemot vērā dalībvalstu atšķirīgās nostājas par dalību ES politikas virzienos brīvības, drošības un tiesiskuma telpas jomā, ir jāpieņem trīs dažādi tiesību akti, kas tomēr darbosies kopā, lai nodrošinātu visaptverošu sistēmas darbību un izmantošanu.

Paralēli ar mērķi veicināt un uzlabot informācijas pārvaldību ES līmenī Komisija 2016. gada aprīlī uzsāka pārdomu procesu "Spēcīgākas un viedākas robežu un drošības informācijas sistēmas"[3]. Vispārējais mērķis ir nodrošināt, ka kompetentajām iestādēm sistemātiski ir pieejama nepieciešamā informācija no dažādām to rīcībā esošām informācijas sistēmām. Lai sasniegtu šo mērķi, Komisija ir pārskatījusi esošo informācijas sistēmas uzbūvi ar mērķi atrast informācijas robus un trūkumus, kas izriet no pašreizējo sistēmu nepilnībām, kā arī no ES datu pārvaldības vispārējās struktūras sadrumstalotības. Lai atbalstītu šo darbu, Komisija izveidoja augsta līmeņa ekspertu grupu jautājumos par informācijas sistēmu savietojamību, kuras pagaidu konstatējumi ir ņemti vērā arī šo pirmo priekšlikumu paketes izstrādē attiecībā uz datu kvalitātes jautājumiem[4]. Priekšsēdētājs Junkers 2016. gada septembra runā par stāvokli Savienībā cita starpā minēja arī nepieciešamību novērst informācijas pārvaldības trūkumus un uzlabot informācijas sistēmu sadarbspēju un savienojamību.

Ņemot vērā augsta līmeņa ekspertu grupas jautājumos par informācijas sistēmām un sadarbspēju konstatējumus, kas tiks publicēti 2017. gada pirmajā pusē, Komisija apsvērs iespēju 2017. gada vidū iesniegt otro priekšlikumu paketi, lai vēl vairāk uzlabotu SIS sadarbspēju ar citām IT sistēmām. Regulas (ES) Nr. 1077/2011[5] par Eiropas Aģentūras lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*) pārskatīšana ir vienlīdz svarīgs šā darba elements un, visticamāk, būs ietverta atsevišķā Komisijas priekšlikumā arī 2017. gadā. Ieguldījumi ātras, efektīvas un kvalitatīvas informācijas apmaiņas un informācijas pārvaldības, kā arī datubāžu sadarbspējas nodrošināšanā un informācijas sistēmās ir svarīgs aspekts, risinot pašreizējās drošības problēmas.

Šis priekšlikums ir daļa no priekšlikumu kopuma[6], ar kuriem paredzēts uzlabot SIS un tās darbību un izmantošanu policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās. Tas īsteno:

(1) Komisijas apņemšanos uzlabot SIS pievienoto vērtību tiesībaizsardzības nolūkos[7], lai reaģētu uz jauniem apdraudējumiem;

(2) pēdējos trīs gados paveiktā SIS īstenošanas darba konsolidētos rezultātus, kas ietver centrālās SIS tehniskos grozījumus, lai paplašinātu dažas esošo brīdinājumu kategorijas un ieviestu jaunas funkcijas;

---

2 Eiropas Parlamenta un Padomes Direktīva 2008/115/EK (2008. gada 16. decembris) par kopīgiem standartiem un procedūrām dalībvalstīs attiecībā uz to trešo valstu valstspiederīgo atgriešanu, kas dalībvalstī uzturas nelikumīgi (OV L 348, 24.12.2008., 98. lpp.).

3 COM(2016) 205 *final*, 6.4.2016.

4 Komisijas Lēmums 2016/C 257/03, 17.6.2016.

5 Eiropas Parlamenta un Padomes Regula (ES) Nr. 1077/2011 (2011. gada 25. oktobris), ar ko izveido Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (OV L 286, 1.11.2011., 1. lpp.).

6 Regula (ES) 2018/xxx [robežpārbaudes] un Regula (ES) Nr. 2018/xxx [tādu trešu valstu valstspiederīgo atgriešana, kuri uzturas nelikumīgi].

7 Sk. Paziņojumu „Eiropas Drošības programmas īstenošana cīņā pret terorismu un virzībā uz efektīvu un patiesu drošības savienību", 4. iedaļa, COM(2016) 230 *final*, 20.4.2016.

(3) ieteikumus tehniskiem un procesuāliem grozījumiem, kas izriet no visaptverošas SIS izvērtēšanas[8];

(4) SIS galalietotāju lūgumus par tehniskiem uzlabojumiem; un

(5) starpposma secinājumus, ko par datu kvalitāti pieņēmusi Augsta līmeņa ekspertu grupa jautājumos par informācijas sistēmu sadarbspēju[9].

Ņemot vērā to, ka šis priekšlikums ir cieši saistīts ar Komisijas priekšlikumu Regulai par SIS izveidi, darbību un izmantošanu robežpārbaužu jomā, daudzi noteikumi ir kopīgi abiem tekstiem. Tie ietver pasākumus attiecībā uz SIS izmantošanu "no viena gala līdz otram", aptverot ne tikai SIS centrālās sistēmas un valstu sistēmu darbību, bet arī galalietotāju vajadzības; stiprinātus pasākumus darbības nepārtrauktībai; pasākumus attiecībā uz datu kvalitāti, datu aizsardzību un datu drošību, un noteikumus par pārraudzību, novērtēšanu un ziņošanas kārtību. Abi priekšlikumi paplašina biometrisko datu izmantošanu[10].

Spēkā esošais otrās paaudzes SIS tiesiskais regulējums – par tās izmantošanu policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās – ir balstīts uz bijušā trešā pīlāra tiesību aktu: Padomes Lēmumu 2007/533/TI[11], kā arī bijušā pirmā pīlāra tiesību aktu – Regulu (EK) Nr. 1986/2006[12].Ar šo priekšlikumu konsolidē spēkā esošos tiesību aktus, vienlaikus pievienojot jaunus noteikumus, lai:

- labāk saskaņotu SIS izmantošanas valsts procedūras, jo īpaši saistībā ar teroristu nodarījumiem, kā arī ar bērnu nolaupīšanu, ko veic viens no vecākiem;
- paplašinātu SIS piemērošanas jomu, ieviešot brīdinājumos jaunus biometrisko identifikatoru elementus;
- veiktu tehniskas izmaiņas, lai uzlabotu drošību un mazinātu administratīvo slogu, paredzot obligātu valsts eksemplāru un kopīgus īstenošanas tehniskos standartus;
- risinātu jautājumu par SIS pilnīgu izmantošanu no viena gala līdz otram, aptverot ne tikai centrālo sistēmu un valstu sistēmas, bet arī nodrošinot, ka galalietotāji saņem visus vajadzīgos datus, lai veiktu savus uzdevumus, un ievēro visus drošības noteikumus, apstrādājot SIS datus.

• Atbilstība citām Savienības politikas jomām, kā arī spēkā esošajiem un nākotnē plānotajiem tiesību aktiem

Šis priekšlikums ir cieši saistīts ar citām Savienības politikas jomām un papildina tās, proti:

---

8 Ziņojums Eiropas Parlamentam un Padomei par otrās paaudzes Šengenas Informācijas sistēmu (SIS II) saskaņā ar Regulas (EK) Nr. 1987/2006 24. panta 5. punktu, 43. panta 5. punktu un 50. panta 5. punktu un Lēmuma 2007/533/TI 59. panta 3. punktu un 66. panta 5. punktu un pievienotais Komisijas dienestu darba dokuments. (OV...).

9 Augsta līmeņa ekspertu grupas priekšsēdētāja ziņojums — 2016. gada 21. decembris.

10 Skatīt 5. sadaļu "Citi elementi", kurā iekļauts detalizēts skaidrojums par šajā priekšlikumā iekļautajām izmaiņām

11 Padomes Lēmums 2007/533/TI (2007. gada 12. jūnijs) par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) izveidi, darbību un izmantošanu (OV L 205, 7.8.2007., 63. lpp.).

12 Eiropas Parlamenta un Padomes Regula (EK) Nr. 1986/2006 (2006. gada 20. decembris) par dalībvalstu dienestu, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izsniegšanu, piekļuvi otrās paaudzes Šengenas Informācijas sistēmai (SIS II) (OV L 381, 28.12.2006., 1. lpp.).

(1) **Iekšējā drošība** – kā uzsvērts Eiropas Drošības programmā[13] un Komisijas paziņojumā par virzību uz efektīvu un patiesu drošības savienību[14], lai novērstu, atklātu, izmeklētu teroristu nodarījumus un citus smagus noziegumus un sauktu pie atbildības par tiem, tiesībaizsardzības iestādēm ir jāspēj apstrādāt to personu personas datus, kuras tiek turētas aizdomās par dalību terora aktos vai smagos noziegumos.

(2) **datu aizsardzība**, ciktāl šis priekšlikums nodrošina pamattiesību aizsardzību personām, kuru personas dati tiek apstrādāti SIS.

Šis priekšlikums ir cieši saistīts ar citiem Savienības tiesību aktiem un papildina tos, proti:

(3) **Eiropas robežu un krasta apsardze** attiecībā uz tās piekļuvi SIS ierosinātās Eiropas ceļošanas informācijas atļauju sistēmas (*ETIAS*) vajadzībām[15], kā arī attiecībā uz tehniskās saskarnes ar SIS nodrošināšanu, lai Eiropas robežu un krasta apsardzes vienību, tāda personāla vienību, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, un migrācijas pārvaldības atbalsta vienības dalībnieki atbilstīgi savām pilnvarām varētu piekļūt SIS un meklēt datos, kas ievadīti SIS;

(4) **Eiropols** – šis priekšlikums piešķir Eiropolam papildu tiesības piekļūt SIS un meklēt SIS ievadītos datus, ievērojot Eiropola pilnvaras.

(5) **Prīme** – uzlabojumi šajā priekšlikumā ļauj identificēt personas, pamatojoties uz pirkstu nospiedumiem (kā arī sejas attēliem un DNS profiliem), un papildina pašreizējos Prīmes noteikumus[16] par savstarpēju pārrobežu tiešsaistes piekļuvi konkrētām valstu DNS datubāzēm un automatizētajām pirkstu nospiedumu identifikācijas sistēmām.

Šis priekšlikums ir cieši saistīts ar citiem nākotnē plānotiem Savienības tiesību aktiem un papildina tos, proti:

(6) **Ārējo robežu pārvaldība**. Šis priekšlikums papildina jauno Šengenas Robežu kodeksa principu par visu ceļotāju, tostarp ES pilsoņu, sistemātiskām pārbaudēm attiecīgajās datubāzēs, kad tie ieceļo un izceļo no Šengenas zonas, minētais princips ieviests, lai vērstos pret ārvalstu kaujiniekiem teroristiem.

(7) **Ieceļošanas/izceļošanas sistēma** Priekšlikumā ir paredzēts atspoguļot ierosināto pirkstu nospiedumu un sejas attēlu kā biometrisko identifikatoru kopīgu izmantošanu ieceļošanas/izceļošanas sistēmas (IIS) darbībai.

(8) ***ETIAS*.** Priekšlikumā ir ņemta vērā ierosinātā *ETIAS*, kura nodrošina visaptverošu drošības novērtējumu, tostarp pārbaudes SIS, attiecībā uz trešo valstu valstspiederīgajiem, kuri ir atbrīvoti no vīzas prasības un plāno ceļot Eiropas Savienībā.

---

13 COM(2015) 185 *final*.

14 COM(2016) 230 *final*.

15 COM(2016) 731 *final*.

16 Padomes Lēmums 2008/615/TI (2008. gada 23. jūnijs) par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu un pārrobežu noziedzību (OV L 210, 6.8.2008., 1. lpp.) un Padomes Lēmums 2008/616/TI (2008. gada 23. jūnijs) par to, kā īstenot Lēmumu 2008/615/TI par pārrobežu sadarbības pastiprināšanu, jo īpaši – apkarojot terorismu un pārrobežu noziedzību (OV L 210, 6.8.2008., 12. lpp.).

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

• Juridiskais pamats

Priekšlikuma juridiskais pamats noteikumiem par policijas sadarbību un tiesu iestāžu sadarbību krimināllietās ir Līguma par Eiropas Savienības darbību 82. panta 1. punkta d) apakšpunkts, 85. panta 1. punkts, 87. panta 2. punkta a) apakšpunkts un 88. panta 2. punkta a) apakšpunkts.

• Valstu atšķirīgās nostājas

Šis priekšlikums pilnveido Šengenas *acquis* noteikumus attiecībā uz policijas sadarbību un tiesu iestāžu sadarbību krimināllietās. Tāpēc ir jāņem vērā šādas sekas saistībā ar dažādajiem protokoliem un nolīgumiem ar asociētajām valstīm.

Dānijā: Saskaņā ar Līgumiem pievienotā 22. protokola par Dānijas nostāju 4. pantu sešos mēnešos pēc tam, kad Padome ir pieņēmusi lēmumu par šo regulu, Dānija izlemj, vai tā ieviesīs savos tiesību aktos šo priekšlikumu, kas pilnveido Šengenas *acquis*.

Apvienotā Karaliste: Saskaņā ar 5. pantu Protokolā par Šengenas *acquis*, kas iekļauts Eiropas Savienības sistēmā, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, un saskaņā ar 8. panta 2. punktu Padomes 2000. gada 29. maija Lēmumā 2000/365/EK par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā[17], šī regula ir saistoša Apvienotajai Karalistei.

Īrija: Saskaņā ar 5. pantu Protokolā par Šengenas *acquis*, kas iekļauts Eiropas Savienības sistēmā un kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, un saskaņā ar 6. panta 2. punktu Padomes 2002. gada 28. februāra Lēmumā 2002/192/EK par Īrijas lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā[18], šī regula ir saistoša Īrijai.

Bulgārija un Rumānija. Šī regula ir akts, kas pieņemts atbilstīgi Šengenas *acquis* vai ir kā citādi saistīts ar to 2005. gada Pievienošanās akta 4. panta 2. punkta nozīmē. Šī regula ir jāskata saistībā ar Padomes 2010. gada 29. jūnija lēmumu Nr. 2010/365/ES[19], ar ko Bulgārija un Rumānijā ar dažiem ierobežojumiem kļuva piemērojami Šengenas *acquis* noteikumi par Šengenas Informācijas sistēmu.

Kipra un Horvātija. Šī regula ir akts, kas pilnveido Šengenas *acquis* vai ir kā citādi saistīts ar to, kā noteikts attiecīgi 2003. gada Pievienošanās akta 3. panta 2. punktā un 2011. gada Pievienošanās akta 4. panta 2. punktā.

Asociētās valstis. Pamatojoties uz attiecīgajiem nolīgumiem, ar ko Islande, Norvēģija, Šveice un Lihtenšteina pievienojas Šengenas *acquis* īstenošanai, piemērošanai un pilnveidei, tām šī ierosinātā regula ir saistoša.

---

17 OV L 131, 1.6.2000., 43. lpp.

18 OV L 64, 7.3.2002., 20. lpp.

19 Padomes Lēmums (2010. gada 29. jūnijs) par Šengenas *acquis* noteikumu īstenošanu saistībā ar Šengenas Informācijas sistēmu Bulgārijas Republikā un Rumānijā (OV L 166, 1.7.2010., 17. lpp.).

- **Subsidiaritāte**

Šis priekšlikums izstrādās un pilnveidos esošo SIS, kas darbojas kopš 1995. gada. Sākotnējo starpvaldību instrumentu 2013. gada 9. aprīlī aizstāja Savienības instrumenti (Regula (EK) Nr. 1987/2006 un Padomes Lēmums 2007/533/TI). Pilnīga subsidiaritātes analīze tika veikta iepriekšējos gadījumos; šīs iniciatīvas mērķis ir turpināt pilnveidot spēkā esošos noteikumus, novēršot konstatētos trūkumus un uzlabojot darbības procedūras.

Šāds ievērojams informācijas apmaiņas līmenis starp dalībvalstīm, izmantojot SIS, nav sasniedzams, izmantojot decentralizētus risinājumus. Darbības mēroga, seku un ietekmes dēļ šo priekšlikumu var labāk sasniegt Savienības līmenī.

Šā priekšlikuma mērķi cita starpā ietver tehniskus uzlabojumus SIS efektivitātes palielināšanai, kā arī centienus saskaņot sistēmas izmantošanu visās iesaistītajās dalībvalstīs. Starptautiskā rakstura dēļ, kas piemīt šiem mērķiem un problēmām saistībā ar efektīvas informācijas apmaiņas nodrošināšanu, lai apkarotu arvien dažādākos apdraudējumiem, ES ir piemērotā situācijā, lai ierosinātu risinājumus šiem jautājumiem, kurus nevar pietiekami labi sasniegt atsevišķās dalībvalstīs.

Ja pastāvošie SIS ierobežojumi netiks atrisināti, pastāv risks palaist garām vairākas iespējas, kā palielināt efektivitāti un ES pievienoto vērtību, un trūkumi kavēs kompetento iestāžu darbu. Kā piemēru var minēt saskaņotu noteikumu trūkumu par vairs nevajadzīgu brīdinājumu dzēšanu no sistēmas, kas var radīt šķēršļus personu pārvietošanās brīvībai, kura ir Eiropas Savienības pamatprincips.

- **Proporcionalitāte**

Līguma par Eiropas Savienību 5. pantā noteikts, ka Savienības rīcība ir samērīga ar Līgumā noteikto mērķu sasniegšanai nepieciešamo. Šīs ES rīcības izvēlētajam veidam jārada iespēja sasniegt priekšlikuma mērķi un to īstenot pēc iespējas efektīvāk. Ar ierosināto iniciatīvu tiek pārskatīta SIS attiecībā uz policijas sadarbību un tiesu iestāžu sadarbību krimināllietās.

Priekšlikuma pamatā ir *integrētas privātuma aizsardzības* principi. Attiecībā uz personas datu aizsardzību šis priekšlikums ir samērīgs, jo tas paredz īpašus brīdinājumu dzēšanas noteikumus un neparedz datu vākšanu un glabāšanu ilgāk, nekā tas ir absolūti nepieciešams, lai sistēma varētu darboties un pildīt savus mērķus. Pamatojoties uz apsvērumiem par darbības prasībām, šajā priekšlikumā ir samazināts saglabāšanas periods brīdinājumiem par priekšmetiem, un tas ir saskaņots ar brīdinājumiem par personām (jo tie ļoti bieži ir saistīti ar personas datiem, piemēram, personu apliecinoši dokumenti vai transportlīdzekļu numura zīmes). Policijas pieredze liecina, ka nozagto īpašumu var atgūt samērā īsā laikā, kas 10 gadu termiņu padara par pārlieku ilgu termiņu brīdinājumu par priekšmetiem spēkā esamībai.

SIS brīdinājumos ir ietverti tikai tādi dati, kas ir vajadzīgi, lai identificētu un atrastu personu vai priekšmetu un nodrošinātu pienācīgu operatīvu rīcību. Visa veida papildu informācija tiek nodrošināta ar *SIRENE* biroju starpniecību, kas ļauj apmainīties ar papildinformāciju.

Turklāt ar priekšlikumu paredzēts ieviest visus nepieciešamos aizsardzības pasākumus un mehānismus, kas vajadzīgi, lai efektīvi aizsargātu datu subjektu pamattiesības, jo īpaši viņu privāto dzīvi un personas datus. Tas ietver arī noteikumus, kas paredzēti, lai nostiprinātu SIS glabāto personas datu drošību.

Lai sistēma darbotos, nebūs vajadzīgi papildu procesi vai saskaņošana ES līmenī. Tādējādi paredzamais pasākums ir proporcionāls, jo tas ES mēroga rīcības ziņā nepārsniedz nepieciešamo, lai sasniegtu nospraustos mērķus.

- **Juridiskā akta izvēle**

Ierosinātā pārskatīšana notiks ar regulu un tā aizstās Padomes Lēmumu 2007/533/TI, vienlaikus saglabājot ievērojamu daļu šā lēmuma satura. Lēmums 2007/533/TI tika pieņemts kā tā dēvētais "trešā pīlāra" instruments saskaņā ar agrāko Līgumu par Eiropas Savienību. Šādus "trešā pīlāra" instrumentus Padome pieņēma bez Eiropas Parlamenta kā viena no likumdevējiem. Šā priekšlikuma juridiskais pamats ir Līgums par Eiropas Savienības darbību (LESD), jo pīlāru struktūra vairs nepastāv kopš Lisabonas līguma stāšanās spēkā 2009. gada 1. decembrī. Juridiskais pamats prasa izmantot parasto likumdošanas procedūru. (Eiropas Parlamenta un Padomes) regula ir jāizvēlas, jo noteikumiem ir jābūt saistošiem un ir tieši piemērojamiem visās dalībvalstīs.

Priekšlikums pilnveidos un uzlabos pastāvošo centralizēto sistēmu, ar kuras starpniecību dalībvalstis sadarbojas cita ar citu, tādēļ tam ir nepieciešama kopīga arhitektūra un saistoši darbības noteikumi. Turklāt tajā noteikti obligātie noteikumi par piekļuvi sistēmai, tostarp tiesībaizsardzības iestāžu vajadzībām, kas ir vienādi visām dalībvalstīm, kā arī Eiropas Aģentūrai lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā[20] (*eu-LISA*). Kopš 2013. gada 9. maija *eu-LISA* ir atbildīga par centrālās SIS darbības pārvaldību, kas aptver visus uzdevumus, kuri vajadzīgi, lai nodrošinātu centrālās SIS darbību pilnā apjomā 24 stundas diennaktī, 7 dienas nedēļā. Šis priekšlikums balstās uz *eu-LISA* pienākumiem attiecībā uz SIS.

Turklāt priekšlikums paredz tieši piemērojamus noteikumus, kas ļauj datu subjektam piekļūt saviem datiem un tiesību aizsardzības līdzekļiem, neprasot papildu īstenošanas pasākumus šajā sakarā.

Tādējādi par juridisko instrumentu var izvēlēties vienīgi regulu.

3. *EX POST* IZVĒRTĒJUMS, APSPRIEŠANĀS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

- ***Ex post* izvērtējumi/spēkā esošo tiesību aktu atbilstības pārbaude**

Saskaņā ar Regulu (EK) Nr. 1987/2006 un Padomes Lēmumu 2007/533/TI trīs gadus pēc darbības uzsākšanas Komisija veica vispārēju centrālās SIS II novērtējumu, kā arī novērtējumu par divpusējo vai daudzpusējo papildinformācijas apmaiņu starp dalībvalstīm.

Novērtējuma rezultāti parādīja, ka ir nepieciešamas izmaiņas SIS juridiskajā pamatā, lai labāk reaģētu uz jaunajām drošības un migrācijas problēmām. Tas ietver, piemēram, priekšlikumu par SIS pilnīgu izmantošanu no viena gala līdz otram, regulējot tās izmantošanu, ko veic galalietotāji, un paredzot datu drošības standartus, kuri piemērojami arī galalietotāju lietojumprogrammām, sistēmas stiprināšanu terorisma apkarošanas nolūkos, paredzot jaunas darbības, situācijas uzlabošanu attiecībā uz bērniem, kuri ir pakļauti vecāku veiktas nolaupīšanas riskam, kā arī sistēmā pieejamo biometrisko identifikatoru paplašināšanu.

Novērtēšanas rezultāti arī liecināja, ka ir vajadzīgi tiesību akta grozījumi, lai uzlabotu sistēmas tehnisko darbību un vienkāršotu procesus valstīs. Šie pasākumi palielinās SIS efektivitāti un iedarbīgumu, atvieglojot tās izmantošanu un samazinot nevajadzīgu slogu. Papildu pasākumi ir paredzēti, lai uzlabotu datu kvalitāti un sistēmas pārredzamību, skaidrāk aprakstot dalībvalstu un *eu-LISA* īpašos ziņošanas uzdevumus.

[20] Izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1077/2011 (2011. gada 25. oktobris), ar ko izveido Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (OV L 286, 1.11.2011., 1. lpp.).

Visaptverošā novērtējuma rezultāti (novērtējuma ziņojums un dienestu darba dokuments tika pieņemti 2016. gada 21. decembrī[21]) veidoja pamatu pasākumiem, kas iekļauti šajā priekšlikumā.

- **Apspriešanās ar ieinteresētajām personām**

Komisijas īstenotā SIS novērtējuma laikā atgriezeniskā saite un ierosinājumi tika lūgti no ieinteresētajām personām, tostarp SISVIS komitejas pārstāvjiem, saskaņā ar procedūru, kas noteikta 67. pantā Padomes Lēmumā (EK) Nr. 533/2007. Šajā komitejā ir dalībvalstu pārstāvji gan *SIRENE* darbības jautājumos (pārrobežu sadarbība saistībā ar SIS), gan tehniskos jautājumos par SIS pilnveidi un uzturēšanu un ar to saistīto *SIRENE* piemērošanu.

Novērtēšanas procesa ietvaros pārstāvji atbildēja uz sīki izstrādātām anketām. Ja bija vajadzīgi papildu skaidrojumi vai jautājumu bija jāizskata sīkāk, tas tika panākts, izmantojot e-pastu apmaiņu vai īpašas aptaujas. Šis iteratīvais process ļāva izskatīt jautājumus visaptverošā un pārredzamā veidā. Visu 2015. un 2016. gadu SISVIS komitejas pārstāvji apsprieda šos jautājumus speciālu tikšanos un darbsemināru laikā.

Datu aizsardzības jomā Komisija turklāt īpaši konsultējās ar dalībvalstu datu aizsardzības iestādēm un SIS II uzraudzības koordinācijas grupas pārstāvjiem. Dalībvalstis dalījās pieredzē par subjektu piekļuves pieprasījumiem un valstu datu aizsardzības iestāžu darbu, atbildot uz īpašas aptaujas jautājumiem. Sākot ar 2015. gada jūniju aptaujas atbildes ir ņemtas vērā šā priekšlikuma izstrādē.

Komisija izveidoja starpdienestu koordinācijas grupu, iekļaujot tajā ģenerālsekretariātu un Migrācijas un iekšlietu ģenerāldirektorātu, Tiesiskuma un patērētāju lietu ģenerāldirektorātu, Cilvēkresursu un drošības ģenerāldirektorātu un Informātikas ģenerāldirektorātu. Šī koordinācijas grupa uzraudzīja novērtēšanas procesu un vajadzības gadījumā sniedza norādījumus.

Novērtējuma konstatējumos ir ņemti vērā arī pierādījumi, kas savākti apmeklējumos uz vietas dalībvalstīs, kuru laikā tika sīki pētīts, kā SIS tiek izmantota praksē. Tas ietvēra diskusijas un pārrunas ar praktiķiem, *SIRENE* biroja darbiniekiem un valstu kompetentajām iestādēm.

Ņemot vērā šīs atsauksmes, šis priekšlikums paredz pasākumus, kuru mērķis ir uzlabot sistēmas tehnisko un operatīvo efektivitāti un iedarbīgumu.

- **Ekspertu atzinumu pieprasīšana un izmantošana**

Papildus konsultācijām ar ieinteresētajām personām Komisija centās iegūt arī ārēju ekspertu viedokli, izmantojot trīs pētījumus, kuru secinājumi tika ir iekļauti šā priekšlikuma izstrādē:

- SIS tehniskais novērtējums (*Kurt Salmon*)[22]

  Šajā novērtējumā tika konstatēti galvenie atrisināmie jautājumi saistībā ar SIS darbību un nākotnes vajadzībām, galvenokārt apzinot problēmas saistībā ar darbības nepārtrauktības maksimālu garantēšanu un nodrošināšanu, ka vispārējā uzbūve ir spējīga pielāgoties palielinātas jaudas prasībām.

- IKT ietekmes novērtējums par iespējamiem uzlabojumiem SIS II uzbūvē (*Kurt Salmon*)[23]

---

[21] Ziņojums Eiropas Parlamentam un Padomei par otrās paaudzes Šengenas Informācijas sistēmu (SIS II) saskaņā ar Regulas (EK) Nr. 1987/2006 24. panta 5. punktu, 43. panta 5. punktu un 50. panta 5. punktu un Lēmuma 2007/533/TI 59. panta 3. punktu un 66. panta 5. punktu un pievienotais Komisijas dienestu darba dokuments.

[22] Eiropas Komisijas nobeiguma ziņojums — SIS II tehniskais novērtējums.

Šajā pētījumā tika novērtētas SIS darbības izmaksas valstu līmenī un izvērtēti divi iespējamie tehniskie risinājumi sistēmas uzlabošanai. Abi risinājumi ietver tehnisko priekšlikumu kopumu ar mērķi uzlabot centrālo sistēmu un vispārējo uzbūvi;

- "IKT ietekmes novērtējums par tehniskiem uzlabojumiem SIS II uzbūvē – nobeiguma ziņojums", 2016. gada 10. novembris, (*Wavestone*)[24]

Šajā pētījumā tika novērtēts, kāda ietekme uz dalībvalstu izmaksām ir valsts eksemplāra uzturēšanai, analizējot trīs scenārijus (pilnībā centralizēta sistēma, standartizēta N.SIS, kuru izstrādā un dalībvalstīm nodrošina *eu-LISA*, un atšķirīgas N.SIS ar vienotiem tehniskajiem standartiem).

- **Ietekmes novērtējums**

Komisija neveica ietekmes novērtējumu.

Trīs iepriekš minētie neatkarīgie novērtējumi (iedaļā "Ekspertu atzinumu pieprasīšana un izmantošana") veidoja pamatu apsvērumiem par sistēmas izmaiņu ietekmi no tehniskā viedokļa. Turklāt kopš 2013. gada, tas ir, kopš 2013. gada 9. aprīlī sāka darboties SIS II un tika sākta Lēmuma 2007/533/TI piemērošana, Komisija ir divas reizes pārskatījusi *SIRENE* rokasgrāmatu. Tas ietver starpposma novērtējumu, kura rezultātā 2015. gada 29. janvārī tika ieviesta jauna *SIRENE* rokasgrāmata[25]. Komisija ir pieņēmusi arī Ieteikumu un labākās prakses katalogu[26]. Turklāt *eu-LISA* un dalībvalstis regulāri veic iteratīvus sistēmas tehniskos uzlabojumus. Tiek uzskatīts, ka šīs iespējas beidzot ir izsmeltas, un ir vajadzīgi vispusīgāki juridiskā pamata grozījumi. Skaidrību tādās jomās kā galalietotāju sistēmas piemērošana, kā arī sīki izstrādāti noteikumi par brīdinājumu dzēšanu, nav panākama ar uzlabotu īstenošanu un izpildi vien.

Turklāt Komisija ir vispusīgi novērtējusi SIS, kā tas ir paredzēts Regulas (EK) Nr. 1987/2006 24. panta 5. punktā, 43. panta 3. punktā un 50. panta 5. punktā un Lēmuma 2007/533/TI 59. panta 3. punktā un 66. panta 5. punktā, un ir publicējusi attiecīgu dienestu darba dokumentu. Visaptverošā novērtējuma rezultāti (novērtējuma ziņojums un dienestu darba dokuments tika pieņemti 2016. gada 21. decembrī) veidoja pamatu pasākumiem, kas iekļauti šajā priekšlikumā.

Šengenas izvērtēšanas mehānisms, kas paredzēts Regulā (ES) Nr. 1053/2013[27], ļauj regulāri izvērtēt SIS darbības juridiskos un operatīvos aspektus dalībvalstīs. Šos izvērtējumus kopīgi veic Komisija un dalībvalstis. Izmantojot šo mehānismu, Padome sniedz ieteikumus atsevišķām dalībvalstīm, pamatojoties uz izvērtējumu, ko veic kā daļu no daudzgadu un gada

---

23 Eiropas Komisijas nobeiguma ziņojums — IKT ietekmes novērtējums par iespējamiem uzlabojumiem SIS II uzbūvē 2016. gads.

24 Eiropas Komisijas nobeiguma ziņojums – IKT ietekmes novērtējums par tehniskiem uzlabojumiem SIS II uzbūvē – nobeiguma ziņojums, 2016. gada 10. novembris, (*Wavestone*)

25 Komisijas Īstenošanas lēmums (ES) 2015/219 (2015. gada 29. janvāris), ar ko aizstāj pielikumu Īstenošanas lēmumam 2013/115/ES par SIRENE rokasgrāmatu un citiem īstenošanas pasākumiem otrās paaudzes Šengenas informācijas sistēmai (SIS II) (OV L 44, 18.2.2015., 75. lpp.).

26 Komisijas ieteikums, ar ko izveido ieteikumu un paraugprakses katalogu par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) pareizu piemērošanu un papildinformācijas apmaiņu starp dalībvalstu kompetentajām iestādēm, kas īsteno un izmanto SIS II (C(2015)9169/1).

27 Padomes Regula (ES) Nr. 1053/2013 (2013. gada 7. oktobris), ar ko izveido izvērtēšanas un uzraudzības mehānismu, lai pārbaudītu Šengenas acquis piemērošanu, un ar ko atceļ Izpildu komitejas lēmumu (1998. gada 16. septembris), ar ko izveido Šengenas izvērtēšanas un īstenošanas pastāvīgo komiteju (OV L 295, 6.11.2013., 27. lpp.).

programmām. Individuālā rakstura dēļ šie ieteikumi nevar aizstāt juridiski saistošus noteikumus, kas ir piemērojami vienlaikus visās dalībvalstīs, kas izmanto SIS.

SISVIS komiteja regulāri apspriež praktiskos un tehniskos jautājumus. Lai gan šīs sanāksmes ir svarīgas sadarbībai starp Komisiju un dalībvalstīm, šo diskusiju rezultāti (ja netiek veiktas izmaiņas tiesību aktos) nespēj risināt jautājumus, kuri rodas, piemēram, dažādas valstu prakses dēļ.

Ierosinātās izmaiņas šajā regulā nerada būtiskas ekonomiskas sekas vai ietekmi uz vidi. Tomēr šīs pārmaiņas atstās būtiski pozitīvu sociālo ietekmi, jo tās palielina drošību, ļaujot sekmīgāk identificēt personas, kas izmanto viltus identitāti, noziedzniekus, kuru identitāte nav zināma pēc smaga nozieguma izdarīšanas, kā arī pazudušus nepilngadīgos. Šo izmaiņu ietekme uz pamattiesībām un datu aizsardzību ir sīkāk izklāstīta nākamajā iedaļā ("Pamattiesības").

Priekšlikums ir sagatavots, izmantojot ievērojamu pierādījumu kopumu, kas savākts otrās paaudzes SIS vispārīgā novērtējuma procesā, kurā tika izskatīta sistēmas darbība un iespējamie uzlabojumi. Turklāt tika veikts izmaksu ietekmes novērtējuma pētījums, lai nodrošinātu, ka izvēlētā uzbūve valstu līmenī ir vispiemērotākā un samērīgākā.

- **Pamattiesības un datu aizsardzība**

Šis priekšlikums attīsta un uzlabo esošu sistēmu, nevis izveido jaunu, un tāpēc tā pamatā ir svarīgi un efektīvi aizsardzības pasākumi, kas jau ir ieviesti. Tomēr sistēma turpina apstrādāt personas datus un tā apstrādās jaunas sensitīvu biometrisko datu kategorijas, tāpēc ir iespējama ietekme uz indivīda pamattiesībām. Ietekme tika rūpīgi izskatīta, un ir ieviesti papildus aizsardzības pasākumi, lai ierobežotu datu vākšanu un turpmāku apstrādi, nepārsniedzot to, kas ir obligāti nepieciešams, un ierobežoti piešķirot piekļuvi attiecīgajiem datiem tikai tiem, kam ir operatīva nepieciešamība tos apstrādāt. Šajā priekšlikumā ir noteikti konkrēti datu saglabāšanas periodi, tostarp saīsināts datu saglabāšanas periods brīdinājumiem par priekšmetiem. Indivīdiem ir skaidri atzītas un nodrošinātas tiesības uz piekļuvi datiem attiecībā uz sevi, tiesības uz datu labošanu un tiesības pieprasīt dzēst datus saskaņā ar viņu pamattiesībām (skat. iedaļu par datu aizsardzību un drošību).

Turklāt priekšlikums paredz pastiprināt pasākumus, lai aizsargātu pamattiesības, jo tas nostiprina tiesību aktā prasības dzēst brīdinājumus un ievieš samērīguma novērtējumu, ja brīdinājums tiek pagarināts. Uzticamāka personu identifikācija būs iespējama, izmantojot biometriskos datus par pazudušām personām, kurām nepieciešama aizsardzība, nodrošinot personas datu precīzumu un atbilstīgu aizsardzību. Priekšlikumā ir definēti plaši un stingri aizsardzības pasākumi attiecībā uz biometrisko identifikatoru izmantošanu, lai novērstu neērtības nevainīgām personām.

Priekšlikumā arī noteikts, ka nepieciešama pilnīga sistēmas drošība no viena gala līdz otram, nodrošinot labāku tajā glabāto datu aizsardzību. Ieviešot skaidru SIS starpgadījumu pārvaldības procedūru, kā arī uzlabotu darbības nepārtrauktību, šis priekšlikums pilnībā atbilst Eiropas Savienības Pamattiesību hartai[28] attiecībā uz tiesībām uz personas datu aizsardzību. SIS uzlabošana un pastāvīga efektivitāte veicinās ikviena drošību sabiedrībā.

Priekšlikums paredz būtiskas izmaiņas attiecībā uz biometriskajiem identifikatoriem. Papildus pirkstu nospiedumiem, ja ir izpildītas juridiskās prasības, būtu jāiegūst arī plaukstu nospiedumi. Pirkstu nospiedumu ieraksti tiek pievienoti SIS burtciparu brīdinājumiem, kā paredzēts 26., 32., 34. un 36. pantā. Nākotnē vajadzētu būt iespējai meklēt šos

[28] Eiropas Savienības Pamattiesību harta (2012/C 326/02).

daktiloskopiskos datus (pirkstu nospiedumus un plaukstu nospiedumus) un salīdzināt ar pirkstu nospiedumiem, kas konstatēti noziedzīga nodarījuma izdarīšanas vietā — ar nosacījumu, ka nodarījums ir uzskatāms par smagu noziegumu vai terorismu, un var konstatēt augstu varbūtības pakāpi, ka tie pieder nodarījuma izdarītājam. Turklāt priekšlikumā paredzēta pirkstu nospiedumu glabāšana par tā sauktām "nezināmām meklētām personām" (nosacījumi ir aprakstīti 5. iedaļas apakšiedaļā "Fotogrāfijas, sejas attēli, daktiloskopiskie dati un DNS profili"). Ja pastāv nenoteiktība par personas identitāti, pamatojoties uz personas dokumentiem, kompetentajām iestādēm būtu jāsalīdzina pirkstu nospiedumi ar pirkstu nospiedumiem, kas glabājas SIS datubāzē.

Priekšlikums paredz papildu datu vākšanu un glabāšanu (piemēram, par personu apliecinošiem dokumentiem), kas atvieglotu darbu darbiniekiem uz vietas, pārbaudot personas identitāti.

Priekšlikums nodrošina datu subjekta tiesības uz efektīviem tiesību aizsardzības līdzekļiem, lai apstrīdētu jebkuru lēmumu, kas jebkurā gadījumā ietver efektīvu tiesību aizsardzību tiesā saskaņā ar Pamattiesību hartas 47. pantu.

4. IETEKME UZ BUDŽETU

SIS ir viena informācijas sistēma. Līdz ar to izdevumi, kas paredzēti abos priekšlikumos (šajā priekšlikumā un priekšlikumā Regulai par Šengenas Informācijas sistēmas (SIS) izveidi, darbību un izmantošanu robežpārbaužu jomā), nebūtu jāuzskata par divām atsevišķām summām, bet par vienu veselumu. Ietekme uz budžetu, kas būtu grozījumiem, kuri vajadzīgi abu priekšlikumu īstenošanai, ir atspoguļota vienā tiesību akta finanšu pārskatā.

Ņemot vērā trešā priekšlikuma (par tādu trešo valstu valstspiederīgo atgriešanu, kuri uzturas nelikumīgi) papildinošo raksturu, tā ietekme uz budžetu ir aplūkota atsevišķi neatkarīga finanšu pārskata ietvaros, kurā apskatīta tikai šīs īpašās brīdinājumu kategorijas izveide.

Pamatojoties uz novērtējumu, kas veikts par dažādiem aspektiem saistībā ar *eu-LISA* darbu, kas nepieciešams attiecībā uz tīklu un centrālo SIS, un valstu sistēmu uzlabojumiem dalībvalstīs, abu regulu priekšlikumiem būs nepieciešama kopējā summa EUR 64,3 miljoni laikposmā no 2018. līdz 2020. gadam.

Tā ietver TESTA-NG platjoslas palielinājumu, ņemot vērā to, ka saskaņā ar abiem priekšlikumiem tīklā tiks pārraidītas pirkstu nospiedumu un sejas attēlu datnes, kurām nepieciešama lielāka caurlaidspēja un jauda (EUR 9,9 miljoni). Tā sedz arī izdevumus saistībā ar *eu-LISA* personāla un darbības izdevumiem (EUR 17,6 miljoni). *Eu-LISA* informēja Komisiju, ka 3 jaunu līgumdarbinieku pieņemšana darbā ir plānota 2018. gada janvārī, lai savlaicīgi varētu sākt izstrādes posmu un nodrošinātu uzlaboto SIS funkciju darbības uzsākšanu 2020. gadā. Šajā priekšlikumā ir paredzēti centrālās SIS tehniskas izmaiņas, lai paplašinātu dažas esošo brīdinājumu kategorijas un ieviestu jaunas funkcijas. Šīs izmaiņas ir atspoguļotas priekšlikumam pievienotajā finanšu pārskatā.

Turklāt Komisija veica izmaksu ietekmes novērtējuma pētījumu, lai novērtētu valstīs veicamo uzlabojumu izmaksas saistībā ar šo priekšlikumu[29]. Aplēstās izmaksas ir EUR 36,8 miljoni, kas, izmantojot vienreizējus maksājumus, jāsadala dalībvalstīm. Tādējādi katra dalībvalsts saņems EUR 1,2 miljonus, lai uzlabotu savu valsts sistēmu saskaņā ar prasībām, kas noteiktas šajā priekšlikumā, tostarp, lai izveidotu daļēju valsts eksemplāru vai rezerves sistēmu, ja tas vēl nav izdarīts.

[29] "IKT ietekmes novērtējums par tehniskiem uzlabojumiem SIS II uzbūvē – nobeiguma ziņojums", *Wavestone*, 2016. gada 10. novembris, 3. risinājums, atsevišķas N.SIS II īstenošana.

Iekšējās drošības fondā paredzētā viedrobežu budžeta atlikuma pārdalīšana ir paredzēta, lai veiktu uzlabojumus un īstenot funkcijas, kas paredzētas abos priekšlikumos. IDF Robežu regula[30] ir finanšu instruments, kurā ir iekļauts budžets viedrobežu tiesību aktu kopuma īstenošanai. Regulas 5. pantā ir paredzēts, ka EUR 791 miljons tiek izmantoti ar programmu IT sistēmu izveidei, ar kurām palīdz pārvaldīt migrācijas plūsmas pāri ārējām robežām saskaņā ar 15. pantā paredzētajiem nosacījumiem. No minētā EUR 791 miljona EUR 480 miljoni ir rezervēti ieceļošanas/izceļošanas sistēmas izstrādei un EUR 210 miljoni - Eiropas ceļošanas informācijas un atļauju sistēmas (*ETIAS*) izveidei. Atlikusī daļa tiks daļēji izmantota, lai segtu abos priekšlikumos paredzēto SIS izmaiņu izdevumus.

5. CITI ELEMENTI

- **Īstenošanas plāni un uzraudzības, izvērtēšanas un ziņošanas kārtība**

Komisija, dalībvalstis un *eu-LISA* regulāri pārskatīs un uzraudzīs SIS izmantošanu, lai nodrošinātu, ka tā joprojām darbojas efektīvi un iedarbīgi. Tehnisko un operatīvo pasākumu īstenošanā, kā aprakstīts šajā priekšlikumā, Komisijai palīdzēs SISVIS komiteja.

Turklāt ierosinātās regulas 71. panta 7. un 8. punktā ir ietverti noteikumi par oficiālu un regulāru pārskatīšanu un novērtēšanas procesu.

Eu-LISA ik pēc diviem gadiem ir pienākums ziņot Eiropas Parlamentam un Padomei par SIS, komunikācijas infrastruktūras, kas atbalsta to, kā arī par divpusējās vai daudzpusējās papildinformācijas apmaiņas starp dalībvalstīm tehnisko darbību, tostarp drošību.

Turklāt, reizi četros gados Komisijai ir pienākums veikt vispārīgu novērtējumu par SIS un informācijas apmaiņu starp dalībvalstīm un informēt par to Parlamentu un Padomi. Tādējādi tiks:

- izskatīta rezultātu atbilstība mērķiem;
- novērtēts, vai sistēmas pamatojums joprojām ir spēkā;
- izskatīts jautājums, kā regula tiek piemērota centrālajai sistēmai;
- novērtēta centrālās sistēmas drošība;
- izpētīta sistēmas turpmākas darbības ietekme.

eu-LISA ir uzticēts pienākums nodrošināt dienas, mēneša un gada statistikas datus par SIS izmantošanu, nodrošinot pastāvīgu sistēmas uzraudzību un tās darbības izvērtēšanu attiecībā pret mērķiem.

- **Konkrētu priekšlikuma noteikumu sīks skaidrojums**

Noteikumi, kas ir kopīgi šim priekšlikumam un Komisijas priekšlikumam Regulai par SIS izveidi, darbību un izmantošanu robežpārbaužu jomā:

- Vispārīgi noteikumi (1. – 3. pants)
- SIS tehniskā arhitektūra un darbības veidi (4. – 14. pants)
- *Eu-LISA* atbildību (15 – 18. pants)
- Piekļuves tiesības un brīdinājumu saglabāšana (43., 46., 48., 50. un 51. pants)

[30] Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Regula (ES) Nr. 515/2014, ar ko kā daļu no Iekšējās drošības fonda izveido finansiāla atbalsta instrumentu ārējām robežām un vīzām (OV L 150, 20.5.2014., 143. lpp.).

- Vispārīgie datu apstrādes un datu aizsardzības noteikumi (53 – 70. pants)
- Uzraudzība un statistika (71. pants)

SIS izmantošana "no viena gala līdz otram"

Ar vairāk nekā 2 miljoniem galalietotāju kompetentajās iestādēs visā Eiropā SIS ir ļoti plaši lietots un efektīvs instruments informācijas apmaiņai. Šie priekšlikumi ietver noteikumus, kas attiecas uz pilnīgu sistēmas darbību no viena gala līdz otram, tostarp uz centrālo SIS, ko uztur *eu-LISA*, valstu sistēmām un galalietotāju lietojumprogrammatūru. Tie skar ne tikai centrālo sistēmu un valstu sistēmas, bet arī galalietotāju tehniskās un operatīvās vajadzības.

Priekšlikuma 9. panta 2. punktā noteikts, ka galalietotāji saņem datus, kas ir vajadzīgi, lai veiktu tiem uzticētos uzdevumus (jo īpaši visus datus, kas vajadzīgi, lai identificētu datu subjektu un veiktu prasītās darbības). Tas paredz arī kopīgu plānu SIS īstenošanai dalībvalstīs, nodrošinot visu valstu sistēmu saskaņotību. Priekšlikuma 6. pantā noteikts, ka katrai dalībvalstij ir jānodrošina nepārtraukta SIS datu pieejamība galalietotājiem, lai palielinātu darbības ieguvumus, samazinot dīkstāves iespējamību.

Priekšlikuma 10. panta 3. punkts nodrošina, ka datu apstrādes drošība attiecas arī uz galalietotāju datu apstrādes darbībām. Priekšlikuma 14. pantā paredzēts, ka dalībvalstis nodrošina tā personāla, kam ir piekļuve SIS, regulāru un pastāvīgu apmācību par datu drošību un datu aizsardzības noteikumiem.

Ņemot vērā šo pasākumu iekļaušanu, šis priekšlikums vispusīgāk aptver SIS pilnīgu darbību no viena gala līdz otram, paredzot noteikumus un pienākumus attiecībā uz miljoniem galalietotāju visā Eiropā. Lai pilnībā efektīvi izmantotu SIS, dalībvalstīm būtu jānodrošina, ka katru reizi, kad to galalietotājiem ir tiesības veikt meklēšanu valsts policijas vai imigrācijas datubāzē, paralēli notiek arī meklēšana SIS. Tādējādi SIS var sasniegt savu mērķi būt par galveno papildinošo pasākumu zonā bez iekšējās robežkontroles, un dalībvalstis var labāk risināt noziedzības un noziedznieku mobilitātes pārrobežu aspektus. Šai paralēlajai meklēšanai jānotiek saskaņā ar Direktīvas (ES) 2016/680 4. pantu[31].

Darbības nepārtrauktība

Priekšlikumi stiprina noteikumus attiecībā uz darbības nepārtrauktību gan valsts, gan *eu-LISA* līmenī (4., 6., 7. un 15. pants). Tie nodrošina, ka SIS arī turpmāk būs funkcionāla un pieejama darbiniekiem uz vietas, pat ja sistēmu skar problēmas.

Datu kvalitāte

Priekšlikums ir balstīts uz principu, ka dalībvalsts, kas ir datu īpašniece, ir arī atbildīga par SIS ievadīto datu pareizību (56. pants). Tomēr ir nepieciešams paredzēt centrālu mehānismu, ko pārvalda *eu-LISA* un kas dalībvalstīm ļauj regulāri pārskatīt brīdinājumus, kurā obligātie datu lauki raisa bažas par kvalitāti. Tāpēc priekšlikuma 15. pants pilnvaro *eu-LISA* regulāri sagatavot datu kvalitātes ziņojumus dalībvalstīm. Šo darbību var atvieglot, izmantojot datu repozitoriju statistikas datu sagatavošanai un datu kvalitātes ziņojumus (71. pants). Šie uzlabojumi atspoguļo starpposma secinājumus, ko pieņēmusi Augsta līmeņa ekspertu grupa jautājumos par informācijas sistēmām un sadarbspēju.

Fotogrāfijas, sejas attēli, daktiloskopiskie dati un DNS profili

[31] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti (OV L 119, 4.5.2016., 89. lpp.).

Iespēja meklēt, izmantojot pirkstu nospiedumus nolūkā identificēt personu jau ir paredzēta 22. pantā Regulā (EK) Nr. 1987/2006 un Padomes Lēmumā 2007/533/TI. Priekšlikumos šī meklēšana ir obligāta, ja personas identitāti nevar noskaidrot nekādā citā veidā. Turklāt 22. panta izmaiņas un jaunais 40., 41. un 42. pants personas identificēšanai papildus pirkstu nospiedumu izmantošanai ļaus izmantot sejas attēlus, plaukstu nospiedumus un DNS profilus. Pašlaik sejas attēlus var izmantot tikai, lai apstiprinātu personas identitāti pēc burtciparu meklēšanas, nevis kā pamatu meklēšanai. Daktiloskopija ir pirkstu nospiedumu zinātniska izpēte kā identifikācijas metode. Daktiloskopijas eksperti atzīst, ka plaukstu nospiedumiem ir raksturīga unikalitāte un ka tie satur atskaites punktus, kas nodrošina precīzu un pārliecinošu salīdzināšanu tieši tāpat kā pirkstu nospiedumi. Plaukstu nospiedumus var izmantot, lai noskaidrotu personas identitāti tādā pašā veidā, kā var izmantot pirkstu nospiedumus. Plaukstu nospiedumu iegūšana kopā ar desmit pirkstu uzspiesto un pārvelto nospiedumu iegūšanu ir policijā izmantota prakse jau vairākus gadu desmitus. Pastāv divi galvenie plaukstu nospiedumu izmantošanas veidi:

i) identifikācijas nolūkos, ja subjektam ir tīši vai nejauši bojāti pirkstu gali. Tas var būt, lai izvairītos no identifikācijas vai pirkstu nospiedumu iegūšanas, vai bojājumu rezultātā, kas radušies nelaimes gadījumā vai smagā fiziskā darbā. Diskusijas gaitā par SIS AFIS tehniskajiem noteikumiem Itālija ziņoja par ievērojamiem panākumiem neatbilstīgo migrantu identificēšanā, kuri ir tīšām bojājuši pirkstu galus, mēģinot izvairīties no identifikācijas. Plaukstu nospiedumu iegūšana Itālijas iestādēm ļāva veikt identifikāciju;

ii) latentie nospiedumi noziedzīga nodarījuma izdarīšanas vietā. Aizdomās turētie bieži atstāj pēdas noziedzīga nodarījuma izdarīšanas vietā, kas atklājas kā plaukstas nospiedumi. Tikai regulāri iegūstot arī plaukstu nospiedumus, kad personai vienlaikus likumīgi tiek noņemti pirkstu nospiedumi, ir iespējams identificēt aizdomās turēto. Plauktas nospiedums parasti arī ir ietvert datus no pirkstu pamatnes, kas bieži vien trūkst uzspiesto un pārvelto pirkstu nospiedumu gadījumā, jo tos parasti iegūst tikai no pirkstu galiem un augšējām pirkstu locītavām.

Sejas attēlu izmantošana identifikācijai nodrošinās lielāku saskaņotību starp SIS un ierosināto ES ieceļošanas/izceļošanas sistēmu, elektroniskajiem vārtiem un pašapkalpošanās iekārtām. Šī funkcija būs pieejama tikai regulārajās robežšķērsošanas vietās.

Gadījumos, kad pirkstu vai plaukstu nospiedumi nav pieejami, 22. panta 1. punkta b) apakšpunkts ļauj izmantot DNS profilus attiecībā uz pazudušām personām, kurām jānodrošina aizsardzība, īpaši bērniem. Šo funkciju var izmantot tikai tad, ja nav pirkstu nospiedumu, un tā būs pieejama tikai pilnvarotiem lietotājiem. Šis noteikums ļauj izmantot pazudušās personas/bērna vecāku vai brāļu un māsu DNS profilus, lai caur tiem dalībvalstu iestādes varētu identificēt un atrast konkrēto personu. Dalībvalstis jau apmainās ar šo informāciju operatīvā līmenī, apmainoties ar papildinformāciju. Šis priekšlikums veido minētās prakses tiesisko regulējumu, iekļaujot to SIS darbības un izmantošanas materiāltiesiskajā pamatā un izveidojot skaidras procedūras saistībā ar apstākļiem, kādos var izmantot šādus profilus.

Ierosinātie grozījumi ļaus izdot SIS brīdinājumus par nezināmām meklētām personām saistībā ar noziedzīgu nodarījumu, pamatojoties uz pirkstu vai plaukstu nospiedumiem (40. – 42. pants). Šādus brīdinājumus var izveidot, ja, piemēram, smaga nozieguma izdarīšanas vietā tiek konstatēti latenti pirkstu vai plaukstu nospiedumi un ir pamatoti iemesli aizdomām, ka pirkstu nospiedumi pieder minētā nozieguma izdarītājam. Piemēram, ja pirkstu nospiedumus atrod uz ieroča, kas izmantots nozieguma izdarīšanā, vai uz jebkura cita priekšmeta, ko izmantojis nozieguma izdarītājs tā izdarīšanas laikā. Šī jaunā brīdinājumu kategorija papildina Prīmes noteikumus, kas padara iespējamu valsts pirkstu nospiedumu identifikācijas sistēmu

savienojamību. Izmantojot Prīmes mehānismu, dalībvalsts var iesniegt pieprasījumu, lai pārliecinātos, vai nozieguma izdarītājs, kuru pirkstu nospiedumi ir atrasti, ir zināms kādā citā dalībvalstī (parasti izmeklēšanas nolūkos). Izmantojot Prīmes mehānismu, personu var identificēt tikai tad, ja viņai citā dalībvalstī ir noņemti pirkstu nospiedumi saistībā ar kriminālu nodarījumu. Tādējādi pirmo reizi likumpārkāpēju nevar identificēt. Šajā priekšlikumā paredzētie jauninājumi, proti, nezināmu meklētu personu pirkstu nospiedumu glabāšana, ļaus nozieguma nezināma izdarītāja pirkstu nospiedumus augšuplādēt SIS, lai viņu varētu identificēt kā meklētu, ja viņš tiek konstatēts citā dalībvalstī. Šīs funkcijas izmantošanas priekšnoteikums ir tas, ka dalībvalstis vispirms ieskatās visos pieejamajos valsts un starptautiskos avotos, taču nav varējušas noteikt attiecīgās personas identitāti. Priekšlikumā ir iekļauti pietiekami aizsardzības pasākumi, lai nodrošinātu to, ka zem šīs kategorijas SIS glabā tikai tādu personu pirkstu nospiedumus, kuras nopietni tiek turētas aizdomās par smaga nozieguma vai teroristu nodarījuma izdarīšanu. Tādēļ šo jauno brīdinājumu kategoriju var atļaut izmantot tikai gadījumos, kad nezināms nozieguma izdarītājs rada ievērojamu apdraudējumu sabiedriskajai drošībai, kas attaisno šo nospiedumu salīdzināšanu ar ceļotāju pirkstu nospiedumiem, piemēram, lai novērstu, ka persona atstāj zonu bez iekšējo robežu kontroles.

Šis noteikums neļauj galalietotājiem ievadīt pirkstu nospiedumus šajā kategorijā, ja to saistība ar nozieguma izdarītāju nav nosakāma. Papildu nosacījums ir tāds, ka attiecīgās personas identitāti nevar noteikt, izmantojot jebkuru citu valsts, Eiropas vai starptautisko datubāzu, kurās uzglabā pirkstu nospiedumus. Ja šādi pirkstu nospiedumi tiek uzglabāti SIS, tos izmantos, lai identificētu personas, kuru identitāti nevar noskaidrot citos veidos. Ja šāda pārbaude noved pie iespējamas atbilstības, dalībvalstij būtu jāveic turpmākas pārbaudes ar attiecīgajiem pirkstu nospiedumiem, iespējams, iesaistot pirkstu nospiedumu ekspertus, lai noteiktu, vai persona ir SIS saglabāto pirkstu nospiedumu īpašnieks, un būtu jānoskaidro personas identitāte. Procedūras piemēro saskaņā ar valsts tiesību aktiem. Ja personu identificē SIS kā "nezināmu meklētu personu", viņu, iespējams, var aizturēt.

Piekļuve SIS

Šajā apakšiedaļā aprakstīti jaunie elementi attiecībā uz kompetento valstu iestāžu un ES aģentūru (institucionālie lietotāji) tiesībām piekļūt SIS.

Valsts iestādes — imigrācijas iestādes

Lai pēc iespējas efektīvāk izmantotu SIS, priekšlikums nodrošina piekļuvi SIS valsts iestādēm, kas izskata un pieņem lēmumus par trešo valstu valstspiederīgo ieceļošanu un uzturēšanos dalībvalstu teritorijā un atgriešanu. Šis papildinājums ļauj ieskatīties SIS saistībā ar neatbilstīgajiem migrantiem, kuri nav pārbaudīti regulāro robežkontroļu laikā. Šis priekšlikums nodrošina vienādu attieksmi pret trešo valstu valstspiederīgajiem, kuri šķērso ārējās robežas regulārās robežšķērsošanas vietās (un tādējādi ir pakļauti pārbaudēm, kas piemērojamas trešo valstu valstspiederīgajiem), un trešo valstu valstspiederīgajiem, kas neatbilstīgi ierodas Šengenas zonā.

Turklāt šis priekšlikums nodrošina, ka transportlīdzekļu, laivu un gaisa kuģu reģistrācijas iestādēm (44. pants) ir ierobežota piekļuve sistēmai, lai veiktu savus pienākumus, ar nosacījumu, ka tās ir valsts dienesti. Tas ļaus izvairīties no minēto satiksmes līdzekļu reģistrācijas, ja tie ir nozagti un tiek meklēti citā dalībvalstī. Attiecībā uz transportlīdzekļu reģistrācijas dienestiem šī iniciatīva nav jauna, jo to piekļuve SIS jau bija paredzēta Šengenas

Konvencijas 102.a pantā un Regulā (EK) Nr. 1986/2006[32]. Ievērojot to pašu loģiku, priekšlikums paredz laivu un gaisa kuģu reģistrācijas iestādēm piekļuvi SIS brīdinājumiem par laivām un gaisa kuģiem.

Institucionālie lietotāji

Eiropolam (46. Pants), *Eurojust* (47. pants) un Eiropas Robežu un krasta apsardzes aģentūrai – kā arī tās vienībām, tāda personāla vienībām, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, un migrācijas pārvaldības atbalsta vienības dalībniekiem – (48. un 49. pants) ir piekļuve SIS un tām nepieciešamajiem SIS datiem. Ir ieviesti atbilstīgi aizsardzības pasākumi, lai nodrošinātu to, ka datus sistēmā pienācīgi aizsargā (tostarp arī 50. pantā paredzētie noteikumi, proti, prasība, ka šādas iestādes var piekļūt vienīgi tiem datiem, kas ir vajadzīgi to uzdevumu veikšanai).

Šīs izmaiņas paplašina Eiropola piekļuvi SIS, aptverot brīdinājumus par pazudušām personām un tādējādi nodrošinot, ka tas var pēc iespējas labāk izmantot sistēmu savu pienākumu veikšanā, un pievieno jaunus noteikumus, lai nodrošinātu, ka Eiropas Robežu un krasta apsardzes aģentūra un tās vienības var piekļūt sistēmai, veicot dažādas darbības saskaņā ar savām pilnvarām palīdzēt dalībvalstīm. Saistībā ar darbu, ko veic Augsta līmeņa ekspertu grupa jautājumos par informācijas sistēmām un sadarbspēju, un lai turpinātu stiprināt informācijas apmaiņu par terorismu, Komisija izvērtēs, vai Eiropolam būtu automātiski jāsaņem paziņojumi no SIS, kad tiek izveidots brīdinājums par darbību saistībā ar terorismu.

Turklāt saskaņā ar Komisijas priekšlikumu Eiropas Parlamenta un Padomes Regulai, ar ko izveido Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*)[33], Eiropas robežu un krasta apsardzes aģentūras *ETIAS* centrālā vienība, izmantojot *ETIAS*, veiks meklēšanu SIS, lai pārliecinātos, vai uz trešās valsts valstspiederīgo, kurš iesniedz ceļošanas atļaujas pieteikumu, neattiecas SIS brīdinājums. Tālab *ETIAS* centrālajai vienībai arī būs pilna piekļuve SIS.

Konkrētas izmaiņas brīdinājumos

Saskaņā ar 26. pantu dalībvalstis var uz laiku apturēt brīdinājumus par apcietināšanu (ja notiek policijas operācija vai izmeklēšana), padarot tos uz ierobežotu laiku pieejamus *SIRENE* birojiem, bet ne darbiniekiem uz vietas. Šis noteikums palīdz izvairīties no situācijas, ka konfidenciālu policijas operāciju īpaši meklēta noziedznieka aizturēšanai apdraud policijas darbinieks, kurš nav iesaistīts konkrētajā lietā.

Priekšlikuma 32. un 33. pants paredz brīdinājumus par pazudušām personām. Izmaiņas šajos noteikumos ļauj izdot preventīvus brīdinājumus gadījumos, kad ir paaugstināts risks, ka viens no vecākiem var nolaupīt bērnu, un nodrošina precīzāku pazudušo personu brīdinājumu sadali par kategorijām. Vecāku veikta nolaupīšana bieži notiek ļoti plānotos apstākļos ar mērķi ātri atstāt dalībvalsti, kurā panākta vienošanās par aizgādību. Šie grozījumi novērš iespējamo nepilnību pašreizējos tiesību aktos, kas paredz, ka brīdinājumus par bērniem var izdot tikai tad, kad viņi jau ir pazuduši. Tas ļaus iestādēm dalībvalstīs norādīt īpašam riskam pakļautus bērnus. Šīs izmaiņas nozīmē, ka gadījumos, kad pastāv augsts nenovēršams risks, ka viens no vecākiem varētu nolaupīt bērnu, robežsardzes un tiesībaizsardzības iestāžu amatpersonas ir informētas par šo risku un varēs rūpīgāk pārbaudīt apstākļus, kad riskam pakļauts bērns dodas

[32] Eiropas Parlamenta un Padomes Regula (EK) Nr. 1986/2006 (2006. gada 20. decembris) par dalībvalstu dienestu, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izsniegšanu, piekļuvi otrās paaudzes Šengenas Informācijas sistēmai (SIS II) (OV L 381, 28.12.2006., 1. lpp.).

[33] COM(2016) 731 *final*.

ceļojumā, nepieciešamības gadījumā aizturot bērnu aizsardzības nolūkos. *SIRENE* biroji nodrošinās papildinformāciju, tostarp tās kompetentās tiesu iestādes lēmumu, kas pieprasījusi brīdinājumu. *SIRENE* rokasgrāmatu attiecīgi pārskatīs. Šim brīdinājumam būs vajadzīgs attiecīgs tiesu iestāžu lēmums par aizgādības piešķiršanu tikai vienam no vecākiem. Papildu nosacījums ir tāds, ka pastāv nenovēršams nolaupīšanas risks. Brīdinājumus par pazudušiem bērniem automātiski atjauninās, lai attiecīgos gadījumos atspoguļotu faktu, ka viņi ir sasnieguši pilngadību.

Priekšlikuma 34. pants ļauj brīdinājumam pievienot datus par transportlīdzekļiem, ja ir skaidra norāde, ka tie ir saistīti ar meklēto personu.

Priekšlikuma 37. pantā ir ieviests jauns pārbaudes veids "izmeklēšanas pārbaude". Tas ir īpaši paredzēts, lai atbalstītu pasākumus cīņā pret terorismu un smagiem noziegumiem. Tas ļauj iestādēm apturēt un nopratināt attiecīgo personu. Tā ir dziļāka pārbaude par pašreizējo diskrēto pārbaudi, bet neietver personas pārmeklēšanu un nevainagojas ar viņas aizturēšanu. Tomēr tā var sniegt pietiekamu informāciju, kas ļauj pieņemt lēmumu par turpmāku rīcību. Ir grozīts arī 36. pants, lai atspoguļotu šo papildu pārbaudes veidu.

Šis priekšlikums paredz, kas noteikums par SIS brīdinājumiem attiecas uz oficiālu dokumentu veidlapām un izdotiem personu apliecinošiem dokumentiem (36. pants) un transportlīdzekļiem, tostarp laivām un gaisa kuģiem (32., 34. pants), ja tie ir saistīti ar brīdinājumiem par personām, kas izdoti saskaņā ar šiem pantiem. Ir grozīts 37. pants, lai noteiktu darbības, kas jāveic, pamatojoties uz šiem brīdinājumiem. Tas ir darīts izmeklēšanas nolūkos, jo ļaus iestādēm risināt situācijas, kad vairākas personas izmanto autentiskus, bet savā starpā līdzīgus dokumentus, nebūdamas to likumīgās turētājas.

Priekšlikuma 38. pantā iekļauts paplašināts to priekšmetu saraksts, par kuriem var izdot brīdinājumu, pievienojot sarakstā viltotus dokumentus, transportlīdzekļus neatkarīgi no to piedziņas sistēmas (t. i., elektriskos, kā arī benzīna/dīzeļdegvielas utt.), viltotas banknotes, IT aprīkojumu un identificējamas transportlīdzekļu un rūpniecības iekārtu detaļas. Vairs nav iekļauti brīdinājumi par maksāšanas līdzekļiem, jo šo brīdinājumu efektivitāte bija ļoti zema un par tiem tikpat kā nav bijuši trāpījumi.

Lai precizētu procedūru, kas jāievēro, kad priekšmets, uz kuru attiecas brīdinājums, ir atrasts, ir grozīts 39. pants, nosakot, ka priekšmeti ir jāizņem saskaņā ar valsts tiesību aktiem, papildus sazinoties ar iestādi, kas izdevusi brīdinājumu.

Datu aizsardzība un drošība

Šajā priekšlikumā ir precizēta atbildība par starpgadījumu novēršanu, ziņošanu par tiem un reaģēšanu uz starpgadījumiem, kas varētu ietekmēt SIS infrastruktūras, SIS datu vai papildinformācijas drošību vai integritāti (10., 16. un 57. pants).

Priekšlikuma 12. pantā iekļauti noteikumi par ierakstu glabāšanu un meklēšanu ierakstos par brīdinājumu vēsturi.

Minētajā 12. pantā arī iekļauti noteikumi par automatizētu transportlīdzekļu numuru zīmju skenēšanas meklēšanu, izmantojot automatizētas numura zīmes atpazīšanas sistēmas, paredzot dalībvalstīm pienākumu glabāt ierakstus par šādu meklēšanu saskaņā ar valsts tiesību aktiem.

Priekšlikuma 15. panta 3. punktā saglabāts Padomes Lēmuma 2007/533/TI 15. panta 3. punkta teksts, un tas paredz, ka Komisija ir atbildīga par komunikācijas infrastruktūras līgumisko pārvaldību, tostarp par uzdevumiem, kas saistīti ar budžeta izpildi, iegādēm un atjaunošanu. Šie uzdevumi tiks nodoti *eu-LISA* priekšlikumu otrajā fāzē 2017. gada jūnijā.

Attiecībā uz lēmumiem par brīdinājumu derīguma termiņa pagarināšanu priekšlikuma 21. pantā ir paplašināta prasība apsvērt, vai gadījums ir pietiekami atbilstīgs, piemērots un

svarīgs. Jauninājums šajā pantā ir prasība dalībvalstīm vienmēr izveidot brīdinājumu attiecīgi saskaņā ar 34., 36. un 38. pantu par personām vai ar tām saistītiem priekšmetiem, ja personu darbībām piemērojams Padomes Pamatlēmuma 2002/475/TI par terorisma apkarošanu 1., 2., 3. un 4. pants.

Datu kategorijas un datu apstrāde

Šis priekšlikums paplašina informācijas veidus (20. pants), ko var glabāt par personām, attiecībā uz kurām ir izdots brīdinājums, papildus ietverot arī:

- informāciju par to, vai persona ir iesaistīta darbībās, uz kurām attiecas 1., 2., 3. un 4. pants Padomes Pamatlēmumā 2002/475/TI;
- citas ar personu saistītas piezīmes; brīdinājuma iemeslu;
- ziņas par personas valsts reģistrācijas numuru un reģistrācijas vietu;
- pazudušas personas gadījuma veidu (tikai attiecībā uz brīdinājumiem, kas minēti 32. pantā);
- sīkāku informāciju par personas identitātes vai ceļošanas dokumentu;
- personas identitātes vai ceļošanas dokumenta krāsu kopiju;
- DNS profilus (tikai tad, ja nav pieejami identifikācijai piemēroti pirkstu nospiedumi).

Priekšlikuma 59. pantā paplašināts arī to personas datu saraksts, kurus var ievadīt un apstrādāt SIS, lai risinātu jautājumu par identitātes ļaunprātīgu piesavināšanos. Šos datus var ievadīt tikai ar tās personas piekrišanu, kas cietusi no identitātes ļaunprātīgas izmantošanas. Tagad šie dati aptver arī:

- sejas attēlus;
- plaukstu nospiedumus;
- ziņas par personu apliecinošiem dokumentiem;
- cietušā adresi;
- cietušā tēva un mātes vārdu.

Priekšlikuma 20. pants paredz detalizētāku informāciju brīdinājumos. Tas ietver informāciju par datu subjekta personu apliecinošiem dokumentiem un atļauju, ņemot vērā pazušanas veidu, iedalīt kategorijās pazudušus bērnus, piemēram, nepavadīti nepilngadīgie, vecāka veikta nolaupīšana, aizbēguši bērni utt. Tas ir ļoti svarīgi, lai galalietotāji šo bērnu aizsardzībai varētu veikt nepieciešamos pasākumus bez jebkādas kavēšanās. Šī paplašinātā informācija ļauj labāk identificēt attiecīgo personu, un, no otras puses, ļauj galalietotājiem pieņemt uz informāciju balstītu lēmumu. Pārbaudes veicošo galalietotāju aizsardzībai SIS parādīs, vai persona, attiecībā uz kuru ir izdots brīdinājums, atbilst kādai no kategorijām, kas paredzētas 1., 2., 3. un 4. pantā Padomes Pamatlēmumā 2002/475/TI par terorisma apkarošanu[34].

Priekšlikumā ir skaidri norādīts, ka dalībvalstis nedrīkst kopēt datus, ko ir ievadījusi cita dalībvalsts, savās valsts datu datnēm (53. pants).

[34] Padomes Pamatlēmums 2002/475/TI (2002. gada 13. jūnijs) par terorisma apkarošanu (OV L 164, 22.6.2002., 3. lpp.).

Saglabāšana

Maksimālais datu saglabāšanas periods brīdinājumiem par personām tiks pagarināts līdz pieciem gadiem, izņemot brīdinājumus par diskrētām, izmeklēšanas vai īpašām pārbaudēm, kur saglabāšanas periods paliks viens gads. Dalībvalstis vienmēr var noteikt īsākus termiņus. Pagarinātais maksimālais termiņš atbilst valstu praksei pagarināt termiņu, ja brīdinājums vēl nav izpildījis savu mērķi, kamēr attiecīgā persona joprojām tiek meklēta. Turklāt bija nepieciešams pielāgot SIS saglabāšanas periodus ar termiņiem citos tiesību aktos, piemēram, Atgriešanas direktīvā un *Eurodac*. Pārredzamības un skaidrības labad ir nepieciešams paredzēt vienu un to pašu saglabāšanas periodu brīdinājumiem par personām, izņemot brīdinājumus par diskrētām, izmeklēšanas vai īpašām pārbaudēm. Saglabāšanas perioda pagarinājums neapdraud datu subjektu intereses, jo brīdinājumu nevar glabāt ilgāk, nekā tas ir nepieciešams tā mērķa sasniegšanai. Brīdinājumu dzēšanas noteikumi ir skaidri izklāstīti 52. pantā. Savukārt 51. pantā ir noteikti termiņi brīdinājumu pārskatīšanai un paredzēts saīsināts saglabāšanas periods brīdinājumiem par priekšmetiem. Ņemot vērā to, ka nav operatīvu vajadzību brīdinājumus par priekšmetiem glabāt ilgāk, saglabāšanas periods ir samazināts līdz pieciem gadiem atbilstoši brīdinājumiem par personām. Periods attiecībā uz izdotiem dokumentiem un oficiālu dokumentu veidlapām tomēr paliek 10 gadi, jo dokumentu derīguma termiņš ir 10 gadi.

Dzēšana

Priekšlikuma 52. pantā ir noteikti apstākļi, kādos brīdinājumi ir jāizdzēš, harmonizējot valstu praksi šajā jomā. Priekšlikuma 51. pantā paredzēti īpaši noteikumi *SIRENE* biroja darbiniekiem, kuriem proaktīvi jādzēš brīdinājumi, kas vairs nav vajadzīgi, ja nav saņemta atbilde no kompetentajām iestādēm.

Datu subjekta tiesības piekļūt datiem, labot neprecīzus datus un dzēst nelikumīgi saglabātus datus)

Noteikumi par datu subjekta tiesībām paliek nemainīgi, jo pašreizējie noteikumi jau nodrošina augstu aizsardzības līmeni un ir saskaņā ar Regulu (ES) Nr. 2016/679[35] un Direktīvu 2016/680[36]. Papildus minētajam 63. pantā ir noteikti apstākļi, kādos dalībvalstis var nolemt nedarīt zināmu informāciju datu subjektiem. To var darīt, pamatojoties uz kādu no iemesliem, kas uzskaitīti šajā pantā, un šim pasākumam ir jābūt samērīgam un nepieciešamam saskaņā ar valsts tiesību aktiem.

Informācijas apmaiņa ar Interpolu par pazaudētiem, nozagtiem un nelikumīgi piesavinātiem dokumentiem.

Priekšlikuma 63. pants pilnībā saglabā Padomes Lēmuma 2007/533/TI 55. panta tekstu, jo SIS dokumentu sadaļas labāka sadarbspēja ar Interpola Zagto un pazaudēto ceļošanas dokumentu datubāzi tiks apskatīta Augsta līmeņa ekspertu grupas paziņojumā un otrajā SIS priekšlikumu paketē, ko iesniegs 2017. gada jūnijā.

Statistika

---

35 Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

36 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti (OV L 119, 4.5.2016., 89. lpp.).

Lai saglabātu pārskatu par to, kā darbojas tiesiskās aizsardzības līdzekļi, 66. pantā, ir paredzēti noteikumi par standarta statistikas sistēmu, lai sniegtu ikgadējus ziņojumus par:

- datu subjekta piekļuves pieprasījumiem;
- pieprasījumiem labot neprecīzus datus un dzēst nelikumīgi saglabātus datus;
- tiesā ierosinātām lietām;
- lietām, kurās tiesa lēmusi par labu prasītājam; un
- novērojumiem saistībā ar citu dalībvalstu tiesu vai iestāžu pieņemto galīgo lēmumu attiecībā uz brīdinājumiem, kurus izveidojusi brīdinājuma izdevēja dalībvalsts, savstarpējas atzīšanas gadījumiem.

Uzraudzība un statistika

Priekšlikuma 71. pantā ir izklāstīta kārtība, kas jāievēro, lai nodrošinātu pienācīgu SIS darbības un tās mērķu sasniegšanas uzraudzību. Šim nolūkam *eu-LISA* uzdevums ir sniegt dienas, mēneša un gada statistiku par to, kā sistēmu izmanto.

Priekšlikuma 71. panta 5. punktā noteikts, ka *eu-LISA* sniedz dalībvalstīm, Komisijai, Eiropolam un Eiropas Robežu un krasta apsardzes aģentūrai statistikas ziņojumus un Komisija var pieprasīt papildu statistikas datus un datu kvalitātes ziņojumus par SIS un *SIRENE* saziņu.

Priekšlikuma 71. panta 6. punkts paredz izveidot un uzturēt centrālo datu repozitāriju *eu-LISA* veiktās SIS darbības uzraudzības ietvaros. Tas ļaus dalībvalstu pilnvarotiem darbiniekiem, Komisijai, Eiropolam, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūrai piekļūt 71. panta 3. punktā minētajiem datiem, lai sagatavotu prasītos statistikas pārskatus.

2016/0409 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par Šengenas Informācijas sistēmas (SIS) izveidi, darbību un izmantošanu policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās, ar ko groza Regulu (ES) Nr. 515/2014 un atceļ Regulu (EK) Nr. 1986/2006, Padomes Lēmumu 2007/533/TI un Komisijas Lēmumu 2010/261/ES

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 82. panta 1. punkta pirmās daļas d) punktu, 85. panta 1. punktu, 87.panta 2.punkta a) apakšpunktu un 88. panta 2. punkta a) apakšpunktu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Šengenas informācijas sistēma (SIS) ir Eiropas Savienības satvarā integrēto Šengenas *acquis* noteikumu svarīgs piemērošanas rīks. SIS ir viens no galvenajiem papildu pasākumiem, kas palīdz uzturēt augstu drošības līmeni Eiropas Savienības brīvības, drošības un tiesiskuma telpā, atbalstot robežsardzes, policijas, muitas un citu tiesībaizsardzības iestāžu un tiesu iestāžu operatīvo sadarbību krimināllietās.

(2) SIS tika izveidota saskaņā ar IV sadaļas noteikumiem 1990. gada 19. jūnija Konvencijā, ar kuru īsteno Šengenas 1985. gada 14. jūnija Nolīgumu starp Beniluksa Ekonomikas savienības valstu valdībām, Vācijas Federatīvās Republikas valdību un Francijas Republikas valdību par pakāpenisku kontroles atcelšanu pie kopīgām robežām[37] (Šengenas Konvencija). Otrās paaudzes SIS (SIS II) izveide tika uzticēta Komisijai saskaņā ar Padomes Regulu (EK) Nr. 2424/2001[38] un Padomes Lēmumu

[37] OV L 239, 22.9.2000., 19. lpp. Konvencija ar grozījumiem, kas izdarīti ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1160/2005 (OV L 191, 22.7.2005., 18. lpp.).

[38] OV L 328, 13.12.2001., 4. lpp.

2001/886/TI[39] un to izveidoja ar Regulu (EK) Nr. 1987/2006[40] un Padomes Lēmumu 2007/533/TI[41]. SIS II aizstāja SIS, kas bija izveidota saskaņā ar Šengenas Konvenciju.

(3) Trīs gadus pēc SIS II darbības sākšanas Komisija veica sistēmas novērtējumu saskaņā ar Regulas (EK) Nr. 1987/2006 24. panta 5. punktu, 43. panta 5. punktu un 50. panta 5. punktu un Lēmuma 2007/533/TI 59. pantu un 65. panta 5. punktu. Novērtējuma ziņojums un saistītais dienestu darba dokuments tika pieņemti 2016. gada 21. decembrī[42]. Ieteikumi, kas izklāstīti šajos dokumentos attiecīgos gadījumos būtu jāatspoguļo šajā regulā.

(4) Šī regula ir nepieciešamais tiesiskais pamats SIS pārvaldībai attiecībā uz jautājumiem, uz ko attiecas Līguma par Eiropas Savienības darbību V daļas 4. un 5. sadaļa. Eiropas Parlamenta un Padomes Regula (ES) Nr. 2018/... par Šengenas informācijas sistēmas (SIS) izveidi, darbību un izmantošanu robežpārbaužu jomā[43], ir nepieciešamais tiesiskais pamats SIS pārvaldībai attiecībā uz jautājumiem, uz ko attiecas Līguma par Eiropas Savienības darbību V daļas 2. sadaļa.

(5) Tas, ka tiesisko pamatu, kas nepieciešams SIS II pārvaldībai, veido atsevišķi akti, neskar principu, ka SIS ir vienota informācijas sistēma, kurai kā tādai būtu jādarbojas. Tāpēc dažiem šo aktu noteikumiem būtu jābūt identiskiem.

(6) Vajadzētu precizēt SIS II mērķus, tās tehnisko uzbūvi un finansējumu, paredzēt noteikumus par tās darbību no viena gala līdz otram un izmantošanu un noteikt pienākumus, sistēmā ievadāmo datu kategorijas, datu ievadīšanas mērķus, ievadīšanas kritērijus, iestādes, kam ir tiesības piekļūt datiem, biometrisko identifikatoru izmantošanu un citus noteikumus par datu apstrādi.

(7) SIS sastāv no centrālās sistēmas (centrālā SIS) un valstu sistēmām ar pilnīgu vai daļēju SIS datubāzes kopiju. Ņemot vērā to, ka SIS ir vissvarīgākais informācijas apmaiņas rīks Eiropā, ir jānodrošina tās nepārtraukta darbība gan centrālajā, gan valstu līmenī. Tādēļ katrai dalībvalstij būtu jāizveido pilnīga vai daļēja SIS datubāzes kopija un jāuztur rezerves sistēma.

(8) Ir nepieciešams sagatavot rokasgrāmatu ar sīki izstrādātiem noteikumiem par konkrētas papildinformācijas apmaiņu attiecībā uz to, kā jārīkojas brīdinājuma gadījumā. Valsts iestādēm katrā dalībvalstī (*SIRENE* birojs) būtu jānodrošina šādas informācijas apmaiņa.

(9) Lai nodrošinātu efektīvu apmaiņu ar papildinformāciju par to, kā jārīkojas konkrēta brīdinājuma gadījumā, ir lietderīgi stiprināt *SIRENE* biroju darbību, precizējot prasības attiecībā uz pieejamajiem resursiem, lietotāju apmācību un reakcijas laiku uz jautājumiem, kas saņemti no citiem *SIRENE* birojiem.

---

39 Padomes Lēmums 2001/886/TI (2001. gada 6. decembris) par otrās paaudzes Šengenas Informācijas Sistēmas (SIS II) izstrādi (OV L 328, 13.12.2001., 1. lpp.)

40 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 (OV L 181, 28.12.2006., 4. lpp.).

41 Padomes Lēmums 2007/533/TI (2007. gada 12. jūnijs) par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) izveidi, darbību un izmantošanu (OV L 205, 7.8.2007., 63. lpp.).

42 Ziņojums Eiropas Parlamentam un Padomei par otrās paaudzes Šengenas Informācijas sistēmu (SIS II) saskaņā ar Regulas (EK) Nr. 1987/2006 24. panta 5. punktu, 43. panta 5. punktu un 50. panta 5. punktu un Lēmuma 2007/533/TI 59. panta 3. punktu un 66. panta 5. punktu un pievienotais Komisijas dienestu darba dokuments. (OV...).

43 Regula (ES) Nr. 2018/…

(10) SIS centrālo komponentu darbības pārvaldību īsteno Eiropas Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā[44] (Aģentūra). Lai Aģentūra varētu piešķirt nepieciešamos finanšu resursus un personālu, kas aptvertu visus centrālās SIS darbības pārvaldības aspektus, šajā regulā būtu detalizēti jāizklāsta Aģentūras uzdevumi, jo īpaši attiecībā uz papildinformācijas apmaiņas tehniskajiem aspektiem.

(11) Neskarot dalībvalstu atbildību par SIS ievadīto datu precizitāti, Aģentūrai būtu jāuztic atbildība par datu kvalitātes uzlabošanu, ieviešot centrālu datu kvalitātes uzraudzības instrumentu, un regulāru ziņojumu sniegšanu dalībvalstīm.

(12) Lai nodrošinātu labāku SIS izmantošanas pārraudzību nolūkā analizēt noziedzīgu nodarījumu tendences, Aģentūras spējām sniegt dalībvalstīm, Komisijai un Eiropas Robežu un krasta apsardzes aģentūrai statistikas ziņojumus būtu jāatbilst jaunākajam tehnikas līmenim, neietekmējot datu integritāti. Tādēļ būtu jāizveido centrālās statistikas reģistrs. Apkopotajā statistikā nebūtu jāietver personas dati.

(13) SIS būtu jāiekļauj papildu datu kategorijas, kas ļauj galalietotājiem, pamatojoties uz brīdinājumu un nezaudējot laiku, pieņemt uz informāciju balstītus lēmumus. Tāpēc, lai atvieglotu personu identifikāciju un atklātu personas, kas izmanto vairākas identitātes, datu kategorijās, kas attiecas uz personām, būtu jāiekļauj atsauce uz personu apliecinošu dokumentu vai tā numuru un šā dokumenta kopija, ja pieejama.

(14) SIS nebūtu jāglabā visi dati, kas izmantoti meklēšanā, izņemot ierakstu glabāšanu, lai pārbaudītu, vai meklēšana ir likumīga, uzraudzītu datu apstrādes likumību, veiktu pašuzraudzību un nodrošinātu N.SIS pareizu darbību, kā arī datu integritāti un drošību.

(15) SIS vajadzētu būt iespējai apstrādāt biometriskos datus, lai palīdzētu ticami identificēt attiecīgas personas. Šai sakarā SIS vajadzētu būt arī iespējai apstrādāt to personu datus, kuru identitāte ir ļaunprātīgi izmantota (lai novērstu nepareizas identifikācijas dēļ radušās grūtības), ievērojot attiecīgas garantijas; jo īpaši ar attiecīgās personas piekrišanu un stingru to mērķu ierobežošanu, kuros šādus datus var apstrādāt.

(16) Dalībvalstīm būtu jāveic vajadzīgie tehniskās sagatavošanās darbi, lai katru reizi, kad galalietotājiem ir tiesības veikt meklēšanu valsts policijas vai imigrācijas datubāzē, viņi paralēli meklētu arī SIS saskaņā ar 4. pantu Eiropas Parlamenta un Padomes Direktīvā (ES) 2016/680[45]. Tam būtu jānodrošina, ka SIS darbojas kā galvenais papildu pasākums zonā bez iekšējās robežkontroles un labāk risina noziedzības un noziedznieku mobilitātes pārrobežu aspektu.

(17) Šajā regulā būtu jāparedz daktiloskopisko datu un sejas attēlu izmantošanas nosacījumi identifikācijas nolūkiem. Sejas attēlu izmantošanai SIS identifikācijas nolūkos būtu arī jāpalīdz nodrošināt robežkontroles procedūru konsekvenci, kad ir nepieciešama identifikācija un identitātes pārbaude, izmantojot pirkstu nospiedumus un sejas attēlus. Daktiloskopisko datu meklēšanai vajadzētu būt obligātai, ja pastāv

---

[44] Izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1077/2011 (2011. gada 25. oktobris), ar ko izveido Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (OV L 286, 1.11.2011., 1. lpp.).

[45] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI, OV L 119, 4.5.2016. (OV L 119, 4.5.2016., 89. lpp.).

šaubas par personas identitāti. Sejas attēli identifikācijas nolūkā būtu jāizmanto tikai saistībā ar regulāro robežkontroli pašapkalpošanās iekārtās un elektroniskajos vārtos.

(18) Automatizēta pirkstu nospiedumu identifikācijas pakalpojuma ieviešana SIS papildina Prīmes mehānismu savstarpējai pārrobežu tiešsaistes piekļuvei valstu DNS datu bāzēm un automatizētajām pirkstu nospiedumu identifikācijas sistēmām[46]. Prīmes mehānisms dara iespējamu valstu pirkstu nospiedumu identifikācijas sistēmu starpsavienojamību, ar kuras palīdzību dalībvalsts var iesniegt pieprasījumu, lai noskaidrotu, vai nozieguma izdarītājs, kura pirkstu nospiedumi ir atrasti, ir zināms kādā citā dalībvalstī. Prīmes mehānisms pārbauda, vai pirkstu nospiedumu īpašnieks ir zināms konkrētā brīdī, tāpēc, ja noziedzīgā nodarījuma izdarītājs kādā no dalībvalstīm kļūst zināms vēlāk – viņš sistēmā visdrīzāk nebūs ietverts. SIS pirkstu nospiedumu meklēšana pieļauj izdarītāja aktīvu meklēšanu. Tādēļ būtu jāparedz iespēja augšupielādēt SIS nezināma izdarītāja pirkstu nospiedumus, ar nosacījumu, ka pirkstu nospiedumu īpašnieku var identificēt ar augstu varbūtības pakāpi kā personu, kas izdarījusi smagu noziegumu vai terorisma aktu. Tas jo īpaši attiecas uz gadījumu, kad pirkstu nospiedumus atrod uz ieroča vai jebkura cita objekta, kas izmantots nodarījumā. Vienkārša pirkstu nospiedumu atrašanās nozieguma vietā nebūtu jāuzskata par norādi uz augstu varbūtības pakāpi, ka konkrētie pirkstu nospiedumi ir izdarītāja pirkstu nospiedumi. Vēl viens priekšnoteikums, lai izveidotu šādu brīdinājumu būtu, ka izdarītāja identitāti nevar noteikt, izmantojot jebkuru citu valsts, Eiropas vai starptautisko datu bāzi. Ja šāda pirkstu nospieduma meklēšana noved pie iespējamas atbilstības, dalībvalstij būtu jāveic turpmākas pārbaudes ar attiecīgajiem pirkstu nospiedumiem, iespējams, iesaistot pirkstu nospiedumu ekspertus, lai noteiktu, vai persona ir SIS saglabāto pirkstu nospiedumu īpašnieks, un būtu jānoskaidro personas identitāte. Procedūras būtu jāpiemēro saskaņā ar valsts tiesību aktiem. Identifikācija par "nezināmu meklētu personu" SIS var būtiski palīdzēt izmeklēšanā, un var novest līdz apcietināšanai ar nosacījumu, ka visi apcietināšanas nosacījumi ir izpildīti.

(19) Pirkstu nospiedumus, kas atrasti noziedzīga nodarījuma izdarīšanas vietā, būtu jāatļauj salīdzināt ar pirkstu nospiedumiem, kas glabājas SIS, ja tiek konstatēta augstu varbūtības pakāpe, ka tie ir smaga nozieguma vai teroristu nodarījuma izdarītāja pirkstu nospiedumi. Ar jēdzienu "smags noziegums" būtu jāsaprot nodarījumi, kas minēti Padomes Pamatlēmumā 2002/584/TI[47], un ar jēdzienu "teroristu nodarījumi" būtu jāsaprot valstu tiesību aktos noteikti nodarījumi, kas minēti Padomes Pamatlēmumā 2002/475/TI[48].

(20) Gadījumos, kad daktiloskopiskie dati nav pieejami, vajadzētu būt iespējai pievienot DNS profilu, kas būtu pieejams tikai pilnvarotiem lietotājiem. DNS profiliem būtu jāatvieglo pazudušu personu identifikācija, kurām vajadzīga aizsardzība, jo īpaši pazudušu bērnu identifikācija, tostarp atļaujot identifikācijai izmantot vecāku vai brāļu un māsu DNS profilus. DNS datos nebūtu jāiekļauj atsauce uz rases piederību.

---

46 Padomes Lēmums 2008/615/TI (2008. gada 23. jūnijs) par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu un pārrobežu noziedzību (OV L 210, 6.8.2008., 1. lpp.). un Padomes Lēmums 2008/616/TI (2008. gada 23. jūnijs) par to, kā īstenot Lēmumu 2008/615/TI par pārrobežu sadarbības pastiprināšanu, jo īpaši – apkarojot terorismu un pārrobežu noziedzību (OV L 210, 6.8.2008., 12. lpp.).

47 Padomes Pamatlēmums 2002/584/TI (2002. gada 13. jūnijs) par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm (OV L 190, 18.7.2002., 1. lpp.).

48 Padomes Pamatlēmums 2002/475/TI (2002. gada 13. jūnijs) par terorisma apkarošanu (OV L 164, 22.6.2002., 3. lpp.).

(21) SIS būtu jāietver brīdinājumi par personām, kuras meklē apcietināšanai nolūkā tās nodot vai izdot. Papildus brīdinājumiem ir lietderīgi paredzēt tādas papildinformācijas apmaiņu, kas nepieciešama nodošanas un izdošanas procedūrās. SIS jo īpaši būtu jāapstrādā dati, kas minēti 2002. gada 13. jūnija Padomes Pamatlēmuma 2002/584/TI par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm[49] 8.pantā. Operatīvu iemeslu dēļ ir lietderīgi, ka izdevēja dalībvalsts brīdinājumu par apcietināšanu uz laiku padara nepieejamu, ja ir saņemta tiesu iestādes atļauja gadījumos, kad kāda persona, uz kuru attiecas Eiropas apcietināšanas orderis, tiek intensīvi un aktīvi meklēta un galalietotāji, kas nav iesaistīti konkrētajā meklēšanas operācijā, var apdraudēt sekmīgu iznākumu. Šādu brīdinājumu pagaidu nepieejamībai nebūtu jāpārsniedz 48 stundas.

(22) Vajadzētu būt iespējai SIS pievienot tulkojumu papildu datiem, kas ievadīti, lai personu nodotu saskaņā ar Eiropas apcietināšanas orderi un lai personu izdotu.

(23) SIS vajadzētu būt brīdinājumiem par pazudušajām personām, lai nodrošinātu šo personu aizsardzību vai novērstu draudus sabiedriskajai drošībai. Brīdinājumu izdošana SIS par nolaupīšanas riskam pakļautiem bērniem (t. i., lai novērstu turpmāku kaitējumu, kas vēl nav iestājies, piemēram, attiecībā uz bērniem, kuriem draud nolaupīšanu, ko veic viens no vecākiem) būtu jāierobežo, tādēļ ir lietderīgi paredzēt stingrus un piemērotus aizsardzības pasākumus. Attiecībā uz bērniem šiem brīdinājumiem un attiecīgajām procedūrām būtu jākalpo bērna interesēm, ņemot vērā Pamattiesību hartas 24. pantu un Eiropas Savienības un Apvienoto Nāciju Organizācijas 1989. gada 20. novembra Konvenciju par bērna tiesībām.

(24) Gadījumiem, kad pastāv aizdomas par terorismu un smagiem noziegumiem, būtu jāiekļauj jauna darbība, kas nolūkā sniegt plašāku informāciju izdevējai dalībvalstij ļauj apturēt un nopratināt personu, kura tiek turēta aizdomās par smaga nozieguma izdarīšanu vai par kuru ir pamats uzskatīt, ka tā izdarīs smagu noziegumu. Šai jaunajai darbībai nebūtu jāizvēršas par personas meklēšanu vai apcietināšanu. Taču tai būtu jāsniedz pietiekama informācija, lai lemtu par turpmāko rīcību. Ar jēdzienu "smagi noziegumi" būtu jāsaprot nodarījumi, kas minēti Padomes Pamatlēmumā 2002/584/TI.

(25) SIS būtu jāiekļauj jaunas kategorijas priekšmetiem ar augstu vērtību, piemēram, elektronikas un tehniskais aprīkojums, kuru var identificēt un meklēt ar unikālu numuru.

(26) Dalībvalstīm vajadzētu būt iespējai brīdinājumam pievienot norādi, t. s. karodziņu, ar ko norāda, ka saskaņā ar brīdinājumu veicamā darbība netiks veikta tās teritorijā. Ja brīdinājumus izdod apcietināšanai nodošanas nolūkā, nekas šajā lēmumā nebūtu jāinterpretē kā atkāpe no Pamatlēmuma 2002/584/TI vai liegums to piemērot. Lēmums brīdinājumam pievienot karodziņu būtu jāpamato vienīgi ar minētajā pamatlēmumā paredzētajiem atteikuma iemesliem.

(27) Ja brīdinājumam pievienots karodziņš un ja kļūst zināma tās personas atrašanās vieta, ko meklē, lai apcietinātu nolūkā to nodot, tad atrašanās vieta vienmēr būtu jāpaziņo izdevējai tiesu iestādei, kas var pieņemt lēmumu pārsūtīt Eiropas apcietināšanas orderi kompetentai tiesu iestādei saskaņā ar Pamatlēmumu 2002/584/TI.

[49] Padomes Pamatlēmums 2002/584/TI (2002. gada 13. jūnijs) par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm (OV L 190, 18.7.2002., 1. lpp.).

(28) Dalībvalstīm vajadzētu būt iespējai veikt brīdinājumu sasaisti SIS. Tam, ka dalībvalsts izveido saites starp diviem vai vairāk brīdinājumiem, nevajadzētu ietekmēt veicamo darbību, saglabāšanas periodu vai piekļuves tiesības brīdinājumiem.

(29) Brīdinājumi SIS nebūtu jāglabā ilgāk kā nepieciešams, lai īstenotu mērķus, kuriem tie izdoti. Lai samazinātu administratīvo slogu dažādām iestādēm, kas iesaistītas personas datu apstrādē dažādos nolūkos, ir lietderīgi par personām izdotu brīdinājumu saglabāšanas periodu saskaņot ar saglabāšanas periodu, kas paredzēts saistībā ar atgriešanu un nelikumīgu uzturēšanos. Turklāt dalībvalstis regulāri pagarina derīguma termiņu brīdinājumiem par personām, ja pieprasīto darbību nav bijis iespējams veikt sākotnēji noteiktajā termiņā. Līdz ar to maksimālais saglabāšanas periods brīdinājumiem par personām būtu pieci gadi. Parasti brīdinājumi par personām būtu automātiski jādzēš no SIS pēc pieciem gadiem, izņemot brīdinājumus par diskrētām, īpašām un izmeklēšanas pārbaudēm. Tie būtu jādzēš pēc viena gada. Brīdinājumi par priekšmetiem, kas ievadīti saistībā ar diskrētām pārbaudēm, izmeklēšanas pārbaudēm vai īpašām pārbaudēm, būtu automātiski jādzēš no SIS pēc viena gada, jo tie vienmēr ir saistīti ar personām. Brīdinājumi par priekšmetiem izņemšanai vai izmantošanai par pierādījumu kriminālprocesā būtu automātiski jādzēš no SIS pēc pieciem gadiem, jo pēc tik ilga laika posma izredzes tos atrast ir ļoti zemas un to ekonomiskā vērtība ir ievērojami samazinājusies. Brīdinājumi par izsniegtiem identifikācijas dokumentiem un oficiālu dokumentu veidlapām būtu jāglabā 10 gadus, jo dokumentu derīguma termiņš izdošanas brīdī ir 10 gadi. Lēmums saglabāt brīdinājumus par personām būtu jāpieņem, pamatojoties uz visaptverošu individuālu izvērtējumu. Dalībvalstīm būtu jāpārskata brīdinājumi par personām noteiktā termiņā un jāglabā statistika par to brīdinājumu skaitu, kuru saglabāšanas periods ir pagarināts.

(30) SIS brīdinājuma beigu termiņa pagarināšanai un ievadīšanai būtu jāpiemēro nepieciešamās proporcionalitātes prasība, izvērtējot, vai konkrētais gadījums ir atbilstīgs, piemērots un pietiekami svarīgs, lai ievadītu brīdinājumu SIS. Padomes Pamatlēmuma 2002/475/TI par terorisma apkarošanu[50] 1., 2., 3. un 4. pantā minētie nodarījumi ļoti nopietni apdraud sabiedrisko drošību, indivīdu dzīves neaizskaramību un sabiedrību kopumā, un šos nodarījumus ir ārkārtīgi grūti novērst, atklāt un izmeklēt zonā bez iekšējās robežkontroles, kurā potenciālie pārkāpēji brīvi pārvietojas. Ja personu vai priekšmetu meklē saistībā ar šiem pārkāpumiem, vienmēr ir nepieciešams izveidot atbilstošu brīdinājumu SIS par personām, kuras meklē krimināltiesvedības procesam, par personām vai objektiem diskrētai, izmeklēšanas un īpašai pārbaudei, kā arī par priekšmetiem izņemšanai, jo citi līdzekļi nebūtu tik efektīvi saistībā ar šo mērķi.

(31) Ir nepieciešams nodrošināt skaidrību par brīdinājumu dzēšanu. Brīdinājums būtu jāglabā tikai tik ilgi, cik vajadzīgs, lai sasniegtu mērķi, kādam tas ievadīts. Ņemot vērā dalībvalstu atšķirīgo praksi attiecībā uz tā laika noteikšanu, kad brīdinājums ir izpildījis savu mērķi, ir lietderīgi katrai brīdinājumu kategorijai noteikt sīki izstrādātus kritērijus, lai varētu noteikt, kad tas būtu jādzēš no SIS.

(32) SIS datu integritāte ir ārkārtīgi nozīmīga. Tāpēc būtu jāparedz attiecīgi aizsardzības pasākumi, lai apstrādātu SIS datus gan centrālajā, gan valsts līmenī, lai nodrošinātu datu drošību "no viena gala līdz otram". Iestādēm, kas iesaistītas datu apstrādē, būtu

[50] Padomes Pamatlēmums 2002/475/TI (2002. gada 13. jūnijs) par terorisma apkarošanu (OV L 164, 22.6.2002., 3. lpp.).

jāievēro šajā regulā noteiktās drošības prasības un jāpiemēro vienota starpgadījumu ziņošanas procedūra.

(33) Datus, kas apstrādāti SIS, piemērojot šo regulu, nevajadzētu nosūtīt vai darīt pieejamus trešām valstīm vai starptautiskām organizācijām. Tomēr it lietderīgi stiprināt sadarbību starp Eiropas Savienību un Interpolu, veicinot pases datu efektīvu apmaiņu. Ja personas datus no SIS nodod Interpolam, minētajiem personas datiem būtu jānodrošina atbilstīga līmeņa aizsardzība, ko garantē nolīgums, kurā noteikti stingri aizsardzības pasākumi un nosacījumi.

(34) Ir lietderīgi piešķirt piekļuvi SIS iestādēm, kas atbildīgas par transportlīdzekļu, laivu un gaisa kuģu reģistrāciju, lai tās varētu pārbaudīt, vai attiecīgo satiksmes līdzekli dalībvalstīs jau meklē, lai izņemtu vai pārbaudītu. Tieša piekļuve būtu jānodrošina iestādēm, kas ir valsts dienesti. Piekļuve būtu jāattiecina tikai uz brīdinājumiem par attiecīgajiem satiksmes līdzekļiem un to reģistrācijas dokumentiem vai numura zīmēm. Attiecīgi Eiropas Parlamenta un Padomes Regulas (EK) Nr. 1986/2006[51] noteikumi būtu jāiekļauj šajā regulā un minētā regula būtu jāatceļ.

(35) Attiecībā uz datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, un izpildītu kriminālsodus, tostarp, lai aizsargātu pret sabiedriskās drošības apdraudējumiem un novērstu tos, būtu jāpiemēro valsts tiesību akti, ar kuriem transponēta Direktīva (ES) 2016/680. Eiropas Parlamenta un Padomes Regulas (ES) Nr. 2016/679[52] un Direktīvas (ES) 2016/680 noteikumi būtu jāprecizē šajā regulā, ja nepieciešams.

(36) Gadījumos, kad Direktīva (ES) 2016/680 nav piemērojama, personas datu apstrādei, ko veic valsts iestādes saskaņā ar šo regulu, būtu jāpiemēro Regula (ES) Nr. 2016/679. Personas datu apstrādei, ko veic Savienības iestādes un struktūras, pildot savus pienākumus saskaņā ar šo regulu, būtu jāpiemēro Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001[53].

(37) Direktīvas (ES) 2016/680, Regulas (ES) Nr. 2016/679 un Regulas (EK) 45/2001 noteikumi nepieciešamos gadījumos būtu jākonkretizē šajā regulā. Personas datu apstrādei, ko veic Eiropols, piemēro Regulu (ES) Nr. 2016/794 par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropola Regula)[54].

(38) Noteikumi par datu aizsardzību, kas paredzēti 2002. gada 28. februāra Lēmumā 2002/187/TI[55], ar ko izveido *Eurojust*, lai pastiprinātu cīņu pret smagiem noziegumiem, attiecas uz SIS datu apstrādi, ko veicis *Eurojust*, tostarp Apvienotās uzraudzības iestādes, kura izveidota saskaņā ar minēto lēmumu, pilnvaras uzraudzīt

---

51 Eiropas Parlamenta un Padomes Regula (EK) Nr. 1986/2006 (2006. gada 20. decembris) par dalībvalstu dienestu, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izsniegšanu, piekļuvi otrās paaudzes Šengenas Informācijas sistēmai (SIS II) (OV L 381, 28.12.2006., 1. lpp.).

52 Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

53 Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).

54 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, 25.5.2016., 53. lpp.).

55 Padomes Lēmums 2002/187/TI (2002. gada 28. februāris), ar ko izveido *Eurojust*, lai pastiprinātu cīņu pret smagiem noziegumiem (OV L 63, 6.3.2002., 1. lpp.).

Eurojust darbības un noteikumi par atbildību sakarā ar personas datu nelikumīgu apstrādi, ko veicis *Eurojust*. Ja *Eurojust* veiktā meklēšanā atklājas, ka SIS ir dalībvalsts izdots brīdinājums, *Eurojust* nevar veikt vajadzīgos pasākumus. Tādēļ tam būtu jāinformē attiecīgā dalībvalsts, kas ļautu tai izskatīt konkrēto gadījumu.

(39) Attiecībā uz konfidencialitāti, ierēdņiem un citiem darbiniekiem, kuri ir nodarbināti un strādā saistībā ar SIS, būtu jāpiemēro attiecīgie Eiropas Savienības Civildienesta noteikumi un Savienības pārējo darbinieku nodarbināšanas kārtība.

(40) Gan dalībvalstīm, gan Aģentūrai būtu jāizstrādā drošības plāns, lai atvieglinātu saistību izpildi drošības jomā, un tām būtu jāsadarbojas, lai no kopīga skatu punkta risinātu drošības jautājumus.

(41) Neatkarīgām valsts uzraudzības iestādēm būtu jāpārrauga to personas datu apstrādes likumību, ko dalībvalstis veic saistībā ar šo regulu. Būtu jānosaka datu subjektu tiesības piekļūt datiem, labot un dzēst savus personas datus, kas glabājas SIS, un turpmākus tiesiskās aizsardzības līdzekļus valsts tiesās, kā arī spriedumu savstarpēju atzīšanu. Tādēļ ir lietderīgi no dalībvalstīm pieprasīt gada statistiku.

(42) Uzraudzības iestādēm būtu jānodrošina, ka vismaz reizi četros gados tiek veikta attiecīgās valsts N.SIS veikto datu apstrādes operāciju revīzija saskaņā ar starptautiskiem revīzijas standartiem. Revīziju būtu jāveic uzraudzības iestādēm, vai valstu uzraudzības iestādēm būtu tieši jāpasūta revīzija no neatkarīga datu aizsardzības revidenta. Valsts uzraudzības iestādei vai iestādēm būtu jāsaglabā kontrole pār neatkarīgo revidentu un atbildība par viņa darbu, tāpēc tām pašām būtu jāpasūta revīzija un jānosaka skaidri definēts revīzijas mērķis, tvērums un metodoloģija, kā arī jānodrošina vadlīnijas un uzraudzība attiecībā uz revīziju un tās galīgajiem rezultātiem.

(43) Regulā (ES) Nr. 2016/794 (Eiropola regula) ir paredzēts, ka Eiropols atbalsta un stiprina dalībvalstu kompetento iestāžu darbības un to savstarpējo sadarbību terorisma un smagu noziegumu novēršanā un apkarošanā un sniedz analītisku atbalstu un draudu novērtējumus. Eiropola piekļuves tiesību paplašināšanai attiecībā uz SIS brīdinājumiem par pazudušām personām būtu jāturpina uzlabot Eiropola spēju nodrošināt valsts tiesībaizsardzības iestādes ar visaptverošiem operatīviem un analītiskiem produktiem saistībā ar cilvēku tirdzniecību un bērnu seksuālu izmantošanu, tostarp tiešsaistē. Tas palīdzētu efektīvāk novērst šos noziedzīgos nodarījumus, uzlabotu potenciālo cietušo aizsardzību un vainīgo atklāšanu. Eiropola Eiropas Kibernoziedzības centrs arī varētu gūt labumu no jaunas Eiropola piekļuves SIS brīdinājumiem par pazudušām personām, tostarp ceļojošu dzimumnoziedznieku un bērnu seksuālas izmantošanas tiešsaistē gadījumos, kad noziedznieki bieži apgalvo, ka viņi var piekļūt vai var iegūt piekļuvi bērniem, kas, iespējams, reģistrēti kā pazuduši. Turklāt, ņemot vērā, ka Eiropola Eiropas Migrantu kontrabandas apkarošanas centram ir svarīga stratēģiska nozīme cīņā pret neatbilstīgās migrācijas veicināšanu, tam būtu jāsaņem piekļuve brīdinājumiem par personām, kurām atteikta ieceļošana vai uzturēšanās dalībvalsts teritorijā vai nu sodāmības dēļ, vai tādēļ, ka nav ievēroti vīzas un uzturēšanās nosacījumi.

(44) Lai novērstu trūkumus informācijas apmaiņā par terorismu, jo īpaši par ārvalstu kaujiniekiem teroristiem – kuru pārvietošanās uzraudzība ir īpaši svarīga –, dalībvalstīm, paralēli ievadot brīdinājumu SIS, būtu jāsniedz Eiropolam informācija par darbībām, kas saistītas ar terorismu, kā arī par trāpījumiem un saistīto informāciju. Tas ļautu Eiropola Eiropas Terorisma apkarošanas centram pārbaudīt, vai pastāv jebkāda papildu kontekstuāla informācija, kas pieejama Eiropola datubāzēs, un

nodrošināt augstas kvalitātes analīzi, kura palīdzētu izjaukt terorisma tīklus un, ja iespējams, novērst uzbrukumus.

(45) Ir arī nepieciešams paredzēt skaidrus noteikumus Eiropolam par SIS datu apstrādi un lejupielādi, lai nodrošinātu pēc iespējas visaptverošu SIS izmantošanu ar nosacījumu, ka tiek ievēroti datu aizsardzības standarti, kas paredzēti šajā regulā un Regulā (ES) Nr. 2016/794. Ja Eiropola veiktā meklēšanā atklājas, ka SIS ir dalībvalsts izdots brīdinājums, Eiropols nevar veikt vajadzīgos pasākumus. Tādēļ tam būtu jāinformē attiecīgā dalībvalsts, kas ļautu tai izskatīt konkrēto gadījumu.

(46) Eiropas Parlamenta un Padomes Regulā (ES) Nr. 2016/1624[56] noteikts, ka šīs regulas nolūkā uzņēmēja dalībvalsts atļauj Eiropas robežu un krasta apsardzes vienību dalībniekiem vai tāda personāla vienību dalībniekiem, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, kurus norīko Eiropas Robežu un krasta apsardzes aģentūra, ieskatīties Eiropas datubāzēs, ja šāda ieskatīšanās ir vajadzīga, lai sasniegtu operatīvos mērķus, kas noteikti operatīvajā plānā par robežpārbaudēm, robežu uzraudzību un atgriešanu. Citas attiecīgas Savienības aģentūras, jo īpaši Eiropas Patvēruma atbalsta birojs un Eiropols, arī var norīkot ekspertus migrācijas pārvaldības atbalsta vienību sastāvā, un šie eksperti nav šo aģentūru personāls. Eiropas robežu un krasta apsardzes vienību, tāda personāla vienību, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, un migrācijas pārvaldības atbalsta vienības izvietošanas mērķis ir sniegt pastiprinātu tehnisko un operatīvo palīdzību dalībvalstīm, kas izteikušas pieprasījumu, jo īpaši tām dalībvalstīm, kas saskaras ar nesamērīgām migrācijas problēmām. Pildot tām uzticētos uzdevumus, Eiropas Robežu un krasta apsardzes vienībām, tāda personāla vienībām, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, un migrācijas pārvaldības atbalsta vienībai ir nepieciešama piekļuve SIS, izmantojot Eiropas robežu un krasta apsardzes aģentūras tehnisko saskarni, kas savienota ar centrālo SIS. Ja meklēšanā, ko SIS veic vienības vai personāla vienības, atklājas dalībvalsts izdots brīdinājums, vienības vai personāla vienības loceklis nevar veikt nepieciešamo darbību, izņemot, ja uzņēmēja dalībvalsts atļauj to darīt. Tādēļ tam būtu jāinformē attiecīgā dalībvalsts, kas ļautu tai izskatīt konkrēto gadījumu.

(47) Saskaņā ar Komisijas priekšlikumu Eiropas Parlamenta un Padomes Regulai, ar ko izveido Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*)[57], Eiropas robežu un krasta apsardzes aģentūras *ETIAS* centrālā vienība, izmantojot *ETIAS*, veiks pārbaudes SIS, lai varētu veikt ceļošanas atļauju pieteikumu izvērtējumu, kas cita starpā prasa pārliecināties, vai uz trešās valsts valstspiederīgo, kurš iesniedz ceļošanas atļaujas pieteikumu, neattiecas SIS brīdinājums. Tālab Eiropas robežu un krasta apsardzes aģentūras *ETIAS* centrālajai vienībai, ciktāl tas nepieciešams, lai veiktu tās uzdevumu, arī vajadzētu būt piekļuvei SIS, proti, visu kategoriju brīdinājumiem par personām un brīdinājumiem par oficiālu dokumentu veidlapām un izdotiem personu apliecinošiem dokumentiem.

(48) Ņemot vērā dažu SIS aspektu tehnisko raksturu, detalizācijas pakāpi un nepieciešamību veikt regulāru atjaunināšanu, tos nevar pilnīgi aptvert šajā regulā. Tie ietver, piemēram, tehniskos noteikumus par datu ievadi, atjaunināšanu, dzēšanu un meklēšanu, datu kvalitāti un datu meklēšanas noteikumus, kas saistīti ar

---

[56] 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.).

[57] COM(2016) 731, *final*.

biometriskajiem identifikatoriem, noteikumus attiecībā uz brīdinājumu savietojamību un prioritāti, karodziņu pievienošanu, saites starp brīdinājumiem, jaunu priekšmetu kategoriju noteikšanu tehniskā un elektronikas aprīkojuma kategorijas ietvaros, brīdinājumu izbeigšanās termiņu noteikšanu maksimālo termiņu ietvaros un papildinformācijas apmaiņu. Īstenošanas pilnvaras attiecībā uz šiem aspektiem tāpēc būtu jāpiešķir Komisijai. Tehniskajos noteikumos brīdinājumu meklēšanai būtu jāņem vērā valstu sistēmu sekmīga darbība.

(49) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir īstenošanas pilnvaras Komisijai. Minētās pilnvaras būtu jāīsteno saskaņā ar Regulu (ES) Nr. 182/2011[58]. Īstenošanas pasākumu pieņemšanas procedūrai vajadzētu būt tādai pašai gan šajā regulā, gan Regulā (ES) Nr. 2018/xxx (robežpārbaudes).

(50) Pārredzamības nodrošināšanai Aģentūrai ik pēc diviem gadiem būtu jāizstrādā ziņojums par centrālās SIS un komunikācijas infrastruktūras tehnisko darbību, tostarp to drošību, un par papildinformācijas apmaiņu. Komisijai ik pēc četriem gadiem būtu jāveic vispārējs novērtējums.

(51) Ņemot vērā to, ka šīs regulas mērķus, proti, izveidot un reglamentēt vienotu informācijas sistēmu un apmaiņu ar attiecīgu papildinformāciju, to būtības dēļ nevar pietiekami labi sasniegt atsevišķās dalībvalstīs un tos var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību (LES) 5. pantā noteikto proporcionalitātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas vajadzīgi minēto mērķu sasniegšanai.

(52) Šajā regulā tiek ievērotas pamattiesības un principi, kas īpaši atzīti Eiropas Savienības Pamattiesību hartā. Jo īpaši šīs regulas mērķis, vienlaikus pilnībā ievērojot personas datu aizsardzību, ir nodrošināt drošu vidi visām personām, kas dzīvo Eiropas Savienības teritorijā, un īpaši aizsargāt bērnus, kuri var kļūt par cilvēku tirdzniecības upuriem vai ciest no vecāku veiktas nolaupīšanas.

(53) Saskaņā ar 1. un 2. pantu 22. protokolā par Dānijas nostāju, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, Dānija nepiedalās šīs regulas pieņemšanā un Dānijai šī regula nav saistoša un nav jāpiemēro. Tā kā šī regula pilnveido Šengenas *acquis*, Dānija saskaņā ar minētā protokola 4. pantu sešos mēnešos pēc tam, kad Padome ir pieņēmusi lēmumu par šo regulu, izlemj, vai tā šo regulu ieviesīs savos tiesību aktos.

(54) Apvienotā Karaliste piedalās šajā regulā saskaņā ar 5. pantu Protokolā par Šengenas *acquis*, kas iekļauts Eiropas Savienības sistēmā, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, un saskaņā ar 8. panta 2. punktu Padomes 2000. gada 29. maija Lēmumā 2000/365/EK par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā[59].

(55) Īrija piedalās šajā regulā saskaņā ar 5. pantu Protokolā par Šengenas *acquis*, kas iekļauts Eiropas Savienības sistēmā un kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, un saskaņā ar 6. panta 2. punktu

[58] Eiropas Parlamenta un Padomes Regula (ES) Nr.182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).

[59] OV L 131, 1.6.2000., 43. lpp.

Padomes 2002. gada 28. februāra Lēmumā 2002/192/EK par Īrijas lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā[60].

(56) Attiecībā uz Islandi un Norvēģiju – saskaņā ar Nolīgumu, kas noslēgts starp Eiropas Savienības Padomi un Islandes Republiku un Norvēģijas Karalisti par šo valstu asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā[61], šī regula ir to Šengenas *acquis* noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta 1. panta G punktā Padomes Lēmumā 1999/437/EK[62] par dažiem pasākumiem minētā nolīguma piemērošanai.

(57) Attiecībā uz Šveici – saskaņā ar Nolīgumu, kas parakstīts starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā, šī regula ir to Šengenas *acquis* noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta Lēmuma 1999/437/EK 1. panta G. punktā, to lasot saistībā ar 4. panta 1. punktu Lēmumos 2004/849/EK[63] un 2004/860/EK[64].

(58) Attiecībā uz Lihtenšteinu – saskaņā ar Protokolu starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju un Lihtenšteinas Firstisti par Lihtenšteinas Firstistes pievienošanos Nolīgumam starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā[65], šī regula ir to Šengenas *acquis* noteikumu pilnveidošana, kuri attiecas uz jomu, kas minēta Lēmuma 1999/437/EK 1. panta G punktā, to lasot saistībā ar Padomes Lēmuma 2011/349/ES[66] 3. pantu un Padomes Lēmuma 2011/350/ES 3. pantu[67].

(59) Attiecībā uz Bulgāriju un Rumāniju šī regula ir akts, kas pilnveido Šengenas *acquis* vai ir kā citādi saistīts ar to 2005. gada Pievienošanās akta 4. panta 2. punkta nozīmē, un būtu jālasa saistībā ar Padomes Lēmumu 2010/365/ES par Šengenas *acquis*

---

60 OV L 64, 7.3.2002., 20. lpp.

61 OV L 176, 10.7.1999., 36. lpp.

62 OV L 176, 10.7.1999., 31. lpp.

63 Padomes Lēmums 2004/849/EK (2004. gada 25. oktobris) par Nolīguma parakstīšanu Eiropas Savienības vārdā starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas acquis īstenošanā, piemērošanā un pilnveidošanā un par dažu tā noteikumu provizorisku piemērošanu (OV L 368, 15.12.2004., 26. lpp.).

64 Padomes Lēmums 2004/860/EK (2004. gada 25. oktobris) par Nolīguma parakstīšanu Eiropas Kopienas vārdā starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas acquis īstenošanā, piemērošanā un pilnveidošanā un par dažu tā noteikumu provizorisku piemērošanu (OV L 370, 17.12.2004., 78. lpp.).

65 OV L 160, 18.6.2011., 21. lpp.

66 Padomes Lēmums 2011/349/ES (2011. gada 7. marts) par to, lai Eiropas Savienības vārdā noslēgtu Protokolu starp Eiropas Savienību, Eiropas Kopienu, Šveices Konfederāciju un Lihtenšteinas Firstisti par Lihtenšteinas Firstistes pievienošanos Nolīgumam starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā, jo īpaši saistībā ar tiesu iestāžu sadarbību krimināllietās un policijas sadarbību (OV L 160, 18.6.2011., 1. lpp).

67 Padomes Lēmums 2011/350/ES (2011. gada 7. marts) par to, lai Eiropas Savienības vārdā noslēgtu Protokolu starp Eiropas Savienību, Eiropas Kopienu, Šveices Konfederāciju un Lihtenšteinas Firstisti par Lihtenšteinas Firstistes pievienošanos Nolīgumam starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā saistībā ar kontroles atcelšanu pie iekšējām robežām un personu pārvietošanos (OV L 160, 18.6.2011., 19. lpp.).

noteikumu īstenošanu saistībā ar Šengenas Informācijas sistēmu Bulgārijas Republikā un Rumānijā[68].

(60) Attiecībā uz Kipru un Horvātiju šī regula ir akts, kas pilnveido Šengenas *acquis* vai ir kā citādi saistīts ar to, kā noteikts attiecīgi 2003. gada Pievienošanās akta 3. panta 2. punktā un 2011. gada Pievienošanās akta 4. panta 2. punktā.

(61) Īrijai šī regula būtu jāpiemēro no dienas, ko nosaka saskaņā ar procedūrām, kuras izklāstītas attiecīgos instrumentos par Šengenas *acquis* piemērošanu minētajai dalībvalstij.

(62) Šajā regulā paredzētās SIS valstu sistēmu modernizācijas un jauno funkciju ieviešanas aprēķinātās izmaksas ir zemākas nekā Eiropas Parlamenta un Padomes Regulā (ES) Nr. 515/2014[69] paredzētās viedrobežu budžeta pozīcijas pārpalikums. Tādēļ ar šo regulu būtu jāpārdala summa, kas patlaban piešķirta IT sistēmu izstrādei migrācijas plūsmu pārvaldībai pie ārējām robežām saskaņā ar 5. panta 5. punkta b) apakšpunktu Regulā (ES) Nr. 515/2014.

(63) Padomes Lēmums 2007/533/TI un Komisijas Lēmums 2010/261/ES[70] tāpēc būtu jāatceļ.

(64) Ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju saskaņā ar Regulas (EK) Nr. 45/2001 28. panta 2. punktu, un tas sniedza atzinumu ...

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants
SIS vispārējais mērķis

SIS mērķis, izmantojot šīs sistēmas izplatīto informāciju, ir nodrošināt augstu drošības līmeni Savienības brīvības, drošības un tiesiskuma telpā, tostarp nodrošināt sabiedriskās drošības un sabiedriskās kārtības uzturēšanu un saglabāšanu dalībvalstu teritorijās, un piemērot Līguma par Eiropas Savienības darbību trešās daļas V sadaļas 4. un 5. nodaļas noteikumus par personu pārvietošanos to teritorijās.

2. pants
Piemērošanas joma

1. Ar šo regulu paredz nosacījumus un kārtību tādu brīdinājumu ievadīšanai un apstrādei SIS, kas izdoti attiecībā uz personām un priekšmetiem, un

---

68 OV L 166, 1.7.2010., 17. lpp.

69 Eiropas Parlamenta un Padomes Regula (ES) Nr. 515/2014 (2014. gada 16. aprīlis), ar ko kā daļu no Iekšējās drošības fonda izveido finansiāla atbalsta instrumentu ārējām robežām un vīzām (OV L 150, 20.5.2014., 143. lpp.).

70 Komisijas Lēmums 2010/261/ES (2010. gada 4. maijs) par drošības plānu Centrālajai SIS II un sakaru infrastruktūrai (OV L 112, 5.5.2010., 31. lpp.)

papildinformācijas un papildu datu apmaiņai ar mērķi policijas un tiesu iestādēm sadarboties krimināllietās.

2. Tāpat ar šo regulu paredz noteikumus par SIS tehnisko uzbūvi, dalībvalstu un Eiropas Aģentūras lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā pienākumiem, vispārēju datu apstrādi, attiecīgo personu tiesībām un atbildību.

3. pants
Definīcijas

1. Šajā regulā piemēro šādas definīcijas:

(a) "brīdinājums" ir datu kopums, tostarp biometriskie identifikatori, kā minēts 22. pantā un 40. pantā, kas ievadīti SIS un kompetentajām iestādēm ļauj identificēt personu vai priekšmetu, lai konkrēti rīkotos;

(b) "papildinformācija" ir informācija, kas nav SIS saglabāto brīdinājumu sastāvdaļa, bet ir saistīta ar SIS brīdinājumiem, un ar ko apmainās:

(1) lai dalībvalstis varētu konsultēties vai informēt cita citu, ievadot brīdinājumu,

(2) pēc trāpījuma, lai varētu attiecīgi rīkoties,

(3) ja nav iespējams veikt prasīto darbību,

(4) apsverot SIS datu kvalitāti,

(5) apsverot brīdinājumu savietojamību un prioritāti;

(6) saistībā ar piekļuves tiesībām;

(c) "papildu dati" ir dati, ko saglabā SIS un kas ir saistīti ar SIS brīdinājumiem un nekavējoties pieejami kompetentajām iestādēm, ja SIS meklēšanas rezultātā atrod personu, par kuru dati ir ievadīti SIS;

(d) "personas dati" ir jebkura informācija par identificētu vai identificējamu fizisko personu ("datu subjektu");

(e) "identificējama fiziska persona" ir persona, kuru tieši vai netieši var identificēt, jo īpaši, izmantojot tādus identifikatorus kā, piemēram, vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datus, tiešsaistes identifikatoru vai vienu vai vairākus minētajai personai raksturīgus fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktorus;

(f) "personas datu apstrāde" ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;

(g) "trāpījums" SIS nozīmē:

(1) lietotājs veic meklēšanu;

(2) meklēšanā tiek konstatēts brīdinājums, ko SIS ir ievadījusi cita dalībvalsts,

(3) dati, kas attiecas uz SIS atrodamo brīdinājumu, atbilst meklētajiem datiem, un

(4) tiek pieprasīts veikt turpmākas darbības.

(h) "karodziņš" ir brīdinājuma derīguma apturēšana valsts līmenī, ko var pievienot brīdinājumiem par apcietināšanu, brīdinājumiem par pazudušām personām un brīdinājumiem par diskrētu, izmeklēšanas un īpašu pārbaudi, ja dalībvalsts uzskata, ka brīdinājuma izpilde nav saderīga ar tās tiesību aktiem, starptautiskajām saistībām vai būtiskām valsts interesēm. Ja brīdinājums ir apzīmēts ar karodziņu, pieprasīto darbību, kas jāveic, pamatojoties uz brīdinājumu, šīs dalībvalsts teritorijā neveic.

(i) "izdevēja dalībvalsts" ir dalībvalsts, kas ir ievadījusi brīdinājumu SIS;

(j) "izpildītāja dalībvalsts" ir dalībvalsts, kas pēc trāpījuma veic vai ir veikusi nepieciešamās darbības;

(k) "galalietotāji" ir kompetentās iestādes, kas tieši meklē CS-SIS, N.SIS vai to tehniskajā eksemplārā;

(l) "daktiloskopiskie dati" ir dati par pirkstu nospiedumiem un plaukstu nospiedumiem, kuri, ņemot vērā to unikālās īpašības un tajos ietvertās atsauces vērtības, dara iespējamu precīzu un pārliecinošu salīdzināšanu attiecībā uz personas identitāti;

(m) "smagi noziegumi" ir nodarījumi, kas uzskaitīti 2. panta 1. un 2. punktā 2002. gada 13. jūnija Pamatlēmumā 2002/584/TI[71];

(n) "teroristu nodarījumi" ir valsts tiesību aktos noteiktie nodarījumi, kas minēti Pamatlēmuma 2002/475/TI 1. – 4. pantā[72].

4. pants
SIS tehniskā arhitektūra un darbības veidi

1. SIS veido:

(a) centrālā sistēma ("centrālā SIS"), ko veido:

– tehniskā nodrošinājuma vienība ("CS-SIS"), kurā ietverta datubāze – "SIS datubāze",

– vienota valsts saskarne (NI-SIS);

(b) valsts sistēma katrā dalībvalstī ("N.SIS"), ko veido valsts datu sistēmas, kuras ir saistītas ar centrālo SIS. N.SIS ietver datu datni ("valsts eksemplārs"), kas ir pilnīga vai daļēja SIS datubāzes kopija, kā arī rezerves N.SIS; N.SIS un rezerves N.SIS var izmantot vienlaicīgi, lai nodrošinātu nepārtrauktu pieejamību tiešajiem galalietotājiem;

(c) CS-SIS un NI-SIS savstarpējās komunikācijas infrastruktūra ("komunikācijas infrastruktūra"), kas nodrošina SIS datiem atvēlētu kodētu virtuālu tīklu un *SIRENE* biroju savstarpēju datu apmaiņu, kā minēts 7. panta 2. punktā.

[71] Padomes Pamatlēmums 2002/584/TI (2002. gada 13. jūnijs) par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm (OV L 190, 18.7.2002., 1. lpp.).

[72] Padomes Pamatlēmums 2002/475/TI (2002. gada 13. jūnijs) par terorisma apkarošanu (OV L 164, 22.6.2002., 3. lpp.).

2. SIS datus ievada, atjaunina, dzēš un tajos veic meklēšanu, izmantojot dažādās N.SIS. Daļēju vai pilnu valsts eksemplāru dara pieejamu, lai veiktu automatizētu meklēšanu katras dalībvalsts teritorijā, kas lieto tādu eksemplāru. Daļējs valsts eksemplārs ietver vismaz 20. panta 2. punktā uzskaitītos datus attiecībā uz priekšmetiem, un datus, kas minēti 20. panta 3. punkta a) - v) apakšpunktā attiecībā uz brīdinājumiem par personām. Veikt meklēšanu citu dalībvalstu N. SIS datu datnēs nav iespējams.

3. CS-SIS veic tehniskās uzraudzības un administrācijas uzdevumus, un tai ir rezerves CS-SIS, kas spēj nodrošināt visas galvenās CS-SIS funkcijas šīs sistēmas avārijas gadījumā. CS-SIS un rezerves CS-SIS atrodas divos tehniskajos centros Eiropas Aģentūrā lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā, kura izveidota ar Regulu (ES) Nr. 1077/2011[73] ("Aģentūra"). CS-SIS vai rezerves CS-SIS var ietvert SIS datubāzes papildu kopiju, un aktīvās operācijās tās var izmantot vienlaicīgi ar nosacījumu, ka katra no tām spēj apstrādāt visas transakcijas saistībā ar SIS brīdinājumiem.

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

a) valsts eksemplāru tiešsaistes atjaunināšanu;

b) valsts eksemplāru un SIS datu bāzes sinhronizāciju un saskanību;

c) kārtību valsts eksemplāru inicializēšanai un rekonstrukcijai;

d) nepārtrauktu pieejamību.

5. pants
Izmaksas

1. Centrālās SIS un komunikācijas infrastruktūras darbības, uzturēšanas un turpmākas izstrādes 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 izveides, darbības, uzturēšanas un turpmākas izstrādes izmaksas sedz attiecīgā dalībvalsts.

II NODAĻA

DALĪBVALSTU ATBILDĪBA

6. pants
Valstu sistēmas

Katra dalībvalsts ir atbildīga par savas N. SIS izveidi, darbību, uzturēšanu un turpmāku izstrādi, kā arī par savas N. SIS sasaistīšanu ar NI-SIS.

[73] Izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1077/2011 (2011. gada 25. oktobris), ar ko izveido Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (OV L 286, 1.11.2011., 1. lpp.).

Katra dalībvalsts ir atbildīga par N.SIS nepārtrauktas darbības nodrošināšanu, tās sasaisti ar NI-SIS un SIS datu nepārtrauktu pieejamību galalietotājiem.

7. pants
N.SIS birojs un SIRENE birojs

1. Katra dalībvalsts norīko iestādi ("N.SIS birojs"), kam ir galvenā atbildība par attiecīgo N.SIS.

   Minētā iestāde ir atbildīga par N.SIS netraucētu darbību un drošību, nodrošina kompetento iestāžu piekļuvi SIS un veic pasākumus, kas vajadzīgi, lai nodrošinātu atbilstību šai regulai. Tā ir atbildīga par to, lai nodrošinātu, ka visas SIS funkcijas ir pienācīgi pieejamas galalietotājiem.

   Katra dalībvalsts nosūta brīdinājumus ar N.SIS biroja starpniecību.

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

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

3. Dalībvalstis informē Aģentūru par attiecīgo valsts N.SIS biroju un *SIRENE* biroju. Aģentūra publicē šo biroju sarakstu kopā ar 53. panta 8. punktā minēto sarakstu.

8. pants
Papildinformācijas apmaiņa

1. Papildinformācijas apmaiņu veic saskaņā ar *SIRENE* rokasgrāmatu un izmantojot komunikācijas infrastruktūru. Dalībvalstis nodrošina nepieciešamos tehniskos un personāla resursus, lai nodrošinātu papildinformācijas nepārtrauktu pieejamību un apmaiņu ar to. Gadījumā, ja komunikācijas infrastruktūra nav pieejama, dalībvalstis var papildinformācijas apmaiņai izmantot citus atbilstīgi nodrošinātus tehniskos līdzekļus.

2. Papildinformāciju izmanto vienīgi nolūkā, kādā tā ir nosūtīta saskaņā ar 61. pantu, izņemot, ja no izdevējas dalībvalsts ir saņemta iepriekšēja piekrišana.

3. *SIRENE* birojs veic savus uzdevumus ātri un efektīvi, jo īpaši, atbildot uz lūgumu pēc iespējas drīz, bet ne vēlāk kā 12 stundu laikā pēc lūguma saņemšanas.

4. Sīki izstrādātus papildinformācijas apmaiņas noteikumus pieņem kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru kā "SIRENE rokasgrāmatu".

9. pants
Tehniskā un funkcionālā atbilstība

1. Lai nodrošinātu datu ātru un efektīvu pārsūtīšanu, katra dalībvalsts, izveidojot savu N.SIS, ievēro kopīgos standartus, protokolus un tehniskās procedūras, kas izveidoti, lai nodrošinātu tās N.SIS savietojamību ar CS-SIS. Šos kopīgos standartus, protokolus un tehniskās procedūras pieņem kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

2. Dalībvalstis ar CS-SIS sniegtu pakalpojumu palīdzību nodrošina, ka dati, ko glabā valsts eksemplārā, veicot 4. panta 4. punktā minēto automātisko atjaunināšanu, ir identiski un saskaņoti ar SIS datubāzi un ka meklēšana attiecīgās valsts eksemplārā sniedz līdzvērtīgu rezultātu SIS datubāzē veiktai meklēšanai. Galalietotāji saņem datus, kas ir vajadzīgi, lai veiktu tiem uzticētos uzdevumus, jo īpaši visus datus, kas vajadzīgi, lai identificētu datu subjektu un veiktu prasītās darbības.

10. pants
Drošība – dalībvalstis

1. Katra dalībvalsts attiecībā uz N.SIS pieņem vajadzīgos pasākumus, tostarp drošības plānu, darbības nepārtrauktības plānu un negadījuma seku novēršanas plānu, lai:

(a) fiziski aizsargātu datus, tostarp izstrādājot ārkārtas rīcības plānus kritiskās infrastruktūras aizsardzībai;

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

(c) novērstu nesankcionētu datu nolasīšanu, kopēšanu, grozīšanu vai datu nesēju izņemšanu (datu nesēju kontrole);

(d) novērstu datu nesankcionētu ievadīšanu, kā arī liegtu saglabāto personas datu nesankcionētu apskati, grozīšanu vai dzēšanu (glabāšanas kontrole);

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

(f) nodrošinātu, ka personām, kas ir pilnvarotas izmantot datu apstrādes automatizētu sistēmu, ir piekļuve tikai tiem datiem, uz kuriem attiecas viņu piekļuves tiesības, izmantojot individuālas un unikālas lietotāju identitātes un konfidenciālus pieejas veidus (datu piekļuves kontrole);

(g) nodrošinātu, ka visas iestādes, kurām ir piekļuves tiesības SIS vai datu apstrādes iekārtām, izstrādā profilus, raksturojot to personu funkcijas un pienākumus, kuras ir pilnvarotas piekļūt, ievadīt, atjaunot, dzēst un meklēt datus, un pēc 66. pantā minēto valstu uzraudzības iestāžu lūguma šos profilus nekavējoties dara tām pieejamus (personālie profili);

(h) nodrošinātu, ka ir iespējams pārbaudīt un noteikt struktūras, kurām personas dati var būt nosūtīti, izmantojot datu komunikācijas iekārtas (komunikācijas kontrole);

(i) nodrošinātu, ka vēlāk iespējams pārbaudīt un noteikt, kādi personas dati ir ievadīti automatizētas datu apstrādes sistēmās, kurā brīdī un kura persona tos ir ievadījusi, un kādā nolūkā (ievades kontrole);

(j) novērstu nesankcionētu personas datu nolasīšanu, kopēšanu, grozīšanu vai dzēšanu personas datu nosūtīšanas laikā vai datu nesēja transportēšanas laikā, jo īpaši izmantojot atbilstošas šifrēšanas metodes (transportēšanas kontrole);

(k) uzraudzītu šajā punktā minēto aizsardzības pasākumu efektivitāti un veiktu vajadzīgos organizatoriskos pasākumus saistībā ar iekšējo uzraudzību (paškontrole).

2. Dalībvalstis pieņem 1. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz drošību saistībā ar papildinformācijas apstrādi un apmaiņu ar to, tostarp nodrošinot *SIRENE* biroja telpu drošību.

3. Dalībvalstis pieņem 1. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz drošību saistībā ar SIS datu apstrādi, ko veic 43. pantā minētās iestādes.

11. pants
Konfidencialitāte – dalībvalstis

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 datiem un papildinformāciju. Šis pienākums ir spēkā arī pēc tam, kad šīs personas vairs neieņem attiecīgo amatu vai netiek nodarbinātas vai kad šo struktūru darbība ir izbeigta.

12. pants
Ierakstu glabāšana valstīs

1. Dalībvalstis nodrošina, ka katra piekļuve personas datiem un visas personas datu apmaiņas CS-SIS ietvaros tiek ierakstītas N.SIS, lai varētu pārbaudīt, vai meklēšana ir likumīga, lai uzraudzītu datu apstrādes likumību, pašuzraudzības nolūkos, un lai nodrošinātu N.SIS pareizu darbību, datu integritāti un drošību.

2. Ieraksti konkrēti parāda brīdinājuma vēsturi, datu apstrādes darbības datumu un laiku, meklēšanā izmantotos datus, atsauci uz pārraidītajiem datiem un gan kompetentās iestādes nosaukumu, gan par datu apstrādi atbildīgās personas vārdu.

3. Ja meklēšana veikta ar daktiloskopiskajiem datiem vai sejas attēlu saskaņā ar 40., 41. un 42. pantu, ieraksti konkrēti parāda meklēšanā izmantoto datu veidu, atsauci uz pārraidīto datu veidu un gan kompetentās iestādes nosaukumu, gan par datu apstrādi atbildīgās personas vārdu.

4. Ierakstus lieto vienīgi 1. punktā minētajā nolūkā un dzēš ne ātrāk kā pēc gada un ne vēlāk kā pēc trim gadiem no to izveides dienas.

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 pareizu darbību, datu integritāti un drošību, atbilstīgi to kompetencei un pēc to lūguma nodrošina piekļuvi šiem ierakstiem, lai tās varētu pildīt savus pienākumus.

7. Ja dalībvalstis veic transportlīdzekļu numuru zīmju automatizētu skenēšanas meklēšanu, izmantojot automatizētas numura zīmes atpazīšanas sistēmas, dalībvalstis glabā ierakstus par meklēšanu saskaņā ar valsts tiesību aktiem. Šo ierakstu saturu nosaka īstenošanas pasākumos saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru. Ja ir konstatēta atbilsme ar datiem, kas tiek glabāti SIS vai valsts eksemplārā, vai SIS datu tehniskajā kopijā, veic pilnu meklēšanu SIS, lai pārliecinātos, ka atbilsme patiešām eksistē. Šādai pilnai meklēšanai piemēro šā panta 1. līdz 6. punktu.

13. pants
Pašuzraudzība

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

14. pants
Personāla apmācība

Pirms tiek piešķirta atļauja apstrādāt SIS uzglabātos datus un periodiski pēc tam, kad piekļuve SIS datiem ir piešķirta, to iestāžu darbiniekus, kam ir tiesības piekļūt SIS, pienācīgi apmāca par datu drošību, datu aizsardzības noteikumiem un datu apstrādes procedūrām, kas izklāstītas *SIRENE* rokasgrāmatā. Darbiniekus informē par visiem attiecīgiem noziedzīgiem nodarījumiem un sodiem.

III NODAĻA

AĢENTŪRAS ATBILDĪBA

15. pants
Darbības pārvaldība

1. Par centrālās SIS darbības pārvaldību atbild Aģentūra. Aģentūra sadarbībā ar dalībvalstīm nodrošina to, ka centrālās SIS vajadzībām vienmēr tiek izmantota vislabākā pieejamā tehnoloģija, izmantojot izmaksu un ieguvumu analīzi.
2. Aģentūra ir atbildīga arī par šādiem uzdevumiem, kas saistīti ar komunikācijas infrastruktūru:
   (a) uzraudzība;
   (b) drošība;
   (c) dalībvalstu un nodrošinātāja attiecību koordinēšana.
3. Komisija ir atbildīga par visiem pārējiem uzdevumiem, kas saistīti ar komunikācijas infrastruktūru, jo īpaši:
   (a) uzdevumiem saistībā ar budžeta izpildi;
   (b) iegādi un atjaunināšanu;
   (c) jautājumiem, kas saistīti ar līgumiem.
4. Aģentūra ir atbildīga par šādiem uzdevumiem, kas saistīti ar *SIRENE* birojiem un komunikāciju starp *SIRENE* birojiem:
   (a) koordinēt un vadīt testēšanu;
   (b) uzturēt un atjaunināt tehniskās specifikācijas papildinformācijas apmaiņai starp *SIRENE* birojiem un komunikācijas infrastruktūru un pārvaldīt tehnisko izmaiņu ietekmi, ja tā skar gan SIS, gan papildinformācijas apmaiņu starp *SIRENE* birojiem.

5. Aģentūra izstrādā un uztur mehānismu un procedūras, lai veiktu CS-SIS datu kvalitātes pārbaudes, un regulāri iesniedz ziņojumus dalībvalstīm. Aģentūra regulāri iesniedz Komisijai ziņojumu par problēmām un attiecīgajām dalībvalstīm. Šo mehānismu, procedūras un datu kvalitātes atbilstības interpretāciju paredz kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

6. Centrālās SIS darbības pārvaldība ir visi uzdevumi, kas vajadzīgi, lai nodrošinātu centrālās SIS darbību 24 stundas diennaktī 7 dienas nedēļā, jo īpaši uzturēšanas darbi un tehniski pielāgojumi, kas vajadzīgi sistēmas nevainojamai darbībai. Šie uzdevumi ietver arī testēšanas pasākumus, lai nodrošinātu, ka centrālā SIS un valstu sistēmas darbojas saskaņā ar tehniskajām un funkcionālajām prasībām saskaņā ar šīs regulas 9. pantu.

16. pants
Drošība

1. Aģentūra attiecībā uz centrālo SIS un komunikācijas infrastruktūru pieņem vajadzīgos pasākumus, tostarp drošības plānu, darbības nepārtrauktības plānu un negadījuma seku novēršanas plānu, lai:

   (a) fiziski aizsargātu datus, tostarp izstrādājot ārkārtas rīcības plānus kritiskās infrastruktūras aizsardzībai;

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

   (c) novērstu nesankcionētu datu nolasīšanu, kopēšanu, grozīšanu vai datu nesēju izņemšanu (datu nesēju kontrole);

   (d) novērstu datu nesankcionētu ievadīšanu, kā arī liegtu saglabāto personas datu nesankcionētu apskati, grozīšanu vai dzēšanu (glabāšanas kontrole);

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

   (f) nodrošinātu, ka personām, kas ir pilnvarotas izmantot datu apstrādes automatizētu sistēmu, ir piekļuve tikai tiem datiem, uz kuriem attiecas viņu piekļuves tiesības, izmantojot individuālas un unikālas lietotāju identitātes un konfidenciālus pieejas veidus (datu piekļuves kontrole);

   (g) izstrādātu profilus, raksturojot to personu funkcijas un pienākumus, kuras ir pilnvarotas piekļūt datiem vai datu apstrādes iekārtām, un pēc 64. pantā minētā Eiropas Datu aizsardzības uzraudzītāja lūguma šos profilus nekavējoties darītu tām pieejamus (personālie profili);

   (h) nodrošinātu, ka ir iespējams pārbaudīt un noteikt struktūras, kurām personas dati var būt nosūtīti, izmantojot datu komunikācijas iekārtas (komunikācijas 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 (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 minēto aizsardzības pasākumu efektivitāti un veiktu vajadzīgos organizatoriskos pasākumus saistībā ar iekšējo uzraudzību, lai nodrošinātu atbilstību šai regulai (paškontrole).

2. Aģentūra veic 1. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz drošību saistībā ar papildinformācijas apstrādi un apmaiņu, izmantojot komunikācijas infrastruktūru.

17. pants
Konfidencialitāte - Aģentūra

1. Neskarot Eiropas Savienības Civildienesta noteikumu un Savienības pārējo darbinieku nodarbināšanas kārtības 17. pantu, Aģentūra visiem saviem darbiniekiem, kas strādā ar SIS datiem, piemēro pienācīgus noteikumus par dienesta noslēpumu vai citas līdzvērtīgas prasības attiecībā uz konfidencialitāti atbilstīgi standartiem, kas pielīdzināmi šīs regulas 11. pantā paredzētajiem. Šis pienākums ir spēkā arī pēc tam, kad minētās personas vairs neieņem attiecīgo amatu vai netiek nodarbinātas, vai viņu darbība ir izbeigta.

2. Aģentūra veic 1. punktā minētajiem pasākumiem līdzvērtīgus pasākumus attiecībā uz konfidencialitāti saistībā ar papildinformācijas apmaiņu, izmantojot komunikācijas infrastruktūru.

18. pants
Ierakstu glabāšana centrālajā līmenī

1. Aģentūra nodrošina, ka 12. panta 1. punktā minētajiem mērķiem tiek saglabāti ieraksti par katru piekļuvi CS-SIS saglabātajiem personas datiem un par visām minēto datu apmaiņām.

2. Ieraksti konkrēti parāda brīdinājumu vēsturi, datu pārraides datumu un laiku, meklēšanā izmantoto datu veidu, atsauci uz pārraidīti datu veidu, kā arī par datu apstrādi atbildīgās kompetentās iestādes nosaukumu.

3. Ja meklēšana veikta ar daktiloskopiskajiem datiem vai sejas attēlu saskaņā ar 40., 41. un 42. pantu, ieraksti konkrēti parāda meklēšanā izmantoto datu veidu, atsauci uz pārraidīto datu veidu un gan kompetentās iestādes nosaukumu, gan par datu apstrādi atbildīgās personas vārdu.

4. Ierakstus lieto vienīgi 1. punktā paredzētajos nolūkos 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 glabāt ilgāk, ja tie vajadzīgi uzraudzības procedūrām, kas jau ir iesāktas.

6. 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.

IV NODAĻA

SABIEDRĪBAS INFORMĒŠANA

19. pants
SIS informācijas kampaņas

Komisija sadarbībā ar valstu uzraudzības iestādēm un Eiropas Datu aizsardzības uzraudzītāju regulāri īsteno kampaņas, lai informētu sabiedrību par SIS mērķiem, glabātajiem datiem, iestādēm, kurām ir piekļuve SIS, un datu subjektu tiesībām. Dalībvalstis sadarbībā ar savām valsts uzraudzības iestādēm izstrādā un īsteno vajadzīgo politiku, lai informētu savus iedzīvotājus par SIS kopumā.

V NODAĻA

DATU KATEGORIJAS UN BRĪDINĀJUMU APZĪMĒŠANA AR KARODZIŅIEM

20. pants
Datu kategorijas

1. Neskarot 8. panta 1. punktu vai šīs regulas noteikumus par papildu datu glabāšanu, SIS ir ietverti tikai to kategoriju dati, ko ir iesniegusi katra dalībvalsts un kas ir vajadzīgi 26., 32., 34., 36. un 38. pantā noteiktajiem nolūkiem.

2. Datu kategorijas ir šādas:

   (a) informācija par personām, attiecībā uz kurām izdots brīdinājums;

   (b) informācija par priekšmetiem, kas minēti 32., 36. un 38. pantā.

3. Informācija par personām, attiecībā uz kurām brīdinājums ir izdots, ietver tikai šādus datus:

   (a) uzvārds(-i);

   (b) vārds(-i);

   (c) vārds, uzvārds (vārdi, uzvārdi) dzimšanas brīdī;

   (d) iepriekš lietoti vārdi un pseidonīmi;

   (e) īpašas fiziskās pazīmes, kas ir objektīvas un nemainīgas;

   (f) dzimšanas vieta;

   (g) dzimšanas datums,

   (h) dzimums;

   (i) valstspiederība/valstspiederības;

   (j) norāde, vai attiecīgā persona ir bruņota, vardarbīga, izbēgusi vai iesaistīta darbībā, kā minēts Padomes Pamatlēmuma 2002/475/TI par terorisma apkarošanu 1., 2., 3. un 4. pantā;

   (k) brīdinājuma iemesls;

(l) brīdinājuma izdevēja iestāde;

(m) norāde uz lēmumu, kas ir brīdinājuma pamatā;

(n) veicamā darbība;

(o) saite(-es) ar citiem brīdinājumiem, kas izdoti SIS saskaņā ar 53. pantu;

(p) noziedzīgā nodarījuma veids, par kuru brīdinājums izdots;

(q) personas reģistrācijas numurs valsts reģistrā;

(r) pazudušas personas gadījuma veids (tikai attiecībā uz brīdinājumiem, kas minēti 32. pantā) atbilstoši kategorijai;

(s) personas identifikācijas dokumenta kategorija;

(t) personas identifikācijas dokumenta izdošanas valsts;

(u) personas identifikācijas dokumenta numurs;

(v) personas identifikācijas dokumenta izdošanas datums;

(w) fotogrāfijas un sejas attēli;

(x) attiecīgie DNS profili saskaņā ar šīs regulas 22. panta 1. punkta b) apakšpunktu;

(y) daktiloskopiskie dati;

(z) identifikācijas dokumenta krāsu kopija.

4. Tehniskos noteikumus, kas vajadzīgi 2. un 3. punktā minēto datu ievadīšanai, atjaunināšanai, dzēšanai un meklēšanai, nosaka un izstrādā kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

5. Tehniskos noteikumus, kas vajadzīgi 3. punktā minēto datu meklēšanai, nosaka un izstrādā saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru. Šie tehniskie noteikumi ir līdzīgi tehniskajiem noteikumiem attiecībā uz meklēšanu CS-SIS, valsts eksemplārā un tehniskajos eksemplāros, kā minēts 53. panta 2. punktā, un ir balstīti uz vienotiem standartiem, kurus nosaka un izstrādā kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

21. pants
Samērīgums

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

2. Ja persona vai priekšmets, ko dalībvalsts meklē saistībā ar nodarījumu, kuram piemērojams Padomes Pamatlēmuma 2002/475/TI par terorisma apkarošanu 1. līdz 4. pants, dalībvalsts vienmēr izveido atbilstošu brīdinājumu saskaņā ar attiecīgi 34., 36. vai 38. pantu.

22. pants
Īpaši noteikumi fotogrāfiju, sejas attēlu, daktiloskopisko datu un DNS profilu ievadīšanai

1. Uz 20. panta 3. punkta w), x) un y) apakšpunktā minēto datu ievadīšanu SIS attiecas šādi noteikumi:

(a) fotogrāfijas, sejas attēlus, daktiloskopiskos datus un DNS profilus ievada vienīgi pēc īpašas kvalitātes pārbaudes, ko veic, lai pārliecinātos, ka ir ievērots datu kvalitātes minimuma standarts;

(b) DNS profilu var pievienot tikai 32. panta 2. punkta a) un c) apakšpunktā minētajiem brīdinājumiem un tikai tad, ja nav pieejamas identifikācijai piemērotas fotogrāfijas, sejas attēli vai daktiloskopiskie dati. Tādu personu DNS profilus, kas ir brīdinājuma subjekta tiešie augšupējie radinieki, pēcnācēji, brāļi vai māsas, var pievienot brīdinājumam ar nosacījumu, ka šīs personas dod nepārprotamu piekrišanu. DNS profilā neiekļauj personas rases piederību.

2. Šā panta 1. punktā un 40. pantā minēto datu glabāšanai nosaka kvalitātes standartus. Šo standartu specifikācijas nosaka kā īstenošanas pasākumus un atjaunina saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

23. pants
Prasības brīdinājuma ievadīšanai

1. Brīdinājumu par personu nevar ievadīt, ja trūkst 20. panta 3. punkta a), g), k), m), n) apakšpunktā, kā arī attiecīgā gadījumā p) apakšpunktā minēto datu, izņemot 40. pantā minētās situācijas.

2. Ievada arī visus pārējos 20. panta 3. punktā minētos datus, ja tie ir pieejami.

24. pants
Vispārīgi noteikumi par brīdinājumu apzīmēšanu ar karodziņiem

1. Ja kāda dalībvalsts uzskata, ka saskaņā ar 26., 32. un 36. pantu ievadīta brīdinājuma īstenošana nav saderīga ar attiecīgas valsts tiesību aktiem, starptautiskām saistībām vai būtiskām valsts interesēm, tā var pieprasīt brīdinājumam pievienot karodziņu, ar ko norāda, ka saskaņā ar brīdinājumu veicamā darbība netiks veikta tās teritorijā. Karodziņu pievieno izdevējas dalībvalsts *SIRENE* birojs.

2. Lai dalībvalstīm dotu iespēju pieprasīt, ka karodziņu pievieno saskaņā ar 26. pantu izdotam brīdinājumam, visām dalībvalstīm, veicot papildinformācijas apmaiņu, automātiski paziņo par jebkādu jaunu šajā kategorijā izdotu brīdinājumu.

3. Ja īpaši steidzamos un nopietnos gadījumos izdevēja dalībvalsts lūdz izpildīt darbību, brīdinājuma izpildītāja dalībvalsts apsver, vai tā var ļaut atcelt pēc tās lūguma pievienoto karodziņu. Ja izpildītāja dalībvalsts var to darīt, tā veic vajadzīgos pasākumus, lai nodrošinātu, ka veicamo darbību var veikt nekavējoties.

25. pants
To brīdinājumu apzīmēšana ar karodziņiem, kas saistās ar personu apcietināšanu nolūkā tās nodot

1. Ja uz gadījumu attiecas Pamatlēmums 2002/584/TI, karodziņu, ar ko norāda apcietināšanas nepieļaušanu, pievieno vienīgi brīdinājumam, kas saistīts ar personas apcietināšanu nolūkā to nodot, ja kompetentā tiesu iestāde saskaņā ar valsts tiesību aktiem Eiropas apcietināšanas ordera izpildei ir atteikusies to izpildīt, balstoties uz neizpildes pamatojumu, un ja ir pieprasīts brīdinājumam pievienot karodziņu.

2. Tomēr pēc kompetentas tiesu iestādes lūguma atbilstīgi valsts tiesību aktiem – vai nu balstoties uz vispārēju instrukciju, vai kādā īpašā gadījumā – var pieprasīt pievienot

karodziņu arī brīdinājumam par personu apcietināšanu nolūkā to nodot, ja ir acīmredzams, ka Eiropas apcietināšanas ordera izpilde būs jāatsaka.

VI NODAĻA

BRĪDINĀJUMI ATTIECĪBĀ UZ PERSONĀM, KO MEKLĒ, LAI TĀS APCIETINĀTU NOLŪKĀ TĀS NODOT VAI IZDOT

26. pants

Brīdinājumu izdošanas mērķi un nosacījumi

1. Datus par personām, ko meklē, lai apcietinātu nolūkā tās nodot, pamatojoties uz Eiropas apcietināšanas orderi, vai par personām, ko meklē, lai apcietinātu nolūkā tās izdot, ievada pēc izdevējas dalībvalsts tiesu iestādes lūguma.

2. Datus par personām, ko meklē, lai apcietinātu nolūkā tās nodot, arī ievada, pamatojoties uz apcietināšanas orderi, kas izdots atbilstīgi nolīgumiem, kuri saskaņā ar Līguma par Eiropas Savienību 37. pantu noslēgti starp Savienību un trešām valstīm par personu nodošanu, pamatojoties uz apcietināšanas orderi, ar kuriem paredzēta šāda apcietināšanas ordera pārsūtīšana, izmantojot SIS.

3. Jebkādu šajā regulā iekļautu atsauci uz Pamatlēmumu 2002/584/TI uzskata par atsauci arī uz atbilstošajiem noteikumiem nolīgumos, kas saskaņā ar Līguma par Eiropas Savienību 37. pantu noslēgti starp Eiropas Savienību un trešām valstīm par personu nodošanu, pamatojoties uz apcietināšanas orderi, ja minētie noteikumi paredz šāda apcietināšanas ordera pārsūtīšanu, izmantojot SIS.

4. Izdevēja dalībvalsts notiekošas meklēšanas operācijas gadījumā ar izdevējas dalībvalsts attiecīgās tiesu iestādes atļauju var uz laiku padarīt meklēšanai nepieejamu saskaņā ar šīs regulas 26. pantu ievadītu brīdinājumu par apcietināšanu, lai brīdinājumu nevarētu meklēt galalietotāji un tam varētu piekļūt tikai *SIRENE* biroji. Šo funkciju var izmantot uz laiku, kas nepārsniedz 48 stundas. Tomēr operatīvos nolūkos to var pagarināt vēl par 48 stundām. Dalībvalstis glabā statistiku par to brīdinājumu skaitu, kuriem šī funkcija ir izmantota.

27. pants

Papildu dati par personām, ko meklē, lai apcietinātu nolūkā tās nodot

1. Ja personu meklē, lai apcietinātu nolūkā to nodot, pamatojoties uz Eiropas apcietināšanas orderi, izdevēja dalībvalsts SIS ievada Eiropas apcietināšanas ordera oriģināleksemplāra kopiju.

2. Izdevēja dalībvalsts var ievadīt Eiropas apcietināšanas ordera tulkojuma kopiju vienā vai vairākās Eiropas Savienības oficiālajās valodās.

28. pants

Papildinformācija par personām, ko meklē, lai apcietinātu nolūkā tās nodot

Dalībvalsts, kas SIS ievadījusi brīdinājumu par personas apcietināšanu nolūkā to nodot, Pamatlēmuma 2002/584/TI 8. panta 1. punktā minēto informāciju paziņo visām dalībvalstīm, veicot papildinformācijas apmaiņu.

29. pants

Papildinformācija par personām, ko meklē, lai apcietinātu nolūkā tās izdot

1. Dalībvalsts, kas SIS ievadījusi brīdinājumu par personas apcietināšanu nolūkā to izdot, veicot papildinformācijas apmaiņu, visām dalībvalstīm paziņo šādu informāciju:

   (a) iestādi, kas izdevusi apcietināšanas pieprasījumu;

   (b) vai ir apcietināšanas orderis vai dokuments ar līdzīgu juridisku spēku, vai izpildāms spriedums;

   (c) noziedzīgā nodarījuma veidu un juridisko kvalifikāciju;

   (d) aprakstu par apstākļiem, kādos izdarīts noziedzīgais nodarījums, tostarp tā laiku, vietu un tās personas līdzdalības pakāpi noziedzīgajā nodarījumā, par kuru ir izdots brīdinājums;

   (e) ja iespējams, noziedzīgā nodarījuma sekas;

   (f) jebkādu citu informāciju, kas ir noderīga vai vajadzīga brīdinājuma izpildei.

2. Šā panta 1. punktā minētos datus nepaziņo, ja jau ir sniegti 27. un 28. pantā minētie dati un ja tos uzskata par pietiekamiem, lai attiecīgā dalībvalsts varētu izpildīt brīdinājumu.

30. pants

To brīdinājumu pārveide, kas attiecas uz personām, ko meklē, lai apcietinātu nolūkā tās nodot vai izdot

Ja apcietināšanu nav iespējams izdarīt – vai nu tāpēc, ka brīdinājuma saņēmēja dalībvalsts atsakās saskaņā ar 24. vai 25. pantā izklāstītajām procedūrām par apzīmēšanu ar karodziņiem, vai arī tāpēc, ka attiecībā uz brīdinājumu par personas apcietināšanu nolūkā to izdot vēl nav pabeigta izmeklēšana –, tad brīdinājuma saņēmēja dalībvalsts brīdinājumu uzskata par brīdinājumu nolūkā paziņot attiecīgās personas atrašanās vietu.

31. pants

Rīcība, pamatojoties uz brīdinājumu par personu, ko meklē, lai apcietinātu nolūkā to nodot vai izdot

1. Ja ir piemērojams Pamatlēmums 2002/584/TI, tad saskaņā ar 26. pantu SIS ievadītu brīdinājumu kopā ar 27. pantā minētajiem papildu datiem uzskata par Eiropas apcietināšanas orderi, kas izdots saskaņā ar minēto pamatlēmumu, un tam ir tāds pats juridisks spēks kā minētajam orderim.

2. Ja Pamatlēmums 2002/584/TI nav piemērojams, tad saskaņā ar 26. un 29. pantu SIS ievadītam brīdinājumam ir tāds pats juridiskais spēks kā pieprasījumam par pagaidu apcietināšanu saskaņā ar 16. pantu 1957. gada 13. decembra Eiropas Konvencijā par izdošanu vai 15. pantu 1962. gada 27. jūnija Beniluksa Līgumā par izdošanu un savstarpēju palīdzību krimināllietās.

VII NODAĻA

BRĪDINĀJUMI PAR PAZUDUŠĀM PERSONĀM

32. pants
Brīdinājumu izdošanas mērķi un nosacījumi

1. Datus par pazudušām personām vai personām, kuras jāaizsargā vai kuru atrašanās vieta ir jānoskaidro, ievada SIS pēc brīdinājuma izdevējas dalībvalsts kompetentas iestādes lūguma.

2. Var ievadīt datus par šādu kategoriju pazudušām personām:

   (a) pazudušas personas, kas jāaizsargā:

      i) viņu pašu aizsardzībai,

      ii) lai novērstu draudus;

   (b) pazudušas personas, kas nav jāaizsargā;

   (c) nolaupīšanas riskam pakļauti bērni saskaņā ar 4. punktu.

3. Šā panta 2. punkta a) apakšpunktu piemēro vienīgi personām, kas jāinternē pēc kompetentas iestādes lēmuma.

4. Brīdinājumu par bērnu, kā minēts 2. punkta c) apakšpunktā, ievada pēc tās dalībvalsts kompetentās tiesu iestādes pieprasījuma, kurai ir jurisdikcija lietās par vecāku atbildību saskaņā ar Padomes Regulu Nr. 2201/2003[74], ja pastāv konkrēts un acīmredzams risks, ka bērnu var nelikumīgi un nenovēršami aizvest no dalībvalsts, kurā atrodas kompetentā tiesu iestāde. Dalībvalstīs, kuras ir līgumslēdzējas puses 1996. gada 19. oktobra Hāgas konvencijai par piekritību, piemērojamiem tiesību aktiem, atzīšanu, izpildi un sadarbību attiecībā uz vecāku atbildību un bērnu aizsardzības pasākumiem, gadījumos, kad nav piemērojama Padomes Regula Nr. 2201/2003, ir piemērojami Hāgas konvencijas noteikumi.

5. Dalībvalstis nodrošina, ka SIS ievadītie dati norāda, pie kuras no 2. punktā minētajām kategorijām pieder pazudusī persona. Turklāt dalībvalstis arī nodrošina, ka SIS ievadītie dati norāda, kāda veida pazudušas vai neaizsargātas personas gadījums ir iesaistīts. Noteikumus par gadījumu veidu klasifikāciju un par šādu datu ievadīšanu nosaka un izstrādā ka īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

6. Četrus mēnešus pirms bērna, par kuru ir ievadīts brīdinājums saskaņā ar šo pantu, pilngadības, CS-SIS automātiski informē izdevēju dalībvalsti, ka pieprasījuma un veicamās darbības pamats ir jāatjaunina vai brīdinājums ir jādzēš.

7. Ja ir skaidra norāde, ka transportlīdzeklis, laiva vai gaisa kuģis ir saistīts ar personu, uz kuru attiecas brīdinājums, kas ievadīts saskaņā ar 2. punktu, par šādiem transportlīdzekļiem, laivām un gaisa kuģiem var izdot brīdinājumus, lai atrastu personu. Šādos gadījumos brīdinājumu par pazudušu personu un brīdinājumu par priekšmetu sasaista saskaņā ar 60. pantu. Tehniskos noteikumus, kas vajadzīgi šajā

[74] Padomes Regula (EK) Nr. 2201/2003 (2003. gada 27. novembris) par jurisdikciju un spriedumu atzīšanu un izpildi laulības lietās un lietās par abu laulāto vecāku atbildību un par Regulas (EK) Nr. 1347/2000 atcelšanu (OV L 338, 23.12.2003., 1. lpp.).

punktā minēto datu ievadīšanai, atjaunināšanai, dzēšanai un meklēšanai, nosaka un izstrādā kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

33. pants
Rīcība, pamatojoties uz brīdinājumu

1. Ja konstatē 32. pantā minētās personas atrašanās vietu, kompetentās iestādes, ievērojot šā panta 2. punktu, paziņo šīs personas atrašanās vietu brīdinājuma izdevējai dalībvalstij. Attiecībā uz pazudušiem bērniem vai bērniem, kas jāaizsargā, izpildītāja dalībvalsts tūlīt konsultējas ar izdevēju dalībvalsti, lai nekavējoties vienotos par pasākumiem, kas veicami bērna interešu aizsardzībai. Šīs regulas 32. panta 2. punkta a) un c) apakšpunktā minētajos gadījumos kompetentās iestādes var attiecīgo personu nogādāt drošībā, lai neļautu turpināt ceļojumu, ja to atļauj attiecīgās valsts tiesību akti.

2. Datu paziņošanai par pazudušu personu, kuras atrašanās vieta ir konstatēta un kura ir pilngadīga – ja tā nav datu paziņošana starp kompetentajām iestādēm –, ir vajadzīga minētās personas piekrišana. Kompetentās iestādes tomēr var ieinteresētajai personai, kas ziņoja par personas pazušanu, paziņot par brīdinājuma dzēšanu sakarā ar to, ka persona ir atrasta.

VIII NODAĻA

BRĪDINĀJUMI PAR PERSONĀM, KO MEKLĒ, LAI TĀS VARĒTU PALĪDZĒT TIESAS PROCESĀ

34. pants
Brīdinājumu izdošanas mērķi un nosacījumi

1. Lai darītu zināmu turpmāk minēto personu uzturēšanās vietu vai pastāvīgo dzīvesvietu, dalībvalstis pēc kompetento iestāžu lūguma SIS ievada datus par:

   (a) lieciniekiem;

   (b) personām, kurām izsniegta pavēste vai kuras cenšas atrast ar mērķi izsniegt šādu pavēsti, lai tās ierastos tiesu iestādēs saistībā ar kriminālatiesvedību, lai tās sauktu pie atbildības par nodarījumiem, kuru dēļ notiek viņu kriminālvajāšana;

   (c) personām, kurām jāizsniedz spriedums krimināllietā vai citi dokumenti saistībā ar kriminālatiesvedību, lai tās sauktu pie atbildības par nodarījumiem, kuru dēļ notiek viņu kriminālvajāšana;

   (d) personām, kurām jāizsniedz pavēste ierasties, lai izciestu brīvības atņemšanas sodu.

2. Ja ir skaidra norāde, ka transportlīdzeklis, laiva vai gaisa kuģis ir saistīts ar personu, uz kuru attiecas brīdinājums, kas ievadīts saskaņā ar 1. punktu, par šādiem transportlīdzekļiem, laivām un gaisa kuģiem var izdot brīdinājumus, lai atrastu personu. Šādos gadījumos brīdinājumu par personu un brīdinājumu par priekšmetu sasaista saskaņā ar 60. pantu. Tehniskos noteikumus, kas vajadzīgi šajā punktā minēto datu ievadīšanai, atjaunināšanai, dzēšanai un meklēšanai, nosaka un izstrādā kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

35. pants
Rīcība, pamatojoties uz brīdinājumu

Pieprasīto informāciju dara zināmu pieprasījuma iesniedzējai dalībvalstij, veicot papildinformācijas apmaiņu.

IX NODAĻA

BRĪDINĀJUMI PAR PERSONĀM UN PRIEKŠMETIEM SAISTĪBĀ AR DISKRĒTĀM PĀRBAUDĒM, IZMEKLĒŠANAS PĀRBAUDĒM VAI ĪPAŠĀM PĀRBAUDĒM

36. pants
Brīdinājumu izdošanas mērķi un nosacījumi

1. Lai nodrošinātu diskrētas pārbaudes, izmeklēšanas pārbaudes vai īpašas pārbaudes atbilstīgi 37. panta 4. punktam, datus par personām vai transportlīdzekļiem, laivām, gaisakuģiem un konteineriem ievada saskaņā ar brīdinājuma izdevējas dalībvalsts tiesību aktiem.

2. Brīdinājumu var izdot saistībā ar kriminālvajāšanu par noziedzīgiem nodarījumiem un nolūkā novērst draudus sabiedriskai drošībai:

   (a) ja ir skaidra norāde, ka attiecīgā persona ir nodomājusi izdarīt vai izdara smagu noziegumu, piemēram, Pamatlēmuma 2002/584/TI 2. panta 2. punktā minētu nodarījumu;

   (b) ja 37. panta 1. punktā minētā informācija ir nepieciešama, lai izpildītu krimināls odu personai, kas notiesāta par smagu noziegumu, piemēram, Pamatlēmuma 2002/584/TI 2. panta 2. punktā minētu nodarījumu; vai

   (c) ja personas vispārējs novērtējums, īpaši ņemot vērā līdz šim izdarītos noziedzīgos nodarījumus, ļauj uzskatīt, ka šī persona nākotnē var izdarīt arī smagu noziegumu, piemēram, Pamatlēmuma 2002/584/TI 2. panta 2. punktā minētu nodarījumu.

3. Turklāt saskaņā ar attiecīgās valsts tiesību aktiem brīdinājumu var izdot pēc to iestāžu lūguma, kuras ir atbildīgas par valsts drošību, ja ir konkrēta norāde, ka 37. panta 1. punktā minētā informācija ir vajadzīga, lai novērstu nopietnus draudus, ko rada attiecīgā persona, vai citus nopietnus draudus valsts iekšējai vai ārējai drošībai. Dalībvalsts, kas izdod brīdinājumu saskaņā ar šo punktu, par to informē pārējās dalībvalstis. Katra dalībvalsts nosaka, kurām iestādēm nosūta šo informāciju.

4. Ja ir skaidra norāde, ka transportlīdzeklis, laiva, gaisa kuģis un konteiners ir saistīts ar smagiem noziegumiem, kā minēts 2. punktā, vai nopietniem draudiem, kā minēts 3. punktā, var izdot brīdinājumu par šādu transportlīdzekli, laivu, gaisakuģi un konteineri.

5. Ja ir skaidra norāde, ka oficiālu dokumentu veidlapas vai izdoti personu apliecinoši dokumenti ir saistīti ar smagiem noziegumiem, kā minēts 2. punktā, vai nopietniem draudiem, kā minēts 3. punktā, var izdot brīdinājumus par šādiem dokumentiem, neatkarīgi no personu apliecinošā dokumenta oriģinālā turētājā identitātes, ja tāds pastāv. Tehniskos noteikumus, kas vajadzīgi šajā punktā minēto datu ievadīšanai,

atjaunināšanai, dzēšanai un meklēšanai, nosaka un izstrādā kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

37. pants
Rīcība, pamatojoties uz brīdinājumu

1. Lai veiktu diskrētas pārbaudes, izmeklēšanas pārbaudes vai īpašas pārbaudes, turpmāk norādīto informāciju vai tās daļu var apkopot un paziņot brīdinājuma izdevējai iestādei, ja dalībvalstī veic robežkontroli, policijas un muitas kontroles vai citus tiesībaizsardzības pasākumus:

   (a) to, ka ir atrasta persona vai transportlīdzeklis, laiva, gaisa kuģis, konteiners, oficiāla dokumenta veidlapa vai izdots personu apliecinošs dokuments, par ko ir izdots brīdinājums;

   (b) kontroles vieta, laiks un iemesls;

   (c) ceļojuma maršruts un galamērķis;

   (d) personas, kas pavada attiecīgo personu, vai transportlīdzekļa, laivas vai gaisakuģa pasažierus, vai kas pavada oficiāla dokumenta veidlapas turētāju vai izdota personu apliecinoša dokumenta turētāju, par kurām ir pietiekams pamats uzskatīt, ka tās ir saistītas ar attiecīgajām personām;

   (e) atklātā personas identitāte un apraksts par to personu, kura izmanto oficiālā dokumenta veidlapu vai izdoto personu apliecinošo dokumentu, uz kuru attiecas brīdinājums;

   (f) izmantotais transportlīdzeklis, laiva, gaisa kuģis vai konteiners;

   (g) transportētie priekšmeti, tostarp ceļošanas dokumenti;

   (h) apstākļi, kādos persona vai transportlīdzeklis, laiva, gaisa kuģis, konteiners, oficiālā dokumenta veidlapa vai izdotais personu apliecinošais dokuments ir atrasts.

2. Šā panta 1. punktā minēto informāciju paziņo, veicot papildinformācijas apmaiņu.

3. Atkarībā no operatīvajiem apstākļiem un saskaņā ar valsts tiesību aktiem diskrēta pārbaude ir personas vai priekšmeta regulārā pārbaude, lai savāktu tik daudz 1. punktā minētās informācijas, cik vien iespējams, neapdraudot diskrētas pārbaudes būtību.

4. Atkarībā no operatīvajiem apstākļiem un saskaņā ar valsts tiesību aktiem izmeklēšanas pārbaude ir padziļināta pārbaude un personas iztaujāšana. Ja saskaņā ar dalībvalsts tiesību aktiem izmeklēšanas pārbaudes nav atļautas, šajā dalībvalstī tās automātiski aizstāj ar diskrētām pārbaudēm.

5. Veicot īpašās pārbaudes, 36. pantā minētajos nolūkos personas, transportlīdzekļus, laivas, gaisakuģus, konteinerus un transportējamos priekšmetus var pārmeklēt atbilstīgi attiecīgās valsts tiesību aktiem. Pārmeklēšanu īsteno saskaņā ar attiecīgās valsts tiesību aktiem. Ja saskaņā ar dalībvalsts tiesību aktiem īpašās pārbaudes nav atļautas, šajā dalībvalstī tās automātiski aizstāj ar izmeklēšanas pārbaudēm.

X NODAĻA

BRĪDINĀJUMI PAR PRIEKŠMETIEM, KO MEKLĒ, LAI IZŅEMTU VAI IZMANTOTU PAR PIERĀDĪJUMU KRIMINĀLPROCESĀ

38. pants
Brīdinājumu izdošanas mērķi un nosacījumi

1. SIS ievada datus par priekšmetiem, ko meklē, lai izņemtu tiesībaizsardzības nolūkos vai izmantotu par pierādījumu kriminālprocesā.

2. Ievada datus par šādām viegli identificējamu priekšmetu kategorijām:

   (a) mehāniskie transportlīdzekļi, kā noteikts valsts tiesību aktos, neatkarīgi no piedziņas sistēmas;

   (b) piekabes, kuru pašmasa pārsniedz 750 kg;

   (c) dzīvojamie furgoni;

   (d) rūpniecības iekārtas;

   (e) laivas;

   (f) laivu dzinēji;

   (g) konteineri;

   (h) gaisa kuģi;

   (i) šaujamieroči;

   (j) nozagtas, nelikumīgi piesavinātas vai pazudušas oficiālu dokumentu veidlapas;

   (k) personu apliecinoši dokumenti, kas nozagti, nelikumīgi piesavināti, pazuduši, anulēti vai, būdami viltoti, tiek uzdoti par īstiem, piemēram, pases, identifikācijas kartes, transportlīdzekļa vadītāja apliecības, uzturēšanās atļaujas un ceļošanas dokumenti;

   (l) transportlīdzekļu reģistrācijas apliecības un transportlīdzekļa numura zīmes, kas nozagtas, nelikumīgi piesavinātas, pazaudētas, anulētas vai, būdamas viltotas, tiek uzdotas par īstām;

   (m) banknotes (reģistrētas naudaszīmes) un viltotas banknotes;

   (n) tehniskais aprīkojums, informācijas tehnoloģiju vienības un citi augstvērtīgi viegli identificējami priekšmeti;

   (o) mehānisko transportlīdzekļu identificējamas detaļas;

   (p) rūpniecības iekārtu identificējamas detaļas.

3. Jaunu priekšmetu apakškategoriju definēšanu saskaņā ar 2. punkta n) apakšpunktu un tehniskos noteikumus, kas vajadzīgi 2. punktā minēto datu ievadīšanai, atjaunināšanai, dzēšanai un meklēšanai, nosaka un izstrādā kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

39. pants

Rīcība, pamatojoties uz brīdinājumu

1. Ja meklēšanā konstatē brīdinājumu par atrastu priekšmetu, tad iestāde, kas to konstatējusi, saskaņā ar valsts tiesību aktiem izņem priekšmetu un sazinās ar brīdinājuma izdevēju iestādi, lai vienotos par veicamajiem pasākumiem. Šajā nolūkā var arī paziņot personas datus saskaņā ar šo regulu.

2. Šā panta 1. punktā minēto informāciju paziņo, veicot papildinformācijas apmaiņu.

3. Dalībvalsts, kura atradusi priekšmetu, veic prasītos pasākumus saskaņā ar saviem tiesību aktiem.

XI NODAĻA

BRĪDINĀJUMI PAR NEZINĀMĀM MEKLĒTĀM PERSONĀM IDENTIFIKĀCIJAS NOLŪKĀ SASKAŅĀ AR VALSTS TIESĪBU AKTIEM UN MEKLĒŠANA, IZMANTOJOT BIOMETRISKOS DATUS

40. pants

Brīdinājumi par nezināmām meklētām personām aizturēšanai saskaņā ar valsts tiesību aktiem

Daktiloskopiskos datus var ievadīt SIS nesaistīti ar personām, kuras ir brīdinājumu subjekti. Šādi daktiloskopiskie dati ir vai nu pilns vai daļējs pirkstu nospiedumu vai plaukstu nospiedumu komplekts, kas konstatēts izmeklēšanā noziedzīga nodarījuma, smaga nozieguma un teroristu nodarījuma izdarīšanas vietā, ja var konstatēt augstu varbūtības pakāpi, ka tie pieder nodarījuma izdarītājam. Daktiloskopiskos datus šajā kategorijā glabā kā "nezināms aizdomās turētais vai meklēta persona", ar nosacījumu, ka kompetentās iestādes nevar noteikt personas identitāti, izmantojot jebkuru citu valsts, Eiropas vai starptautisku datubāzi.

41. pants

Rīcība, pamatojoties uz brīdinājumu

Trāpījuma vai iespējamas atbilstības ar datiem, kas glabāti saskaņā ar 40. pantu, gadījumā personas identitāti nosaka saskaņā ar valsts tiesību aktiem, vienlaikus pārliecinoties, ka SIS saglabātie daktiloskopiskie dati pieder šai personai. Dalībvalstis sazinās savā starpā, apmainoties ar papildinformāciju, lai atvieglotu savlaicīgu lietas izskatīšanu.

42. pants

Īpaši noteikumi pārbaudēm vai meklēšanai, izmantojot fotogrāfijas, sejas attēlus, daktiloskopiskos datus un DNS profilus

1. Fotogrāfijas, sejas attēlus, daktiloskopiskos datus un DNS profilus izgūst no SIS, lai pārbaudītu tāda trešās valsts valstspiederīgā identitāti, kurš noteikts SIS burtciparu meklēšanas rezultātā.

2. Daktiloskopiskos datus var arī izmantot, lai identificētu personu. Daktiloskopiskos datus, kas glabājas SIS, var izmantot meklēšanā identifikācijas nolūkos, ja personas identitāti nevar noskaidrot, izmantojot citus līdzekļus.

3. Daktiloskopiskajos datos, ko glabā SIS saistībā ar brīdinājumiem, kas izdoti saskaņā ar 26. pantu, 34. panta 1. punkta b) un d) apakšpunktu un 36. pantu, var meklēt arī, izmantojot pilnu vai nepilnu pirkstu nospiedumu komplektu vai delnas nospiedumus,

kas konstatēti izmeklējamu noziedzīgu nodarījumu izdarīšanas vietās, ja var konstatēt augstu varbūtības pakāpi, ka tie pieder nodarījuma izdarītājam, ar nosacījumu, ka kompetentās iestādes nespēj noteikt tās personas identitāti, izmantojot jebkuru citu valsts, Eiropas vai starptautisku datu bāzi.

4. Tiklīdz tas tehniski ir iespējams un vienlaikus nodrošinot augstu identifikācijas uzticamības pakāpi, fotogrāfijas un sejas attēlus var izmantot personas identificēšanai. Identificēšanu, pamatojoties uz fotogrāfijām vai sejas attēliem, izmanto tikai regulārās robežšķērsošanas vietās, kurās izmanto pašapkalpošanās sistēmas un automatizētas robežkontroles sistēmas.

XII NODAĻA

PIEKĻUVES TIESĪBAS UN BRĪDINĀJUMU SAGLABĀŠANA

43. pants
Iestādes, kurām ir tiesības piekļūt brīdinājumiem

1. Piekļuve SIS ievadītajiem datiem un tiesības tieši meklēt šajos datos vai SIS datu eksemplārā ir tikai iestādēm, kas ir atbildīgas par to, lai:

   a) veiktu robežkontroli saskaņā ar 2016. gada 9. marta Eiropas Parlamenta un Padomes Regulu (EK) Nr. 2016/399, ar kuru ievieš Savienības Kodeksu par noteikumiem, kas reglamentē personu pārvietošanos pār robežām (Šengenas Robežu kodekss);

   b) veiktu attiecīgajā dalībvalstī paredzētās policijas un muitas pārbaudes un lai norīkotās iestādes koordinētu šādas pārbaudes;

   c) īstenotu citas tiesībaizsardzības darbības, ko veic, lai novērstu, atklātu un izmeklētu noziedzīgus nodarījumus attiecīgajā dalībvalstī;

   d) izpētītu nosacījumus un pieņemtu lēmumus saistībā ar trešo valstu valstspiederīgo ieceļošanu un uzturēšanos dalībvalstu teritorijā, tostarp attiecībā uz uzturēšanās atļaujām un ilgtermiņa uzturēšanās vīzām, un trešo valstu valstspiederīgo atgriešanu.

2. Tiesības piekļūt SIS ievadītajiem datiem un tieši meklēt 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. Tiesības piekļūt SIS ievadītajiem datiem un tieši meklēt šajos datos var izmantot iestādes, kas ir kompetentas veikt uzdevumus, kas minēti 1. punkta c) apakšpunktā, veicot minētos uzdevumus. Šo iestāžu piekļuvi reglamentē katras dalībvalsts tiesību akti.

4. Šajā pantā minētās iestādes iekļauj 53. panta 8. punktā minētajā sarakstā.

44. pants

Transportlīdzekļu reģistrācijas iestādes

1. Dalībvalstu dienestiem, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izdošanu, kā minēts Padomes Direktīvā 1999/37/EK[75], ir piekļuve šādiem datiem, kas ievadīti SIS saskaņā ar šīs regulas 38. panta 2. punkta a), b), c) un l) apakšpunktu, vienīgi nolūkā pārbaudīt, vai tām reģistrācijai pieteiktie transportlīdzekļi nav zagti, nelikumīgi piesavināti vai pazaudēti un vai netiek meklēti kā pierādījums kriminālprocesā:

   (a) datiem par mehāniskajiem transportlīdzekļiem, kā noteikts valsts tiesību aktos, neatkarīgi no piedziņas sistēmas;

   (b) datiem par piekabēm, kuru pašmasa pārsniedz 750 kg, un datiem par dzīvojamiem furgoniem;

   (c) datiem par nozagtām, nelikumīgi piesavinātam, pazudušām vai nederīgām transportlīdzekļu reģistrācijas apliecībām un transportlīdzekļu numura zīmēm.

   Šo dienestu, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izdošanu, piekļuvi minētajiem datiem reglamentē attiecīgās dalībvalsts valsts tiesību akti.

2. Šā panta 1. punktā minētajiem dienestiem, kas ir valdības dienesti, ir tiesības tieši piekļūt SIS ievadītajiem datiem.

3. Šā panta 1. punktā minētajiem dienestiem, kas nav valdības dienesti, ir tiesības piekļūt SIS ievadītajiem datiem vienīgi ar iestādes starpniecību, kā paredzēts šīs regulas 43. pantā. Minētājai iestādei ir tiesības tieši piekļūt datiem un nodot tos attiecīgajam dienestam. Attiecīgā dalībvalsts nodrošina, ka atbilstīgajam dienestam un tā darbiniekiem izvirza prasību ievērot jebkādus ierobežojumus par to datu pieļaujamo izmantošanu, kurus tiem sniegusi iestāde.

4. Šīs regulas 39. pantu nepiemēro piekļuvei, kas iegūta saskaņā ar šo pantu. Ja 1. punktā minētie dienesti, piekļūstot SIS, atklāj informāciju, kas rada aizdomas par noziedzīga nodarījuma izdarīšanu, šādas informācijas paziņošanu policijai vai tiesu iestādēm reglamentē attiecīgās valsts tiesību akti.

45. pants

Laivu un gaisa kuģu reģistrācijas iestādes

1. Dalībvalstu dienestiem, kas ir atbildīgi par laivu, tostarp laivu dzinēju, un gaisa kuģu reģistrācijas apliecību izdošanu vai satiksmes pārvaldības nodrošināšanu, ir piekļuve šādiem datiem, kas ievadīti SIS saskaņā ar šīs regulas 38. panta 2. punktu, vienīgi nolūkā pārbaudīt, vai tām reģistrācijai pieteikta vai satiksmes pārvaldībai pakļauta laiva, tostarp laivas dzinējs, gaisa kuģis vai konteiners nav zagts, nelikumīgi piesavināts vai pazaudēts un vai netiek meklēts kā pierādījums kriminālprocesā:

   (a) dati par laivām;

   (b) dati par laivu dzinējiem;

   (c) dati par gaisa kuģiem.

[75] Padomes Direktīva 1999/37/EK (1999. gada 29. aprīlis) par transportlīdzekļu reģistrācijas dokumentiem (OV L 138, 1.6.1999., 57. lpp.).

Ievērojot 2. punktu, katras dalībvalsts tiesību akti reglamentē attiecīgo dienestu piekļuvi šiem datiem attiecīgajā dalībvalstī. Piekļuve a) līdz c) apakšpunktā minētajiem datiem aprobežojas ar attiecīgo dienestu īpašo kompetenci.

2. Šā panta 1. punktā minētajiem dienestiem, kas ir valdības dienesti, ir tiesības tieši piekļūt SIS ievadītajiem datiem.

3. Šā panta 1. punktā minētajiem dienestiem, kas nav valdības dienesti, ir tiesības piekļūt SIS ievadītajiem datiem vienīgi ar iestādes starpniecību, kā paredzēts šīs regulas 43. pantā. Minētājai iestādei ir tiesības tieši piekļūt datiem un nodot tos attiecīgajam dienestam. Attiecīgā dalībvalsts nodrošina, ka atbilstīgajam dienestam un tā darbiniekiem izvirza prasību ievērot jebkādus ierobežojumus par to datu pieļaujamo izmantošanu, kurus tiem sniegusi iestāde.

4. Šīs regulas 39. pantu nepiemēro piekļuvei, kas iegūta saskaņā ar šo pantu. Ja 1. punktā minētie dienesti, piekļūstot SIS, atklāj informāciju, kas rada aizdomas par noziedzīgu nodarījumu, šādas informācijas paziņošanu policijai vai tiesu iestādēm reglamentē attiecīgās valsts tiesību akti.

46. pants
Eiropola piekļuve SIS datiem

1. Eiropas Savienības Aģentūrai tiesībaizsardzības sadarbībai un apmācībai (Eiropolam) atbilstīgi savām pilnvarām ir tiesības piekļūt datiem, kas ievadīti SIS, un meklēt tajos.

2. Ja Eiropola veiktā meklēšanā konstatē, ka SIS ir brīdinājums, Eiropols informē izdevēju dalībvalsti, izmantojot kanālus, kas definēti Regulā (ES) Nr. 2016/794.

3. SIS meklēšanā iegūtās informācijas izmantošanai ir vajadzīga attiecīgās dalībvalsts piekrišana. Ja attiecīgā dalībvalsts atļauj izmantot šādu informāciju, Eiropola darbības ar šo informāciju reglamentē Regula (ES) 2016/794. Eiropols var šādu informāciju sniegt trešām valstīm un trešām struktūrām vienīgi ar attiecīgās dalībvalsts piekrišanu.

4. Saskaņā ar Regulas (ES) 2016/794 noteikumiem Eiropols var lūgt attiecīgajai dalībvalstij sīkāku informāciju.

5. Eiropols:

(a) neskarot 3., 4. un 6. punktu, nesasaista SIS daļas un nepārsūta tur esošos datus, kuriem tas var piekļūt, nevienai datorsistēmai datu vākšanai un apstrādei, kas darbojas Eiropola pakļautībā vai Eiropolā, kā arī neveic nekādu SIS daļu lejupielādi vai citādu kopēšanu;

(b) tiesības piekļūt SIS ievadītajiem datiem nodrošina vienīgi īpaši pilnvarotiem Eiropola darbiniekiem;

(c) pieņem un piemēro 10. un 11. pantā paredzētos pasākumus;

(d) ļauj Eiropas Datu aizsardzības uzraudzītājam pārbaudīt Eiropola darbības, ko tas veic, īstenojot tiesības piekļūt SIS ievadītajiem datiem un veikt meklēšanu šajos datos.

6. Datus var kopēt vienīgi tehniskos nolūkos, ja šāda kopēšana ir vajadzīga, lai pienācīgi pilnvaroti Eiropola darbinieki varētu veikt tiešu meklēšanu šajos datos. Uz šādām kopijām attiecas šī regula. Tehnisko kopiju izmanto, lai saglabātu SIS datus,

kamēr tajos notiek meklēšana. Tiklīdz meklēšana ir pabeigta, datus dzēš. Šādu izmantošanu neuzskata par nelikumīgu lejupielādi vai SIS datu kopēšanu. Eiropols nekopē brīdinājumu datus vai papildu datus, ko izdevušas dalībvalstis, vai no CS-SIS citās Eiropola sistēmās.

7. Visas 6. punktā minētās kopijas, kuru rezultātā veidojas bezsaistes datubāzes, drīkst saglabāt laiku, ka nav ilgāks par 48 stundām. Ārkārtas situācijās šo laiku var pagarināt līdz ārkārtas situācijas beigām. Eiropols ziņo par visiem šādiem pagarinājumiem Eiropas Datu aizsardzības uzraudzītājam.

8. Eiropols var saņemt un apstrādāt papildinformāciju par atbilstošajiem SIS brīdinājumiem ar nosacījumu, ka tiek attiecīgi piemēroti datu apstrādes noteikumi, kas minēti 2. – 7. punktā.

9. Lai pārbaudītu datu apstrādes likumību, veiktu pašuzraudzību un nodrošinātu datu pienācīgu integritāti un drošību, Eiropols saglabā ierakstus par katru piekļuvi un meklēšanu SIS. Šādus ierakstus un dokumentus neuzskata par nelikumīgu SIS sastāvdaļu lejupielādi vai kopēšanu.

47. pants
Eurojust piekļuve SIS datiem

1. *Eurojust* valstu locekļiem un viņu asistentiem atbilstīgi viņu pilnvarām ir tiesības piekļūt datiem, kas SIS ievadīti atbilstīgi viņu pilnvarām un saskaņā ar 26., 32., 34., 38. un 40. pantu, un veikt meklēšanu šajos datos.

2. Ja *Eurojust* valsts locekļa veiktā meklēšanā konstatē, ka SIS ir brīdinājums, attiecīgais valsts loceklis informē brīdinājuma izdevēju dalībvalsti.

3. Neko šajā pantā neinterpretē kā tādu, kas ietekmē Lēmuma 2002/187/TI noteikumus par datu aizsardzību un *Eurojust* valstu locekļu vai viņu asistentu atbildību par šādu datu neatļautu vai nepareizu apstrādi, vai kā tādu, kas ietekmē saskaņā ar minēto lēmumu izveidotās Apvienotās uzraudzības iestādes pilnvaras.

4. Saskaņā ar 12. pantu saglabā ierakstus par ikvienu piekļuvi vai meklēšanu, ko veic *Eurojust* valsts loceklis vai asistents, un saglabā ierakstus par to datu izmantošanu, kam viņi ir piekļuvuši.

5. Nevienu SIS daļu nepievieno nevienai datorsistēmai datu vākšanai un apstrādei, ko darbina *Eurojust*, un SIS iekļautos datus, kuriem piekļūst valsts locekļi vai asistenti, nenosūta nevienai šādai datorsistēmai. SIS daļas netiek lejupielādētas. Ierakstu glabāšanu par piekļuvi un meklēšanu neuzskata par nelikumīgu lejupielādi vai SIS datu kopēšanu.

6. Tiesības piekļūt SIS ievadītajiem datiem nodrošina vienīgi valstu locekļiem un viņu asistentiem, un šīs tiesības neattiecina uz *Eurojust* personālu.

7. Pieņem un piemēro 10. pantā un 11. pantā paredzētos pasākumus drošības un konfidencialitātes nodrošināšanai.

48. pants

Piekļuve SIS datiem, ko piešķir Eiropas robežu un krasta apsardzes vienībām, tāda personāla vienībām, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, un migrācijas pārvaldības atbalsta vienībai

1. Saskaņā ar Regulas (ES) Nr. 2016/1624 40. panta 8. punktu Eiropas Robežu un krasta apsardzes vienību vai tāda personāla vienību, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, kā arī migrācijas pārvaldības atbalsta vienību dalībniekiem atbilstīgi savām pilnvarām ir tiesības piekļūt SIS un meklēt SIS ievadītajos datos.

2. Saskaņā ar 1. punktu Eiropas Robežu un krasta apsardzes vienību vai tāda personāla vienību, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, kā arī migrācijas pārvaldības atbalsta vienību dalībnieki piekļūst SIS un meklē SIS ievadītajos datos, izmantojot tehnisko saskarni, ko izveido un uztur Eiropas Robežu un krasta apsardzes aģentūra, kā minēts 49. panta 1. punktā.

3. Ja Eiropas Robežu un krasta apsardzes vienību vai tāda personāla vienību, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, vai migrācijas pārvaldības atbalsta vienības dalībnieka veiktā meklēšanā atklājas brīdinājums SIS, par to informē izdevēju dalībvalsti. Saskaņā ar Regulas (ES) Nr. 2016/1624 40. pantu vienību dalībnieki saistībā ar brīdinājumu SIS var rīkoties tikai saskaņā ar uzņēmējas dalībvalsts, kurā tie darbojas, robežsargu vai ar atgriešanu saistītos uzdevumos iesaistītā personāla norādījumiem un parasti tikai viņu klātbūtnē. Uzņēmēja dalībvalsts var vienību dalībniekus pilnvarot rīkoties tās vārdā.

4. Saskaņā ar 12. panta noteikumiem saglabā ierakstus par katru piekļuves gadījumu un katru meklēšanu, ko veic Eiropas Robežu un krasta apsardzes vienību vai tāda personāla vienību, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, vai migrācijas pārvaldības atbalsta vienības dalībnieks un saglabā ierakstus par katru to datu izmantošanu, kuriem piekļuvuši minētie vienību dalībnieki.

5. Piekļuve datiem, kas ievadīti SIS, attiecas tikai uz Eiropas Robežu un krasta apsardzes vienību vai tāda personāla vienību, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, vai migrācijas pārvaldības atbalsta vienības dalībnieku, un to neattiecina uz citiem vienību dalībniekiem.

6. Pieņem un piemēro 10. pantā un 11. pantā paredzētos pasākumus drošības un konfidencialitātes nodrošināšanai.

49. pants

Eiropas Robežu un krasta apsardzes aģentūras piekļuve SIS

1. Eiropas Robežu un krasta apsardzes aģentūra 48. panta 1. punkta nolūkos un šā panta 2. punkta nolūkos izveido un uztur tehnisko saskarni, kas ļauj nodrošināt tiešu savienojumu ar centrālo SIS.

2. Eiropas Robežu un krasta apsardzes aģentūrai, lai veiktu uzdevumus, kas tai uzticēti ar Regulu, ar ko izveido ES ceļošanas informācijas un atļauju sistēmu (*ETIAS*), ir tiesības piekļūt SIS ievadītajiem datiem un meklēt šajos datos saskaņā ar 26., 32., 34., 36. pantu un 38. panta 2. punkta j) un k) apakšpunktu.

3. Ja pārbaudē, ko veic Eiropas Robežu un krasta apsardzes aģentūra, atklājas brīdinājums SIS, piemēro procedūru, kas noteikta Regulas, ar ko izveido ES ceļošanas informācijas un atļauju sistēmu (*ETIAS*), 22. pantā.

4. Neko šajā pantā neinterpretē kā tādu, kas ietekmētu Regulas (ES) Nr. 2016/1624 noteikumus par datu aizsardzību un atbildību par jebkādu neatļautu vai nepareizu datu apstrādi, ja to veic Eiropas Robežu un krasta apsardzes aģentūra.

5. Saskaņā ar 12. panta noteikumiem saglabā ierakstus par katru piekļuves gadījumu un katru meklēšanu, ko veic Eiropas Robežu un krasta apsardzes aģentūra, un saglabā ierakstus par katru to datu izmantošanu, kuriem tā piekļuvusi.

6. Izņemot gadījumus, kad tas ir vajadzīgs, lai veiktu uzdevumus Regulas, ar ko izveido Eiropas ceļojumu informācijas un atļauju sistēmas (*ETIAS*) nolūkos, nevienu SIS daļu nepievieno nevienai datorsistēmai datu vākšanai un apstrādei, ko darbina Eiropas Robežu un krasta apsardzes aģentūra vai ko darbina tās ietvaros, un SIS iekļautos datus, kuriem piekļuvusi Eiropas Robežu un krasta apsardzes aģentūra nenosūta nevienai šādai sistēmai. SIS daļas netiek lejupielādētas. Ierakstu saglabāšanu par piekļuvi un meklēšanu neuzskata par nelikumīgu lejupielādi vai SIS datu kopēšanu.

7. Eiropas Robežu un krasta apsardzes aģentūra pieņem un piemēro 10. pantā un 11. pantā paredzētos pasākumus drošības un konfidencialitātes nodrošināšanai.

50. pants
Piekļuves apjoms

Galalietotāji, tostarp Eiropols, *Eurojust* valstu locekļi un viņu asistenti un Eiropas Robežu un krasta apsardzes aģentūra, var piekļūt vienīgi tiem datiem, kas ir vajadzīgi attiecīgo lietotāju uzdevumu veikšanai.

51. pants
Brīdinājumu saglabāšanas periods

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

2. Dalībvalsts, kas izdod brīdinājumu, piecos gados pēc tā ievadīšanas SIS izvērtē vajadzību to saglabāt. Brīdinājumus, kas izdoti saskaņā ar šīs regulas 36. pantu, glabā ilgākais vienu gadu.

3. Saskaņā ar 38. pantu ievadītus brīdinājumus par oficiālu dokumentu veidlapām glabā ilgākais desmit gadus. Īsākus saglabāšanas periodus brīdinājumu par priekšmetiem kategorijām var noteikt ar īstenošanas pasākumiem, kurus pieņem saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

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

5. Gadījumos, kad *SIRENE* biroja darbiniekam, kurš atbild par datu kvalitātes koordināciju un pārbaudi, kļūst skaidrs, ka brīdinājums par personu ir sasniedzis savu mērķi un to būtu jādzēš no SIS, darbinieks paziņo iestādei, kas izveidojusi brīdinājumu, lai pievērstu iestādes uzmanību šim jautājumam. Iestāde 30 kalendāro dienu laikā no šāda paziņojuma saņemšanas norāda, ka brīdinājums ir dzēsts vai tiks dzēsts, vai norāda iemeslus saglabāt brīdinājumu. Ja 30 dienu termiņš beidzas un šāda atbilde nav saņemta, brīdinājumu dzēš *SIRENE* biroja darbinieks. *SIRENE* biroji par šādu problēmu atkārtošanos šajā jomā ziņo savai valsts uzraudzības iestādei.

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

7. Brīdinājumus automātiski dzēš, tiklīdz beidzas 2. punktā minētais izvērtēšanas termiņš, izņemot gadījumu, kad brīdinājuma izdevēja dalībvalsts saskaņā ar 6. punktu ir paziņojusi CS-SIS par brīdinājuma termiņa pagarināšanu. CS-SIS četrus mēnešus iepriekš automātiski informē dalībvalstis par paredzamo datu dzēšanu sistēmā.

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

XIII NODAĻA

BRĪDINĀJUMU DZĒŠANA

52. pants
Brīdinājumu dzēšana

1. Brīdinājumus par apcietināšanu nolūkā nodot vai izdot saskaņā ar 26. pantu dzēš pēc tam, kad persona ir nodota vai izdota izdevējas dalībvalsts kompetentajām iestādēm. Tos var arī dzēst, ja kompetentā tiesu iestāde saskaņā ar valsts tiesību aktiem ir atcēlusi tiesas nolēmums, uz kura pamata bija izdots brīdinājums.

2. Brīdinājumus par pazudušām personām dzēš saskaņā ar šādiem noteikumiem:

   (a) brīdinājumu par pazudušiem bērniem saskaņā ar 32. pantu dzēš:

   – ja lieta ir atrisināta, piemēram, ja bērns ir repatriēts vai kompetentās iestādes izpildītājā dalībvalstī ir pieņēmušas lēmumu par bērna aprūpi;

   – beidzoties brīdinājuma termiņam saskaņā ar 51. pantu;

   – saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu, vai

   – ja bērns ir atrasts;

   (b) brīdinājumus par pazudušiem pieaugušajiem saskaņā ar 32. pantu, ja nav jāveic nekādi aizsardzības pasākumi, dzēš:

   – izpildot veicamo darbību (izpildītāja dalībvalsts ir konstatējusi atrašanās vietu);

   – beidzoties brīdinājuma termiņam saskaņā ar 51. pantu; vai

   – saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu.

   (c) brīdinājumus par pazudušiem pieaugušajiem saskaņā ar 32. pantu, ja ir jāveic aizsardzības pasākumi, dzēš:

   – īstenojot veicamo darbību (personai piešķirta aizsardzība);

   – beidzoties brīdinājuma termiņam saskaņā ar 51. pantu; vai

– saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu.

Ievērojot valsts tiesību aktus, ja persona ir internēta saskaņā ar kompetentās iestādes lēmumu, brīdinājumu var saglabāt līdz brīdim, kamēr attiecīgā persona ir repatriēta.

3. Brīdinājumus par personām, kuras meklē tiesas procesam, dzēš saskaņā ar šādiem noteikumiem:

brīdinājumus par personām, kuras meklē tiesas procesam, saskaņā ar 34. pantu dzēš:

(a) personas atrašanās vietu paziņojot izdevējas dalībvalsts kompetentajai iestādei. Ja attiecībā uz nosūtīto informāciju nevar veikt nekādu rīcību, izdevējas dalībvalsts *SIRENE* birojs par to informē izpildītājas dalībvalsts *SIRENE* biroju nolūkā atrisināt problēmu;

(b) beidzoties brīdinājuma termiņam saskaņā ar 51. pantu; vai

(c) saskaņā ar izdevējas dalībvalsts kompetentās iestādes lēmumu.

Ja kādā dalībvalstī ir gūts trāpījums un ziņas par adresi ir nosūtītas izdevējai dalībvalstij, un ja attiecīgajā dalībvalstī pēc tam ir gūts trāpījums, kurā tiek konstatēta tā pati adrese, šo trāpījumu ieraksta izpildītājā dalībvalstī, taču izdevējai dalībvalstij netiek atkārtoti nosūtītas ne ziņas par adresi, ne papildinformācija. Šādos gadījumos izpildītāja dalībvalsts informē izdevēju dalībvalsti par atkārtoto trāpījumu, un izdevēja dalībvalsts apsver nepieciešamību saglabāt brīdinājumu.

4. Brīdinājumus par diskrētu, izmeklēšanas un īpašu pārbaudi dzēš saskaņā ar šādiem noteikumiem:

brīdinājumus par diskrētu, izmeklēšanas un īpašu pārbaudi saskaņā ar 36. pantu dzēš:

(a) beidzoties brīdinājuma termiņam saskaņā ar 51. pantu;

(b) izdevējas dalībvalsts kompetentajai iestādei pieņemot lēmumu par dzēšanu.

5. Brīdinājumus par priekšmetiem izņemšanai vai izmantošanai par pierādījumu dzēš saskaņā ar šādiem noteikumiem:

attiecībā uz brīdinājumiem par priekšmetiem izņemšanai vai izmantošanai par pierādījumu kriminālprocesā saskaņā ar 38. pantu brīdinājumu dzēš:

(a) izņemot attiecīgo priekšmetu vai veicot līdzvērtīgu pasākumu, tiklīdz ir notikusi nepieciešamā turpmākās papildinformācijas apmaiņa starp *SIRENE* birojiem vai tiklīdz attiecīgajam priekšmetam piemēro citu tiesvedības vai administratīvo procedūru;

(b) beidzoties brīdinājuma termiņam; vai

(c) izdevējas dalībvalsts kompetentajai iestādei pieņemot lēmumu par dzēšanu.

6. Brīdinājumus par nezināmām meklētām personām saskaņā ar 40. pantu dzēš saskaņā ar šādiem noteikumiem:

7. a) identificējot personu; vai

8. b) beidzoties brīdinājuma termiņam.

XIV NODAĻA

VISPĀRĪGI DATU APSTRĀDES NOTEIKUMI

53. pants
SIS datu apstrāde

1. Dalībvalstis var apstrādāt 20. pantā minētos datus tikai nolūkos, kas noteikti katrai brīdinājumu kategorijai, kā minēts 26., 32., 34., 36., 38. un 40. pantā.

2. Datus var kopēt vienīgi tehniskos nolūkos, ja šāda kopēšana ir vajadzīga, lai 43. pantā minētās iestādes varētu veikt tiešu meklēšanu šajos datos. Uz šādām kopijām attiecas šī regula. Dalībvalsts nekopē brīdinājuma datus vai papildus datus, ko ievadījusi cita dalībvalsts, no tās N.SIS vai no CS-SIS uz citām valsts datu datnēm.

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

4. 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.

5. Piekļuvi šādiem datiem atļauj vienīgi saskaņā ar 43. pantā minēto attiecīgo valstu iestāžu kompetenci un vienīgi pienācīgi pilnvarotam personālam.

6. Attiecībā uz šīs regulas 26., 32., 34., 36., 38. un 40. pantā paredzētajiem brīdinājumiem ikvienai šajos brīdinājumos ietvertās informācijas apstrādei citiem mērķiem nekā tiem, kādēļ tā ievadīta SIS, jābūt saistītai ar konkrētu gadījumu un pamatotai ar vajadzību novērst tūlītējus nopietnus draudus sabiedriskai kārtībai un drošībai, ar svarīgiem valsts drošības apsvērumiem vai ar vajadzību novērst smagu noziegumu. Šādā nolūkā saņem brīdinājuma izdevējas dalībvalsts iepriekšēju atļauju.

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

8. Katra dalībvalsts nosūta Aģentūrai to savu kompetento iestāžu sarakstu, kuras saskaņā ar šo regulu ir pilnvarotas tieši veikt meklēšanu SIS ievadītajos datos, kā arī jebkuras izmaiņas šajā sarakstā. Minētajā sarakstā attiecībā uz katru iestādi norāda, kuros datos un kādos nolūkos tās drīkst veikt meklēšanu. Aģentūra nodrošina saraksta gadskārtēju publicēšanu *Eiropas Savienības Oficiālajā Vēstnesī*.

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

54. pants
SIS dati un valsts datnes

1. Šīs regulas 53. panta 2. punkts neskar dalībvalsts tiesības savās datnēs glabāt SIS datus, saistībā ar kuriem tās teritorijā ir veiktas darbības. Tādus datus valsts datnēs saglabā ne ilgāk kā trīs gadus, izņemot gadījumus, kad attiecīgās valsts īpašos tiesību aktos ir paredzēts ilgāks saglabāšanas periods.

2. Šīs regulas 53. panta 2. punkts neskar dalībvalsts tiesības savās datnēs saglabāt SIS datus par konkrētu brīdinājumu, ko šī dalībvalsts ir izdevusi SIS.

55. pants
Informācija brīdinājuma neizpildes gadījumā

Ja pieprasīto darbību nevar veikt, brīdinājuma saņēmēja dalībvalsts nekavējoties informē brīdinājuma izdevēju dalībvalsti.

56. pants
SIS apstrādāto datu kvalitāte

1. Brīdinājuma izdevēja dalībvalsts ir atbildīga par to, lai dati būtu precīzi, atjaunināti un likumīgi ievadīti SIS.

2. Vienīgi brīdinājuma izdevēja dalībvalsts ir tiesīga grozīt, papildināt, labot, atjaunināt vai dzēst savus ievadītos datus.

3. Ja dalībvalstij, kura nav brīdinājuma izdevēja dalībvalsts, ir pierādījumi, 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 izdevēju dalībvalsti. Izdevēja dalībvalsts pārbauda šo informāciju un vajadzības gadījumā attiecīgo ierakstu nekavējoties labo vai dzēš.

4. Ja dalībvalstis nespēj vienoties divu mēnešu laikā no brīža, kad pirmoreiz atklājās pierādījumi, kā aprakstīts 3. punktā, tad dalībvalsts, kura nav izdevusi brīdinājumu, jautājumu nodod attiecīgajām valsts uzraudzības iestādēm lēmuma pieņemšanai.

5. Dalībvalstis apmainās ar papildinformāciju, ja persona sūdzas, ka viņš vai viņa nav tā persona, par kuru izdots brīdinājums. Ja pārbaudē konstatē, ka tās tiešām ir divas dažādas personas, sūdzības iesniedzēju informē par 59. pantā minētajiem pasākumiem.

6. Ja par kādu personu SIS jau ir ievadīts brīdinājums, tad dalībvalsts, kura datubāzē ievada jaunu brīdinājumu, par brīdinājuma ievadīšanu vienojas ar dalībvalsti, kas ievadījusi pirmo brīdinājumu. Vienošanos panāk, apmainoties ar papildinformāciju.

57. pants
Drošības starpgadījumi

1. Jebkurš notikums, kurš ietekmē vai var ietekmēt SIS drošību un var kaitēt SIS datiem vai izraisīt to zudumu, ir uzskatāms par drošības starpgadījumu, jo īpaši, ja ir radusies piekļuve datiem vai ir apdraudēta vai var tikt apdraudēta datu pieejamība, integritāte un konfidencialitāte.

2. Drošības starpgadījumus pārvalda, lai nodrošinātu ātru, efektīvu un pareizu reakciju.

3. Dalībvalstis paziņo Komisijai, Aģentūrai un Eiropas Datu aizsardzības uzraudzītājam par drošības starpgadījumiem. Aģentūra paziņo Komisijai un Eiropas Datu aizsardzības uzraudzītājam par drošības starpgadījumiem.

4. Informāciju par drošības starpgadījumu, kas ietekmē vai var ietekmēt SIS darbību dalībvalstī vai Aģentūrā vai citu dalībvalstu ievadīto vai nosūtīto datu pieejamību,

integritāti un konfidencialitāti, sniedz dalībvalstīm, un par to ziņo saskaņā ar starpgadījumu pārvaldības plānu, ko nodrošina Aģentūra.

58. pants
Personu ar līdzīgām īpašībām atšķiršana

Ja, ievadot jaunu brīdinājumu, konstatē, ka SIS 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) ja dažādu avotu pārbaudē atklājas, ka jaunā brīdinājuma subjekts un persona, kas jau norādīta SIS, patiešām ir viena un tā pati persona, *SIRENE* birojs piemēro 56. panta 6. punktā minēto procedūru vairāku brīdinājumu ievadīšanai. Ja pārbaudē atklājas, ka tās ir divas dažādas personas, *SIRENE* birojs apstiprina lūgumu ievadīt otru brīdinājumu, pievienojot vajadzīgos elementus, lai novērstu nepareizu identifikāciju.

59. 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, izdevēja 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 drīkst ievadīt un turpmāk apstrādāt vienīgi šādus personas datus:

   (a) uzvārds(-i);

   (b) vārds(-i);

   (c) vārds, uzvārds (vārdi, uzvārdi) dzimšanas brīdī;

   (d) iepriekš lietoti vārdi un pseidonīmi, ko var ievadīt atsevišķi;

   (e) īpašas fiziskas pazīmes, kas ir objektīvas un nemainīgas;

   (f) dzimšanas vieta;

   (g) dzimšanas datums,

   (h) dzimums;

   (i) fotogrāfijas un sejas attēli;

   (j) pirkstu nospiedumi;

   (k) valstspiederība(-as);

(l) personu apliecinoša dokumenta kategorija;

(m) personu apliecinoša dokumenta izdošanas valsts;

(n) personu apliecinoša dokumenta numurs;

(o) personu apliecinoša dokumenta izdošanas datums;

(p) cietušā adrese;

(q) cietušā tēva vārds;

(r) cietušā mātes vārds;

4. Tehniskos noteikumus, kas vajadzīgi 3. punktā minēto datu ievadīšanai un turpmākai apstrādei, paredz kā īstenošanas pasākumus, kurus nosaka un izstrādā saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

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

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

60. pants
Brīdinājumu sasaiste

1. Jebkura dalībvalsts var veikt to brīdinājumu sasaisti, kurus tā ievada SIS. 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 periodu.

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, ja ir skaidra operatīva vajadzība.

5. 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.

6. Tehniskos noteikumus par brīdinājumu sasaisti nosaka un izstrādā saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

61. pants
Papildinformācijas nolūks un saglabāšanas periods

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 dzēš ne vēlāk kā vienu gadu pēc tam, kad no SIS 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. Termiņu, cik ilgi atļauts datnēs glabāt šādus datus, reglamentē attiecīgās valsts tiesību akti.

62. pants
Personas datu nodošana trešām personām

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

63. pants
Datu apmaiņa ar Interpolu attiecībā uz zagtām, nelikumīgi piesavinātām, pazaudētām vai spēkā neesošām pasēm

1. Atkāpjoties no 62. panta, ar Interpola locekļiem var apmainīties ar informāciju par SIS ievadīto zagto, nelikumīgi piesavināto, pazaudēto vai spēkā neesošo pasu numuriem, izdevējvalstīm un dokumentu veidiem, izveidojot sasaisti starp SIS un Interpola datubāzi attiecībā uz nozagtiem vai pazudušiem ceļošanas dokumentiem, ja starp Interpolu un Eiropas Savienību noslēdz attiecīgu nolīgumu. Nolīgumā paredz, ka dalībvalsts ievadītu datu pārsūtīšanai ir vajadzīga šīs dalībvalsts piekrišana.

2. Šā panta 1. punktā minētajā nolīgumā paredz, ka kopīgi izmantojamiem datiem Interpola locekļi var piekļūt vienīgi no tām valstīm, kuras nodrošina personas datu pienācīgu aizsardzības līmeni. Pirms šā nolīguma noslēgšanas Padome lūdz Komisijas atzinumu par personas datu aizsardzības līmeņa un pamattiesību un brīvību ievērošanas pietiekamību attiecībā uz personas datu automātisku apstrādi, ko veic Interpols un valstis, kuras norīkojušas locekļus uz Interpolu.

3. Šā panta 1. punktā minētajā nolīgumā var paredzēt arī dalībvalstu piekļuvi, izmantojot SIS, datiem Interpola datubāzē attiecībā uz nozagtiem vai pazudušiem ceļošanas dokumentiem saskaņā ar attiecīgiem šīs regulas noteikumiem, ar ko reglamentē SIS ievadītus brīdinājumus par zagtām, nelikumīgi piesavinātām, pazaudētām vai spēkā neesošām pasēm.

XV NODAĻA

DATU AIZSARDZĪBA

64. pants
Piemērojamie tiesību akti

1. Regulu (EK) Nr. 45/2001 piemēro personas datu apstrādei, ko veic Aģentūra saskaņā ar šo regulu.

2. Personas datu apstrādei piemēro Regulu (ES) Nr. 2016/679 ar noteikumu, ka nav piemērojami valsts tiesību akti, ar kuriem transponē Direktīvu (ES) 2016/680.

3. Attiecībā uz datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināLsodus, tostarp, lai aizsargātu pret sabiedriskās drošības apdraudējumiem un

novērstu tos, piemēro valsts tiesību aktus, ar kuriem transponē Direktīvu (ES) 2016/680.

65. pants

Tiesības uz piekļuvi, neprecīzu datu labošanu un nelikumīgi glabātu datu dzēšanu

1. Datu subjektu tiesības piekļūt datiem, kas attiecas uz šīm personām un kas ir ievadīti SIS, un tiesības uz šo datu labošanu vai dzēšanu īsteno saskaņā ar tās dalībvalsts tiesību aktiem, kurā attiecīgās personas atsaucas uz minētajām tiesībām.

2. Ja attiecīgas valsts tiesību akti to paredz, valsts uzraudzības iestāde pieņem lēmumu par to, vai un kādā veidā informācija ir jādara zināma.

3. Dalībvalsts, kas nav brīdinājuma izdevēja dalībvalsts, informāciju par šādiem datiem var darīt zināmu vienīgi tad, ja tā iepriekš dod iespēju brīdinājuma izdevējai dalībvalstij darīt zināmu savu nostāju. To dara, apmainoties ar papildinformāciju.

4. Saskaņā ar valsts tiesību aktiem dalībvalsts pieņem lēmumu pilnībā vai daļēji nesniegt informāciju datu subjektam tādā apjomā un tik ilgi, cik ilgi šāds daļējs vai pilnīgs ierobežojums ir nepieciešams un samērīgs demokrātiskā sabiedrībā, pienācīgi ņemot vērā pamattiesības un attiecīgo fizisko personu leģitīmās intereses, lai:

   (a) novērstu, ka tiek traucētas oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras;

   (b) netraucētu noziedzīgu nodarījumu novēršanu, atklāšanu un izmeklēšanu vai saukšanu pie krimināltatbildības par tiem, vai kriminālsodu izpildi;

   (c) aizsargātu sabiedrisko drošību;

   (d) aizsargātu valsts drošību;

   (e) aizsargātu citu personu tiesības un brīvības.

5. Ikvienai personai ir tiesības uz datu labošanu, ja datos par viņu ir faktu kļūda, vai uz datu dzēšanu, ja dati nav glabāti likumīgi.

6. Attiecīgo personu informē, tiklīdz iespējams un jebkurā gadījumā ne vēlāk kā 60 dienas pēc datuma, kad šī persona iesniedz piekļuves pieteikumu, vai agrāk, ja to paredz valsts tiesību akti.

7. Attiecīgo personu informē par papildpasākumiem, kas veikti, īstenojot viņas tiesības uz labojumiem un dzēšanu, tiklīdz iespējams un jebkurā gadījumā ne vēlāk kā trīs mēnešus pēc datuma, kad šī persona iesniedz labojuma vai dzēšanas pieteikumu, vai agrāk, ja to paredz valsts tiesību akti.

66. pants

Tiesiskās aizsardzības līdzekļi

1. Ikviena persona var vērsties tiesā vai saskaņā ar attiecīgās dalībvalsts tiesību aktiem kompetentā iestādē, lai saistībā ar brīdinājumu, kas attiecas uz konkrēto personu, iegūtu piekļuvi informācijai, labotu, dzēstu vai iegūtu informāciju vai saņemtu kompensāciju.

2. Neskarot 70. pantu, dalībvalstis savstarpēji apņemas īstenot galīgos lēmumus, ko pieņem tiesa vai šā panta 1. punktā minētās iestādes.

3. Lai gūtu pilnīgu pārskatu par tiesību aizsardzības līdzekļu darbību, valsts iestādes izstrādā standarta statistikas sistēmas, lai katru gadu ziņotu par:

(a) piekļuves pieprasījumu skaitu, kas iesniegti datu pārzinim, un to gadījumu skaitu, kad tika piešķirta piekļuve datiem;

(b) piekļuves pieprasījumu skaitu, kas iesniegti valsts uzraudzības iestādei, un to gadījumu skaitu, kad tika piešķirta piekļuve datiem;

(c) pieprasījumu skaitu, kas iesniegti datu pārzinim par neprecīzu datu labošanu un nelikumīgi glabātu datu dzēšanu, un to gadījumu skaitu, kad dati ir laboti vai dzēsti;

(d) pieprasījumu skaitu, kas iesniegti valsts uzraudzības iestādei par neprecīzu datu labošanu un nelikumīgi glabātu datu dzēšanu;

(e) to lietu skaitu, kuras izskata tiesā;

(f) to gadījumu skaitu, kad tiesa ir lēmusi par labu prasītājam jebkurā lietas jautājumā;

(g) visiem novērojumiem saistībā ar citu dalībvalstu tiesu vai iestāžu pieņemto galīgo lēmumu attiecībā uz brīdinājumiem, kurus izveidojusi brīdinājuma izdevēja dalībvalsts, savstarpējas atzīšanas gadījumiem.

Valsts uzraudzības iestāžu ziņojumus nosūta sadarbības mehānismam, kas minēts 69. pantā.

67. pants
N.SIS uzraudzība

1. Katra dalībvalsts nodrošina, ka uzraudzības iestāde vai iestādes, kas norīkotas katrā dalībvalstī un kam piešķirtas Direktīvas (ES) 2016/680 VI nodaļā vai Regulas (ES) 2016/679 VI nodaļā minētās pilnvaras, neatkarīgi uzrauga SIS personas datu apstrādes likumīgumu attiecīgās valsts teritorijā un to nosūtīšanas no attiecīgās valsts teritorijas, kā arī papildinformācijas apmaiņas un turpmākās apstrādes likumīgumu.

2. Attiecīgās valsts uzraudzības iestāde nodrošina, ka vismaz reizi četros gados tiek veikta attiecīgās valsts N.SIS veikto datu apstrādes operāciju revīzija saskaņā ar starptautiskiem revīzijas standartiem. Revīziju veic valsts uzraudzības iestāde(-s), vai valsts uzraudzības iestāde(-s) tieši pasūta revīziju no neatkarīga datu aizsardzības revidenta. Valsts uzraudzības iestāde vienmēr saglabā pār neatkarīgo revidentu un uzņemas atbildību.

3. Dalībvalstis nodrošina, ka valsts uzraudzības iestādei ir pietiekami resursi, lai pildītu ar šo regulu noteiktos uzdevumus.

68. pants
Aģentūras uzraudzība

1. Eiropas Datu aizsardzības uzraudzītājs nodrošina, ka Aģentūras veiktā personu datu apstrāde notiek saskaņā ar šo regulu. Attiecīgi 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 notiek Aģentūras veikto personas datu apstrādes darbību revīzija saskaņā ar starptautiskiem revīzijas standartiem. Ziņojumu par minēto revīziju nosūta Eiropas Parlamentam,

Padomei, Aģentūrai, Komisijai un valsts uzraudzības iestādēm. Pirms ziņojuma pieņemšanas Aģentūrai dod iespēju izteikt savus apsvērumus.

69. pants

Valstu uzraudzības iestāžu un Eiropas Datu aizsardzības uzraudzītāja sadarbība

1. Valstu uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs, rīkojoties saskaņā ar savām attiecīgajām pilnvarām, aktīvi sadarbojas savu pienākumu ietvarā un nodrošina SIS koordinētu uzraudzību.

2. Rīkojoties katrs saskaņā ar savām attiecīgajām pilnvarām, tie apmainās ar svarīgu informāciju, palīdz cits citam veikt revīzijas un pārbaudes, izskata šīs regulas un citu piemērojamo Savienības tiesību aktu interpretācijas vai piemērošanas grūtības, analizē problēmas, kas atklājas neatkarīgas uzraudzības gaitā vai datu subjektu tiesību īstenošanas rezultātā, sagatavo saskaņotus priekšlikumus, meklējot kopīgus risinājumus visām problēmām, un pēc vajadzības palīdz apzināt datu aizsardzības tiesības.

3. Šā panta 2. punktā paredzētajos nolūkos valsts uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs tiekas vismaz divreiz gadā Regulā (ES) Nr. 2016/679 paredzētās Eiropas Datu aizsardzības kolēģijas ietvaros. Šo sanāksmju izmaksas sedz un rīkošanu uzņemas kolēģija, kas izveidota ar Regulu (ES) Nr. 2016/679. Reglamentu pieņem pirmajā sanāksmē. Ja nepieciešams, kopīgi izstrādā turpmākas darba metodes.

4. Kopīgu darbības pārskatu par koordinēto uzraudzību kolēģija, kas izveidota ar Regulu (ES) Nr. 2016/679, reizi divos gados nosūta Eiropas Parlamentam, Padomei un Komisijai.

XVI NODAĻA

ATBILDĪBA

70. pants

Atbildība

1. Katra dalībvalsts ir atbildīga par jebkuru kaitējumu personai, kas radies, izmantojot N. SIS. Tas attiecas arī uz kaitējumu, ko radījusi 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 pieprasa atlīdzināt izmaksāto kompensāciju, nav pārkāpusi šo regulu, izmantojot datus.

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

XVII NODAĻA

NOBEIGUMA NOTEIKUMI

71. pants
Uzraudzība un statistika

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

2. Tehniskās uzturēšanas, ziņošanas un statistikas nolūkos aģentūrai ir piekļuve vajadzīgajai informācijai, kas attiecas uz apstrādes darbībām, kuras veic centrālajā SIS.

3. Aģentūra izstrādā dienas, mēneša un gada statistiku, norādot ierakstu skaitu pa brīdinājumu kategorijām, saņemto trāpījumu skaitu pa brīdinājumu kategorijām un to, cik reizes notika meklēšana SIS, un to, cik reizes piekļūts SIS, lai ievadītu, atjauninātu vai dzēstu brīdinājumu kopumā un par katru dalībvalsti. Minētajā statistikā neietver personas datus. Gada statistikas ziņojumu publicē. Aģentūra sniedz gada statistikas datus kopumā un par katru dalībvalsti par to, kā izmantota funkcionalitāte par brīdinājuma, kas izdots saskaņā ar šīs regulas 26. pantu, padarīšanu meklēšanai nepieejamu, tostarp par visiem 48 stundu termiņa pagarinājumiem.

4. Dalībvalstis, kā arī Eiropols, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūra sniedz Aģentūrai un Komisijai informāciju, kas nepieciešama, lai izstrādātu 3., 7. un 8. punktā minētos ziņojumus. Šī informācija ietver atsevišķus statistikas datus par to, cik reižu meklēšanu ir veikuši tādi dalībvalstu dienesti vai meklēšana ir veikta tādu dalībvalstu dienestu vārdā, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izsniegšanu, un tādi dalībvalstu dienesti vai tādu dalībvalstu dienestu vārdā, kas ir atbildīgi par reģistrācijas apliecību izsniegšanu vai satiksmes pārvaldības nodrošināšanu attiecībā uz laivām, tostarp laivu dzinējiem, gaisa kuģiem un konteineriem. Statistikā uzrāda arī trāpījumu skaitu pa brīdinājumu kategorijām.

5. Aģentūra iesniedz dalībvalstīm, Komisijai, Eiropolam, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūrai visus sagatavotos statistikas ziņojumus. Lai uzraudzītu to, kā tiek īstenoti Savienības tiesību akti, Komisijai ir jābūt iespējai pieprasīt, lai Aģentūra sniedz papildu īpašus statistikas ziņojumus vai nu regulāri vai *ad hoc* par SIS un *SIRENE* komunikācijas darbību vai izmantojumu.

6. Šā panta 3., 4. un 5. punkta un 15. panta 5. punkta nolūkos Aģentūra izveido, īsteno un mitina centrālo repozitoriju savās tehniskajās tīmekļa vietnēs, kurš satur datus, kas minēti šā panta 3. punktā un 15. panta 5. punktā, kas neļauj identificēt personas un ļauj Komisijai un 5. punktā minētajām aģentūrām iegūt minētos ziņojumus un statistiku. Aģentūra dalībvalstīm, Komisijai, Eiropolam, *Eurojust* un Eiropas Robežu un krasta apsardzes aģentūrai piešķir piekļuvi centrālajam repozitorijam ar aizsargātu piekļuvi, izmantojot komunikācijas infrastruktūru, kas kontrolē piekļuvi un konkrētus lietotāju profilus vienīgi ziņojumu un statistikas nolūkā.

   Sīki izstrādātus noteikumus par centrālā repozitorija darbību un datu aizsardzību un drošības noteikumus, ko piemēro repozitorijam, pieņem kā īstenošanas pasākumus saskaņā ar 72. panta 2. punktā minēto pārbaudes procedūru.

7. Divus gadus pēc SIS darbības sākšanas un pēc tam reizi divos gados Aģentūra iesniedz Eiropas Parlamentam un Padomei ziņojumu par centrālās SIS un komunikācijas infrastruktūras tehnisko darbību, tostarp to drošību, un papildinformācijas divpusēju un daudzpusēju apmaiņu starp dalībvalstīm.

8. Trīs gadus pēc SIS darbības sākšanas un pēc tam reizi četros gados Komisija sagatavo vispārēju izvērtējumu par centrālo SIS un papildinformācijas divpusēju un daudzpusēju apmaiņu starp 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, centrālās SIS drošību un turpmāko darbību iespējamo ietekmi. Komisija izvērtējumu nosūta Eiropas Parlamentam un Padomei.

72. pants
Komiteju procedūra

1. Komisijai palīdz komiteja Regulas (ES) Nr. 182/2011 nozīmē.

2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.

73. pants
Grozījumi Regulā (ES) 515/2014

Regulu (ES) Nr. 515/2014[76] groza šādi:

regulas 6. pantu papildina ar šādu 6. punktu:

"6. Izstrādes posmā dalībvalstis saņem papildu finansējumu EUR 36,8 miljonu apmērā, ko sadala, izmantojot vienreizēju maksājumu, kuru pieskaita to pamata piešķīrumam, un pilnībā velta šo finansējumu SIS valsts sistēmai, lai nodrošinātu tās ātru un efektīvu uzlabošanu atbilstīgi centrālās SIS īstenošanai, kā noteikts Regulā (ES) 2018/...* un Regulā (ES) 2018/...**.

**Regulā par Šengenas informācijas sistēmas (SIS) izveidi, darbību un izmantošanu policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās un Regulā (OV...*

***Regulā (ES) 2018/... par Šengenas informācijas sistēmas (SIS) izveidi, darbību un izmantošanu robežpārbaužu jomā un Regulā (OV ...)".*

74. pants
Atcelšana

No šīs regulas piemērošanas dienas atceļ šādus tiesību aktus:

Eiropas Parlamenta un Padomes Regula (EK) Nr. 1986/2006 (2006. gada 20. decembris) par dalībvalstu dienestu, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izsniegšanu, piekļuvi otrās paaudzes Šengenas Informācijas sistēmai (SIS II);

[76] Eiropas Parlamenta un Padomes Regula (ES) Nr. 515/2014 (2014. gada 16. aprīlis) , ar ko kā daļu no Iekšējās drošības fonda izveido finansiāla atbalsta instrumentu ārējām robežām un vīzām (OV L 150, 20.5.2014., 143. lpp.).

Padomes Lēmums 533/2007/TI (2007. gada 12. jūlijā) par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) izveidi, darbību un izmantošanu;

Komisijas Lēmums 2010/261/ES (2010. gada 4. maijs) par drošības plānu Centrālajai SIS II un sakaru infrastruktūrai[77].

75. pants
Stāšanās spēkā un piemērojamība

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

2. To piemēro no dienas, ko nosaka Komisija pēc tam, kad:

   a) ir pieņemti vajadzīgie īstenošanas pasākumi;

   b) dalībvalstis ir paziņojušas Komisijai, ka tās veikušas tehniskos un juridiskos pasākumus, kas vajadzīgi SIS datu apstrādei un papildinformācijas apmaiņai saskaņā ar šo regulu;

   c) Aģentūra ir informējusi Komisiju par to, ka ir pabeigtas visas testēšanas darbības attiecībā uz CS-SIS un mijiedarbību starp CS-SIS un N.SIS.

3. Šī regula uzliek saistības kopumā un ir tieši piemērojama dalībvalstīs saskaņā ar Līgumu par Eiropas Savienības darbību.

Briselē,

Eiropas Parlamenta vārdā — priekšsēdētājs	*Padomes vārdā — priekšsēdētājs*

[77] Komisijas Lēmums 2010/261/ES (2010. gada 4. maijs) par drošības plānu Centrālajai SIS II un sakaru infrastruktūrai (OV L 112, 5.5.2010., 31. lpp.).

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

1.2. Attiecīgās politikas jomas *ABM/ABB* struktūrā

1.3. Priekšlikuma/iniciatīvas būtība

1.4. Mērķis(-i)

1.5. Priekšlikuma/iniciatīvas pamatojums

1.6. Ilgums un finansiālā ietekme

1.7. Paredzētie pārvaldības veidi

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

2.2. Pārvaldības un kontroles sistēma

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Kopsavilkums par paredzamo ietekmi uz izdevumiem

3.2.2. Paredzamā ietekme uz darbības apropriācijām

3.2.3. Paredzamā ietekme uz administratīvajām apropriācijām

3.2.4. Saderība ar kārtējo daudzgadu finanšu shēmu

3.2.5. Trešo personu iemaksas

3.3. Paredzamā ietekme uz ieņēmumiem

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA par Šengenas informācijas sistēmas (SIS) izveidi, darbību un izmantošanu policijas sadarbībā un tiesu iestāžu sadarbībā krimināllietās, ar ko groza Regulu (ES) Nr. 515/2014 un atceļ Regulu (EK) Nr. 1986/2006, Padomes Lēmumu 2007/533/TI un Komisijas Lēmumu 2010/261/ES.

1.2. Attiecīgās politikas jomas *ABM/ABB* struktūrā[78]

Politikas joma: Migrācija un iekšlietas (18. sadaļa)

1.3. Priekšlikuma/iniciatīvas būtība

☐Priekšlikums/iniciatīva attiecas uz **jaunu darbību**

☐Priekšlikums/iniciatīva attiecas uz **jaunu darbību, pamatojoties uz izmēģinājuma projektu/sagatavošanas darbību**[79]

☑Priekšlikums/iniciatīva attiecas uz **esošas darbības pagarināšanu**

☐Priekšlikums/iniciatīva attiecas uz **darbību, kas pārveidota jaunā darbībā**

1.4. Mērķis(-i)

1.4.1. Komisijas daudzgadu stratēģiskie mērķi, kurus plānots sasniegt ar priekšlikumu/iniciatīvu

Mērķis — "Novērst organizēto noziedzību"

Mērķis — "Spēcīga ES reakcija terorisma apkarošanai un radikalizācijas novēršanai"

Vajadzība pārskatīt SIS juridisko pamatu, lai risinātu jaunās drošības un migrācijas problēmu, kā Komisija to jau vairākkārt ir uzsvērusi. Piemēram, "Eiropas Drošības programmā"[80] Komisija paziņoja par savu nodomu 2015. — 2016. gadā novērtēt SIS un noteikt, vai pastāv jaunas operatīvās vajadzības, kas prasa izmaiņas tiesību aktos. Turklāt drošības programmā uzsvērts, ka SIS ir policijas informācijas apmaiņas galvenais rīks un tā būtu vēl vairāk jāstiprina. Nesen paziņojumā "Spēcīgākas un viedākas robežu un drošības informācijas sistēmas"[81] Komisija norādīja, ka, pamatojoties uz vispārēju novērtējuma ziņojumu, tiks izvērtētas sistēmas papildu funkcijas nolūkā iesniegt priekšlikumus, ar ko pārskatītu SIS juridisko pamatu. Visbeidzot, 2016. gada 20. aprīļa paziņojumā "Eiropas Drošības programmas īstenošana cīņā pret terorismu un virzībā uz efektīvu un patiesu drošības savienību"[82] Komisija ierosināja vairākas izmaiņas SIS, lai uzlabotu tās pievienoto vērtību tiesībaizsardzības nolūkos.

Komisijas veiktais vispārējais novērtējums apstiprināja, ka SIS darbojas ar panākumiem. Tomēr, neraugoties uz daudzajiem panākumiem, novērtējumā arī

78 *ABM*: budžeta līdzekļu vadība pa darbības jomām; *ABB:* budžeta līdzekļu sadale pa darbības jomām.

79 Kā paredzēts Finanšu regulas 54. panta 2. punkta attiecīgi a) un b) apakšpunktā.

80 COM(2015) 185 *final*.

81 COM(2016) 205 *final*.

82 COM(2016) 230 *final*.

sniegti vairāki ieteikumi ar mērķi uzlabot tehnisko un darbības efektivitāti un sistēmas iedarbīgumu.

Ņemot vērā vispārējā novērtējuma ziņojuma ieteikumus, un pilnībā atbilstīgi Komisijas mērķiem, kas norādīti iepriekš minētajos paziņojumos un Migrācijas un iekšlietu ĢD Stratēģiskajā plānā 2016. – 2020. gadam[83], šā priekšlikuma mērķis ir īstenot:

- Komisijas apņemšanos uzlabot SIS pievienoto vērtību tiesībaizsardzības nolūkos, lai reaģētu uz jauniem apdraudējumiem;
- ieteikumus tehniskiem un procesuāliem grozījumiem, kas izriet no visaptverošas SIS izvērtēšanas;
- galalietotāju lūgumus par tehniskiem uzlabojumiem;
- starpposma secinājumus, ko par datu kvalitāti pieņēmusi Augsta līmeņa ekspertu grupa jautājumos par informācijas sistēmu sadarbspēju.

1.4.2. Konkrētie mērķi un attiecīgās ABM/ABB darbības

Konkrētais mērķis Nr.

Migrācijas un iekšlietu ĢD vadības plāns 2017. gadam

Konkrētais mērķis Nr. 2.1. – "Spēcīga ES reakcija terorisma apkarošanai un radikalizācijas novēršanai";

Konkrētais Nr. 2.2. – Novērst smagu un organizētu pārrobežu noziedzību.

Attiecīgās ABM/ABB darbības

18 02. nodaļa. Iekšējā drošība

[83] Ares(2016)2231546–12/05/2016.

1.4.3. Paredzamais(-ie) rezultāts(-i) un ietekme

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz finansējuma saņēmējiem/mērķgrupām.

Ierosināto juridisko un tehnisko SIS izmaiņu galvenais mērķis ir padarīt sistēmas darbību efektīvāku. SIS vispārējā novērtējuma, kuru veica Iekšlietu ĢD 2015. – 2016. gadā, rezultātā tika ieteikti tehniski sistēmas uzlabojumi un valsts procedūru saskaņošana sadarbībai tiesībaizsardzības jomā.

Jaunais priekšlikums ievieš pasākumus, lai risinātu galalietotāju darbības un tehniskās vajadzības. Jo īpaši jauni datu lauki jau esošajos brīdinājumos, ļaus policistiem iegūt visu vajadzīgo informāciju, lai efektīvi pildītu savus uzdevumus. Turklāt priekšlikumā īpaši uzsvērts, cik svarīga ir nepārtraukta SIS pieejamība, jo darbības pārtraukumi var būtiski ietekmēt tiesībaizsardzības jomā strādājošo darbu. Turklāt šis priekšlikums paredz tehniskas izmaiņas, lai padarītu sistēmu efektīvāku un vienkāršāku.

Tiklīdz priekšlikumi būs pieņemti un īstenoti, tie uzlabos arī darbības nepārtrauktību – dalībvalstu pienākums būs izveidot pilnīgu vai daļēju valsts eksemplāru un rezerves sistēmu. Tādējādi sistēma vienmēr būs pilnībā funkcionāla, un darbinieki uz vietas varēs to izmantot.

Priekšlikums īpašos un ierobežotos gadījumos paredz jaunus biometriskos identifikatorus – plaukstu nospiedumi, sejas attēli un DNS profilus. Tas – kopā ar 32. un 33. pantā (brīdinājumi par pazudušām personām) paredzētajām izmaiņām, kas ļaus ievadīt preventīvus brīdinājumus un iedalīt pazudušo personu gadījumus kategorijās, – ļaus, pirmkārt, ievērojami pastiprināt nepavadītu nepilngadīgo aizsardzību un, otrkārt, identificēt viņus, pamatojoties uz viņu vai viņu vecāku un/vai brāļu un māsu DNS profiliem (ar piekrišanu).

Dalībvalstu iestādes arī varēs izdot brīdinājumus attiecībā uz nezināmām personām, kuras meklē saistībā ar noziegumu, pamatojoties tikai uz latentiem vai nozieguma izdarīšanas vietā atrastiem pirkstu vai plaukstu nospiedumiem. Tas nav iespējams saskaņā ar pašreizējo tiesisko un tehnisko regulējumu, un tādējādi tas ir nozīmīgs uzlabojums.

1.4.4. Rezultātu un ietekmes rādītāji

Norādīt priekšlikuma/iniciatīvas īstenošanas uzraudzībā izmantojamos rādītājus.

Sistēmas modernizācijas laikā:

Pēc priekšlikuma projekta apstiprināšanas un tehnisko specifikāciju pieņemšanas SIS tiks modernizēta, lai labāk saskaņotu valstu procedūras sistēmas izmantošanai, paplašinātu sistēmas darbības jomu, ieviešot jaunus brīdinājumu kategoriju elementus, un ieviestu tehniskas izmaiņas, ar kurām tiks uzlabota drošība un kas palīdzēs mazināt administratīvo slogu. *Eu-LISA* koordinēs sistēmas modernizācijas projekta vadību. *Eu-LISA* izveidos projekta vadības struktūru un sniegs sīki izstrādātu grafiku ar starpposma mērķiem ierosināto grozījumu īstenošanai, kas ļaus Komisijai cieši pārraudzīt priekšlikuma īstenošanu.

Konkrētais mērķis – SIS modernizēto funkciju darbības uzsākšana 2020. gadā

Rādītājs – sekmīgi pabeigta vispusīga atjauninātās sistēmas pirmspalaišanas testēšana.

Kad sistēma būs sākusi darboties

Kad sistēma būs sākusi darboties, *eu-LISA* nodrošinās, ka tiek ieviestas procedūras, ar kuru palīdzību uzrauga Šengenas Informācijas sistēmas darbības atbilstību mērķiem, darbības efektivitāti, izmaksu lietderīgumu, drošību un pakalpojuma kvalitāti. Divus gadus pēc SIS darbības sākšanas un pēc tam reizi divos gados *eu-LISA* ir pienākums iesniegt Eiropas Parlamentam un Padomei ziņojumu par centrālās SIS un komunikācijas infrastruktūras tehnisko darbību, tostarp to drošību, un papildinformācijas divpusēju un daudzpusēju apmaiņu starp dalībvalstīm. Turklāt *eu-LISA* izstrādās dienas, mēneša un gada statistiku, norādot ierakstu skaitu pa brīdinājumu kategorijām, saņemto trāpījumu skaitu pa brīdinājumu kategorijām un to, cik reizes notika meklēšana SIS, un to, cik reizes piekļūts SIS, lai ievadītu, atjauninātu vai dzēstu brīdinājumu kopumā un par katru dalībvalsti. Turklāt aģentūra sniegs gada statistikas datus kopumā un par katru dalībvalsti par to, kā izmantota funkcionalitāte par brīdinājuma, kas izdots saskaņā ar šīs regulas 26. pantu, padarīšanu meklēšanai nepieejamu, tostarp par visiem 48 stundu termiņa pagarinājumiem.

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

Konkrētais mērķis Nr.1. – "Novērst organizēto noziedzību".

Rādītājs — ES informācijas apmaiņas mehānisma izmantošana. To var izmērīt ar trāpījumu skaita pieaugumu SIS. Rādītāji ir statistikas ziņojumi, kurus izdod *eu-LISA* un dalībvalstis. Tie ļaus Komisijai novērtēt, kā tiek izmantotas sistēmas jaunās funkcijas.

Konkrētais mērķis Nr. 2. – "Spēcīga ES reakcija terorisma apkarošanai un radikalizācijas novēršanai".

Rādītājs – brīdinājumu un trāpījumu skaita pieaugums, jo īpaši saistībā ar priekšlikuma 36. panta 3. punktu par brīdinājumiem par personām un priekšmetiem diskrētām pārbaudēm, izmeklēšanas pārbaudēm vai īpašām pārbaudēm.

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņa vai ilgtermiņa vajadzības

1. Uzlabot augsta drošības līmeņa uzturēšanu brīvības, drošības un tiesiskuma telpā ES;

2. Labāk saskaņot valstu procedūras SIS izmantošanai;

3. Paplašināt to institucionālo lietotāju sarakstu, kuriem ir piekļuve SIS datiem, piešķirot Eiropolam un jaunajai Eiropas Robežu un krasta apsardzei pilnīgu piekļuvi sistēmai.

4. Ieviest jaunus elementus SIS brīdinājumos un jaunas funkcijas, lai paplašinātu sistēmas darbības jomu, ļaujot tai risināt problēmas saistībā ar pašreizējo drošības vidi, stiprināt sadarbību starp dalībvalstu tiesībaizsardzības un drošības iestādēm un samazināt administratīvo slogu;

5. Risināt jautājumu par SIS pilnīgu izmantošanu no viena gala līdz otram, aptverot ne tikai centrālo sistēmu un valstu sistēmas, bet arī nodrošinot, ka galalietotāji saņem visus vajadzīgos datus, lai veiktu savus uzdevumus;

6. Pastiprināt darbības nepārtrauktību un nodrošināt SIS nepārtrauktu darbību centrālā un valstu līmenī;

7. Uzlabot cīņu pret starptautisko noziedzību, terorismu un kibernoziedzību, kas ir saistītas jomas ar ievērojamu pārrobežu dimensiju.

1.5.2. ES iesaistīšanās pievienotā vērtība

SIS ir galvenā drošības datubāze Eiropā. Tā kā nepastāv iekšējo robežu kontrole, efektīvai noziedzības un terorisma apkarošanai ir visas Eiropas dimensija. Šā priekšlikuma mērķi attiecas uz tehniskiem uzlabojumiem, lai palielinātu sistēmas efektivitāti un iedarbīgumu, un saskaņotu tās lietošanu visās iesaistītajās dalībvalstīs. Šo mērķu starptautisks raksturs, kā arī problēmas, kuras jārisina, lai nodrošinātu efektīvu informācijas apmaiņu, lai apkarotu aizvien dažādākos draudus, nozīmē, ka ES atrodas visizdevīgākajā pozīcijā, lai ierosinātu šo problēmu risinājumus. Mērķus uzlabot SIS efektivitāti un saskaņot izmantošanu, proti, palielināt informācijas apmaiņas apjomu, kvalitāti un ātrumu, izmantojot centralizētu informācijas apmaiņas liela mēroga informācijas sistēmu, ko pārvalda regulatīva aģentūra (*eu-LISA*) nevar sasniegt dalībvalstis vienas pašas un ir nepieciešama iejaukšanās ES līmenī. Ja šīs problēmas netiks risinātas, SIS turpinās darboties saskaņā ar noteikumiem, ko piemēro pašlaik, tādējādi tiks palaista garām iespēja palielināt efektivitāti un ES pievienoto vērtību, kas konstatēta SIS novērtēšanā, un izmantošanu dalībvalstīs.

Tikai 2015. gadā vien dalībvalstu kompetentās iestādes piekļuva sistēmai gandrīz 2,9 miljardus reižu, kas skaidri parāda sistēmas nozīmīgo ieguldījumu tiesībaizsardzības iestāžu sadarbībā Šengenas zonā. Šī augsta līmeņa informācijas apmaiņa starp dalībvalstīm nebūtu panākta, izmantojot decentralizētus valstu risinājumus, un dalībvalstu līmenī nebūtu iespējams sasniegt šos rezultātus. Turklāt SIS ir izrādījusies visefektīvākais informācijas apmaiņas līdzeklis terorisma apkarošanas nolūkos, un tā nodrošina ES pievienoto vērtību, jo ļauj valsts drošības dienestiem ātri, konfidenciāli un efektīvi sadarboties. Ar jaunajiem priekšlikumiem tiks vēl vairāk atvieglota informācijas apmaiņa un sadarbība starp ES dalībvalstīm. Turklāt to kompetences ietvaros, Eiropolam un Eiropas Robežu un krasta apsardzes aģentūrai tiks piešķirta pilnīga piekļuve šai sistēmai, kas skaidri liecina par ES iesaistīšanās pievienoto vērtību.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

1. Izstrādes posms būtu jāsāk tikai pēc tam, kad ir pilnībā definētas darbības un galalietotāju prasības. Izstrādi var sākt tikai tad, kad būs pilnībā pieņemti pamatā esošie juridiskie instrumenti, kuros izklāstīts mērķis, darbības joma, funkcijas un tehniskā informācija.

2. Komisija ir apspriedusies (un turpina regulāri apspriesties) ar attiecīgajām ieinteresētajām personām, tostarp ar SISVIS komitejas pārstāvjiem komitoloģijas procedūras ietvaros. Šajā komitejā ir dalībvalstu pārstāvji gan *SIRENE* darbības jautājumos (pārrobežu sadarbība saistībā ar SIS), gan tehniskos jautājumos par SIS pilnveidi un uzturēšanu un ar to saistīto *SIRENE* piemērošanu. Ar šo regulu ierosinātās izmaiņas tika apspriestas ļoti pārredzamā un visaptverošā veidā speciālu tikšanos un darbsemināru laikā. Komisija izveidoja iekšēju dienestu koordinācijas grupu, iekļaujot tajā ģenerālsekretariātu un Migrācijas un iekšlietu

ģenerāldirektorātu, Tiesiskuma un patērētāju lietu ģenerāldirektorātu, Cilvēkresursu un drošības ģenerāldirektorātu un Informātikas ģenerāldirektorātu. Šī koordinācijas grupa uzraudzīja novērtēšanas procesu un vajadzības gadījumā sniedza norādījumus.

3. Komisija centās iegūt arī ārēju ekspertu viedokli, izmantojot divus pētījumus, kuru secinājumi tika ir iekļauti šā priekšlikuma izstrādē:

- SIS tehniskais novērtējums – novērtējumā apzināja galvenos atrisināmos jautājumus saistībā ar SIS un nākotnes vajadzības; tajā izteiktas bažas attiecībā uz darbības nepārtrauktības maksimālu nodrošināšanu un vispārējās struktūru spēju pielāgoties jaudas palielināšanai;

– IKT ietekmes novērtējums par iespējamiem uzlabojumiem SIS II uzbūvē – pētījumā tika novērtētas gan SIS darbības izmaksas valstu līmenī un izvērtēti divi iespējamie tehniskie risinājumi sistēmas uzlabošanai. Visi risinājumi ietver tehnisko priekšlikumu kopumu ar mērķi uzlabot uz centrālo sistēmu un vispārējo uzbūvi.

1.5.4. Saderība un iespējamā sinerģija ar citiem atbilstošiem instrumentiem

Šis priekšlikums būtu jāuzskata par to pasākumu īstenošanu, kas ietverti 2016. gada 6. aprīļa paziņojumā par "Spēcīgākas un viedākas robežu un drošības informācijas sistēmas"[84], kurā uzsvērts, ka ES ir jāstiprina un jāuzlabo tās IT sistēmas, datu uzbūve un informācijas apmaiņa tiesībaizsardzības, terorisma apkarošanas un robežu pārvaldības jomā.

Turklāt šis priekšlikums ir cieši saistīts ar citām Savienības politikas jomām un papildina tās, proti:

a) Iekšējā drošība – kā uzsvērts Eiropas Drošības programmā[85], lai novērstu, atklātu, izmeklētu smagus noziegumus un teroristu nodarījumus un sauktu pie atbildības par tiem, tiesībaizsardzības iestādēm ir jāspēj apstrādāt to personu personas datus, kuras tiek turētas aizdomās par dalību terora aktos vai smagos noziegumos.

b) datu aizsardzība, jo šim priekšlikumam ir jānodrošina pamattiesību aizsardzību attiecībā uz privātās dzīves neaizskaramību personām, kuru personas dati tiek apstrādāti SIS.

Priekšlikums ir saderīgs ar pašreizējiem Eiropas Savienības tiesību aktiem, proti:

a) Eiropas robežu un krasta apsardze [86], pirmkārt, attiecībā uz Aģentūras darbinieku iespējām veikt riska analīzi un, otrkārt, attiecībā uz viņu piekļuvi SIS ierosinātās ETIAS vajadzībām. Priekšlikuma mērķis cita starpā ir nodrošināt tehnisko saskarni piekļuvei SIS, lai Eiropas Robežu un krasta apsardzes vienību vai tāda personāla vienību, kas iesaistīts ar atgriešanu saistītu uzdevumu izpildē, kā arī migrācijas pārvaldības atbalsta vienības dalībnieki atbilstīgi savām pilnvarām varētu piekļūt SIS un meklēt SIS ievadītajos datos;

b) Eiropols, jo ar šo priekšlikums Eiropols saņem papildu tiesības piekļūt un meklēt datus, kas ievadīti SIS, saskaņā ar savām pilnvarām.

84 COM(2016) 205 *final*.

85 COM(2015) 185 *final*.

86 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.).

c) Prīme[87] – uzlabojumi šajā priekšlikumā ļauj identificēt personas, pamatojoties uz pirkstu nospiedumiem (kā arī sejas attēliem un DNS profiliem), un papildina pašreizējos Prīmes noteikumus par savstarpēju pārrobežu tiešsaistes piekļuvi konkrētām valstu DNS datubāzēm un automatizētajām pirkstu nospiedumu identifikācijas sistēmām.

Priekšlikums ir saderīgs ar nākotnē plānotajiem Eiropas Savienības tiesību aktiem, proti:

a) Ārējo robežu pārvaldība. Šis priekšlikums papildina jauno Šengenas Robežu kodeksa principu par visu ceļotāju, tostarp ES pilsoņu, sistemātiskām pārbaudēm attiecīgajās datubāzēs, kad tie ieceļo un izceļo no Šengenas zonas, kas ieviests, lai reaģētu uz ārvalstu kaujinieku teroristu parādību.

b) Ieceļošanas/izceļošanas sistēma[88] (IIS)P, jo priekšlikumā ir paredzēts atspoguļot ierosināto pirkstu nospiedumu un sejas attēlu kā biometrisko identifikatoru kopīgu izmantošanu IIS darbībai.

c) *ETIAS*, jo priekšlikumā ir ņemta vērā ierosinātā *ETIAS*, kura nodrošina visaptverošu drošības novērtējumu, tostarp pārbaudes SIS, attiecībā uz trešo valstu valstspiederīgajiem, kuri ir atbrīvoti no vīzas prasības un plāno ceļot Eiropas Savienībā.

87 Padomes Lēmums 2008/615/TI (2008. gada 23. jūnijs) par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu un pārrobežu noziedzību (OV L 210, 6.8.2008., 1. lpp.). un Padomes Lēmums 2008/616/TI (2008. gada 23. jūnijs) par to, kā īstenot Lēmumu 2008/615/TI par pārrobežu sadarbības pastiprināšanu, jo īpaši – apkarojot terorismu un pārrobežu noziedzību (OV L 210, 6.8.2008., 12. lpp.).

88 Priekšlikums Eiropas Parlamenta un Padomes regulai, ar ko izveido ieceļošanas/izceļošanas sistēmu (IIS), lai reģistrētu to trešo valstu valstspiederīgo ieceļošanas un izceļošanas datus un ieceļošanas atteikumus, kuri šķērso
Eiropas Savienības dalībvalstu ārējās robežas, un ar ko paredz nosacījumus piekļuvei IIS tiesībaizsardzības nolūkos un groza Regulu (EK) Nr. 767/2008 (COM(2016) 194 *final*).

1.6. Ilgums un finansiālā ietekme

☐**Ierobežota ilguma** priekšlikums/iniciatīva

– ☐ Priekšlikuma/iniciatīvas darbības laiks: [DD.MM.]GGGG.–[DD.MM.]GGGG.

– ☐Finansiālā ietekme: GGGG.– GGGG.

☑**Beztermiņa** priekšlikums/iniciatīva

– Sagatavošanās posms 2017. gads

– Īstenošana ar uzsākšanas periodu no 2018. līdz 2020. gadam,

– pēc kura turpinās normāla darbība

1.7. Paredzētie pārvaldības veidi[89]

☑ Komisijas īstenota **tieša pārvaldība**:

– ☑ ko veic tās struktūrvienības, tostarp personāls Savienības delegācijās;

– ☐ ko veic izpildaģentūras;

☑ **Dalīta pārvaldība** kopā ar dalībvalstīm

☑ **Netieša pārvaldība**, kurā budžeta īstenošanas uzdevumi uzticēti:

– ☐trešām valstīm vai to izraudzītām struktūrām;

– ☐ starptautiskām organizācijām un to aģentūrām (precizēt);

– ☐ EIB un Eiropas Investīciju fondam;

– ☑ Finanšu regulas 208. un 209. pantā minētajām struktūrām;

– ☐ publisko tiesību subjektiem;

– ☐ privāttiesību subjektiem, kas veic valsts pārvaldes uzdevumus, ja tie sniedz pienācīgas finanšu garantijas;

– ☐ struktūrām, kuru darbību reglamentē dalībvalsts privāttiesības, kurām ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuras sniedz pienācīgas finanšu garantijas;

– ☐ personām, kurām ir uzticēts veikt īpašas darbības KĀDP saskaņā ar Līguma par Eiropas Savienību V sadaļu un kuras ir noteiktas attiecīgā pamataktā.

– *Ja norādīti vairāki pārvaldības veidi, sniedziet papildu informāciju iedaļā "Piezīmes".*

Piezīmes

Komisija būs atbildīga par politikas vispārējo pārvaldību un *eu-LISA* būs atbildīga par sistēmas attīstību, darbību un uzturēšanu.

SIS ir viena informācijas sistēma. Līdz ar to izdevumi, kas paredzēti abos priekšlikumos (šajā priekšlikumā un priekšlikumā Regulai par Šengenas Informācijas sistēmas (SIS) izveidi, darbību un izmantošanu robežpārbaužu jomā), nebūtu jāuzskata par divām atsevišķām summām, bet par vienu veselumu. Ietekme uz budžetu, kas būtu grozījumiem, kas vajadzīgi, lai īstenotu abus priekšlikumus, ir atspoguļota vienā tiesību akta finanšu pārskatā.

[89] Skaidrojumus par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt BudgWeb tīmekļa vietnē: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

Norādīt periodiskumu un nosacījumus.

Komisija, dalībvalstis un Aģentūra regulāri pārskatīs un uzraudzīs SIS izmantošanu, lai nodrošinātu, ka tā joprojām darbojas efektīvi un iedarbīgi. Tehnisko un operatīvo pasākumu īstenošanā, kā aprakstīts šajā priekšlikumā, Komisijai palīdzēs komiteja.

Turklāt ierosinātās regulas 71. panta 7. un 8. punktā ir ietverts noteikums par oficiālu un regulāru pārskatīšanu un novērtēšanas procesu.

Eu-LISA ik pēc diviem gadiem ir pienākums ziņot Eiropas Parlamentam un Padomei par SIS, komunikācijas infrastruktūras, kas atbalsta to, kā arī par divpusējās vai daudzpusējās papildinformācijas apmaiņas starp dalībvalstīm tehnisko darbību, tostarp drošību.

Turklāt, reizi četros gados Komisijai ir pienākums veikt vispārīgu novērtējumu par SIS un informācijas apmaiņu starp dalībvalstīm un informēt par to Parlamentu un Padomi. Tādējādi tiks:

a) izskatīta rezultātu atbilstība mērķiem;

b) novērtēts, vai sistēmas pamatojums joprojām ir spēkā;

c) izskatīts jautājums, kā regula tiek piemērota centrālajai sistēmai;

d) novērtēta centrālās sistēmas drošība;

e) izpētīta sistēmas turpmākas darbības ietekme.

Turklāt *eu-LISA* ir pienākums nodrošināt dienas, mēneša un gada statistikas datus par SIS izmantošanu, nodrošinot pastāvīgu sistēmas uzraudzību un tās darbības izvērtēšanu attiecībā pret mērķiem.

2.2. Pārvaldības un kontroles sistēma

2.2.1. Apzinātie riski

Tiek apskatīti šādi gadījumi.

1. Iespējamās grūtības, ar kurām var saskarties *eu-LISA*, pārvaldot priekšlikumā paredzētos jauninājumus līdztekus citiem jau notiekošiem jauninājumiem (piemēram, AFIS integrēšanu SIS) un nākotnē paredzētiem jauninājumiem (piemēram, Ieceļošanas/izceļošanas sistēma, *ETIAS* un *Eurodac* modernizācija). Šo risku var mazināt, nodrošinot *eu-LISA* ir pietiekamu personālu un resursiem, lai tā varētu veikt šos uzdevumus un darbuzņēmēju pārvaldību attiecībā uz uzturēšanu darba kārtībā.

2. Grūtības dalībvalstīm:

2.1. Šīs grūtības galvenokārt ir finansiāla rakstura. Piemēram, tiesību aktu priekšlikumi paredz obligātu daļēja valsts eksemplāra izveidi katrā N.SIS II. Dalībvalstīm, kas nav tādu jau izstrādājušas, būs jāveic ieguldījumi. Tāpat arī valsts saskarnes kontroldokumenta īstenošanai vajadzētu būt pilnīgai īstenošanai. Tām dalībvalstīm, kas to vēl nav izdarījušas, tas būs jāparedz attiecīgo ministriju budžetā. Šo risku var mazināt, nodrošinot ES finansējumu dalībvalstīm, piemēram, no Iekšējās drošības fonda (IDF) Robežu daļas.

2.2. Valstu sistēmas ir jāsaskaņo ar centrālajām prasībām un diskusijas ar dalībvalstīm par šo jautājumu var kavēt jauninājumu ieviešanu. Šo risku var mazināt, izmantojot dalībvalstu agrīnu iesaistīšanu šā jautājuma risināšanā, lai būtu iespējams rīkoties attiecīgajā laikā.

2.2.2. Informācija par izveidoto iekšējās kontroles sistēmu

Par SIS centrālo daļu ir atbildīga *eu-LISA*. Lai varētu labāk pārraudzīt SIS izmantojumu un lai analizētu migrācijas spiediena tendences, robežu pārvaldību un noziedzīgus nodarījumus, *eu-LISA* būtu jāspēj attīstīt mūsdienīgas statistikas ziņojumu ģenerēšanas spējas, lai ziņotu dalībvalstīm un Komisijai. *eu-LISA* pārskatus iesniegs Revīzijas palātai apstiprināšanai, un uz tiem attiecinās budžeta izpildes apstiprinājuma procedūru. Komisijas Iekšējās revīzijas dienests veiks revīzijas sadarbībā ar *eu-LISA* iekšējo revidentu.

2.2.3. Paredzamās pārbaužu izmaksas un ieguvumi un gaidāmā kļūdas riska līmeņa novērtējums

Neattiecas

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus.

Krāpšanas apkarošanai paredzētie pasākumi ir noteikti Regulas (ES) 1077/2011 35. pantā, kurā noteikts šādi. 1. Nolūkā apkarot krāpšanu, korupciju un citas nelikumīgas darbības, piemēro Regulu (EK) Nr. 1073/1999. 2. Aģentūra pievienojas Iestāžu nolīgumam par Eiropas Biroja krāpšanas apkarošanai (OLAF) veikto iekšējo izmeklēšanu un nekavējoties pieņem attiecīgus noteikumus, kas piemērojami visiem Aģentūras darbiniekiem. 3. Lēmumos par finansēšanu un no tiem izrietošos īstenošanas nolīgumos un instrumentos skaidri paredz noteikumu, ka vajadzības gadījumā Revīzijas palāta un OLAF var uz vietas pārbaudīt Aģentūras finansējuma saņēmējus un par tā piešķiršanu atbildīgās personas. Saskaņā ar šo noteikumu Eiropas aģentūras lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā valde 2012. gada 28. jūnijā pieņēma lēmumu par iekšējās izmeklēšanas noteikumiem saistībā ar krāpšanas, korupcijas un citu Savienības interesēm kaitējošu prettiesisku darbību novēršanu. Tiks piemērota HOME ĢD krāpšanas novēršanas un atklāšanas stratēģija.

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

- Esošās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām

Daudzgadu finanšu shēmas izdevumu kategorija:	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	3. izdevumu kategorija – Drošība un pilsonība	Dif./nedif.[90]	no EBTA valstīm[91]	no kandidātvalstīm[92]	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē
	18.0208 – Šengenas informācijas sistēma	Dif.	NĒ	NĒ	JĀ	NĒ
	18.020101 – Atbalsts robežas pārvaldībai un kopējai vīzu politikai, lai atvieglotu likumīgu ceļošanu	Dif.	NĒ	NĒ	JĀ	NĒ
	18.0207 – Eiropas Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*)	Dif.	NĒ	NĒ	JĀ	NĒ

[90] Dif. = diferencētās apropriācijas / nedif. = nediferencētās apropriācijas.

[91] EBTA: Eiropas Brīvās tirdzniecības asociācija.

[92] Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Kopsavilkums par paredzamo ietekmi uz izdevumiem

Daudzgadu finanšu shēmas izdevumu kategorija	3	Drošība un pilsonība

HOME ĢD			2018. **gads**	**2019. gads**	**2020. gads**	**KOPĀ**
•Darbības apropriācijas						
18.0208 – Šengenas informācijas sistēma	Saistības	(1)	6,234	1,854	1,854	**9,942**
	Maksājumi	(2)	6,234	1,854	1,854	**9,942**
18.020101 (Robežas un Vīzas)	Saistības	(1)		18,405	18,405	**36,810**
	Maksājumi	(2)		18,405	18,405	**36, 810**
KOPĀ HOME ĢD apropriācijas	Saistības	=1+1.a +3	6,234	20,259	20,259	**46,752**
	Maksājumi	=2+2.a +3	6,234	20,259	20,259	**46,752**

EUR miljonos (trīs zīmes aiz komata)

Daudzgadu finanšu shēmas izdevumu kategorija	3	Drošība un pilsonība

eu-LISA			**2018. gads**	**2018. gads**	**2018. gads**	**KOPĀ**
•Darbības apropriācijas						
1. sadaļa: Personāla izdevumi	Saistības	(1)	0,210	0,210	0,210	**0,630**
	Maksājumi	(2)	0,210	0,210	0,210	**0,630**
2. sadaļa: Infrastruktūras un darbības izdevumi	Saistības	(1.a)	0	0	0	**0**
	Maksājumi	(2.a)	0	0	0	**0**
3. sadaļa: Darbības izdevumi	Saistības	(1.a)	12,893	2,051	1,982	**16,926**
	Maksājumi	(2.a)	2,500	7,893	4,651	**15,044**
KOPĀ — *eu-LISA* apropriācijas	Saistības	=1+1.a +3	13,103	2,261	2,192	**17,556**
	Maksājumi	=2+2.a +3	2,710	8,103	4,861	**15,674**

3.2.2. Paredzamā ietekme uz darbības apropriācijām

•KOPĀ darbības apropriācijas	Saistības	(4)								
	Maksājumi	(5)								
•KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem		(6)								
KOPĀ	Saistības	=4+ 6								

daudzgadu finanšu shēmas < …. > **IZDEVUMU KATEGORIJAS** apropriācijas	Maksājumi	=5+ 6								

Ja priekšlikums/iniciatīva ietekmē vairākas izdevumu kategorijas

•KOPĀ darbības apropriācijas	Saistības	(4)							
	Maksājumi	(5)							
•KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem		(6)							
KOPĀ daudzgadu finanšu shēmas **1. līdz 4. IZDEVUMU KATEGORIJAS** (Pamatsumma)	Saistības	=4+ 6	19,337	22,520	22,451				**64,308**
	Maksājumi	=5+ 6	8,944	28,362	25,120				**62,426**

3.2.3. Paredzamā ietekme uz administratīvajām apropriācijām

Daudzgadu finanšu shēmas izdevumu kategorija	**5**	"Administratīvie izdevumi"

		N gads	**N+1 gads**	**N+2 gads**	**N+3 gads**	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			**KOPĀ**
<…….> ĢD									
• Cilvēkresursi									
• Pārējie administratīvie izdevumi									
KOPĀ <….> **ĢD**	Apropriācijas								

EUR miljonos (trīs zīmes aiz komata)

KOPĀ daudzgadu finanšu shēmas **5. IZDEVUMU KATEGORIJAS apropriācijas**	(Saistību summa = maksājumu summa)								

EUR miljonos (trīs zīmes aiz komata)

		N gads[93]	**N+1 gads**	**N+2 gads**	**N+3 gads**	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			**KOPĀ**
KOPĀ daudzgadu finanšu shēmas **1.–5. IZDEVUMU KATEGORIJAS apropriācijas**	Saistības								
	Maksājumi								

[93] N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot.

3.2.3.1. Paredzamā ietekme uz HOME ĢD apropriācijām

– ☐ Priekšlikums/iniciatīva neparedz darbības apropriāciju izmantošanu

– ☑ Priekšlikums/iniciatīva paredz darbības apropriācijas izmantot šādā veidā:

Norādīt mērķus un rezultātus ⇩			**2018.gads**		2019. **gads**		**2018.gads**		Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		**KOPĀ**							
	REZULTĀTI																	
	Rezultāta veids[94]	Rezultāta vidējais izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Kopējais rezultātu daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS Nr. 1[95] Valsts sistēmas izstrāde			1		1	1,221	1	1,221										2,442
KONKRĒTAIS MĒRĶIS Nr. 2 Infrastruktūra			1		1	17,184	1	17,184										34,368
KOPĒJĀS IZMAKSAS						18,405		18,405										36,810

94 Rezultāti ir attiecīgie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

95 Kā norādīts 1.4.2. punktā. "Konkrētie mērķi…"

3.2.3.2. Paredzamā ietekme uz eu-LISA apropriācijām

– ☐ Priekšlikums/iniciatīva neparedz darbības apropriāciju izmantošanu

– ☑ Priekšlikums/iniciatīva paredz darbības apropriācijas izmantot šādā veidā:

Saistību apropriācijas EUR miljonos (trīs zīmes aiz komata)

Norādīt mērķus un rezultātus ⇩			**2018.gads**		2019. **gads**		**2018.gads**		Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		**KOPĀ**							
	REZULTĀTI																	
	Rezultāta veids[96]	Rezultāta vidējās izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Kopējais rezultātu daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS Nr. 1[97] Centrālās sistēmas izstrāde																		
- Darbuzņēmējs			1	5,013														5,013
- Programmatūra			1	4,050														4,050
- Aparatūra			1	3,692														3,692
Starpsumma – konkrētais mērķis Nr. 1				12,755														12,755
KONKRĒTAIS MĒRĶIS Nr. 2 Centrālās sistēmas uzturēšana																		
Darbuzņēmējs			1	0	1	0,365	1	0,365										0,730
Programmatūra			1	0	1	0,810	1	0,810										1,620

96 Rezultāti ir attiecīgie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

97 Kā norādīts 1.4.2. punktā. "Konkrētie mērķi…"

Aparatūra			1	0	1	0,738	1	0,738										1,476
Starpsumma – konkrētais mērķis Nr. 2						1,913		1,913										3,826
KONKRĒTAIS MĒRĶIS Nr. 3 Sanāksmes/mācības																		
Mācību pasākumi			1	0,138	1	0,138	1	0,069										0,345
Starpsumma – konkrētais mērķis Nr. 3				0,138		0,138		0,069										0,345
KOPĒJĀS IZMAKSAS				12,893		2,051		1,982										16,926

3.2.3.3. Paredzamā ietekme uz eu-LISA cilvēkresursiem

Kopsavilkums

– ☐Priekšlikums/iniciatīva neparedz izmantot administratīvās apropriācijas

– ☑Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādā veidā:

EUR miljonos (trīs zīmes aiz komata)

	2018.gads	**2019.gads**	**2020.gads**	**KOPĀ**
Ierēdņi (AD kategorija)				
Ierēdņi (AST kategorijas)				
Līgumdarbinieki	0,210	0,210	0,210	0,630
Pagaidu darbinieki				
Norīkotie valstu eksperti				
KOPĀ	**0,210**	**0,210**	**0,210**	**0,630**

Darbinieku pieņemšana ir plānota 2018. gada janvārī. Visiem darbiniekiem jābūt pieejamiem 2018. gada sākumā, lai varētu savlaicīgi sākt izstrādes posmu ar mērķi nodrošināt pārskatītās SIS II darbības uzsākšanu 2020. gadā. Ir vajadzīgi 3 jauni līgumdarbinieki (*CA*), lai segtu vajadzības gan projekta īstenošanai, gan atbalsta un uzturēšanas vajadzības pēc darbības uzsākšanas. Šos resursus izmantos, lai:

- atbalstītu projekta īstenošanu kā projekta grupas loceklis, tostarp tādas darbības kā: prasību un tehnisko specifikāciju definēšana, sadarbība un atbalsts dalībvalstīm, īstenošanas laikā, saskarnes kontroldokumenta (ICD) atjaunināšana, līgumā paredzēto piegāžu uzraudzība, piegāžu dokumentēšana un atjaunināšana utt.;
- atbalstītu pārejas pasākumus saistībā ar sistēmas darbības uzsākšanu sadarbībā ar darbuzņēmēju (izlaides uzraudzība, operatīvo procesu atjauninājumi, mācības (tostarp dalībvalstu mācību pasākumi) utt.;
- atbalstītu ilgtermiņa pasākumus, specifikāciju definēšana, līgumu sagatavošana gadījumā, ja ir nepieciešama sistēmas pārveide (piemēram, attēlu atpazīšanas dēļ) vai ja jaunais SIS II uzturēšanas darba kārtībā līgums ir jāgroza, lai iekļautu papildu izmaiņas (no tehniskā un budžeta aspekta);
- īstenotu otrā līmeņa atbalstu pēc darbības uzsākšanas pastāvīgas uzturēšanas un darbības nodrošināšanai.

Jānorāda, ka trīs jaunie resursi (*FTE CA*) darbosies papildus iekšējo vienību resursiem, kas būs norīkoti arī projektu/līgumu un finanšu uzraudzības/operatīvās darbības pasākumiem. Izmantojot *CA*, var panākt atbilstīgu līgumu ilgumu un nepārtrauktību, lai nodrošinātu darbības nepārtrauktību un izmantotu vienādi specializētus cilvēkus darbības atbalsta pasākumiem pēc projekta pabeigšanas. Turklāt darbības atbalsta pasākumi prasa piekļuvi ražošanas videi, ko nevar piešķirt darbuzņēmējiem vai ārštata darbiniekiem.

3.2.3.4. Paredzamās vajadzības pēc cilvēkresursiem

– ☐ Priekšlikums/iniciatīva neparedz cilvēkresursu izmantošanu.

– ☐ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Aplēse izsakāma ar pilnslodzes ekvivalentu

		N gads	**N+1gads**	**N+2** gads	**N+3** gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
•Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)								
XX 01 01 01 (Galvenā mītne un Komisijas pārstāvniecības)								
XX 01 01 02 (Delegācijas)								
XX 01 05 01 (Netiešā pētniecība)								
10 01 05 01 (Tiešā pētniecība)								
•Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu – *FTE*)[98]								
XX 01 02 01 (AC, END, INT, ko finansē no vispārīgajām apropriācijām)								
XX 01 02 02 (AC, LA, END, INT un JED delegācijās)								
XX 01 04 **yy** [99]	galvenajā mītnē							
	delegācijās							
XX 01 05 02 (AC, END, INT - netiešā pētniecība)								
10 01 05 02 (AC, END, INT – tiešā pētniecība)								
Citas budžeta pozīcijas (precizēt)								
KOPĀ								

XX ir attiecīgā politikas joma vai budžeta sadaļa.

Vajadzības pēc cilvēkresursiem tiks nodrošinātas, izmantojot attiecīgā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ģenerāldirektorātā, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

Veicamo uzdevumu apraksts

Ierēdņi un pagaidu darbinieki	
Ārštata darbinieki	

98 *AC* = līgumdarbinieki, *AL* = vietējie darbinieki, *END* = norīkotie valstu eksperti; *INT* = aģentūras darbinieki, *JED* – jaunākie eksperti delegācijās.

99 Ārštata darbiniekiem paredzēto maksimālo summu finansē no darbības apropriācijām (kādreizējām "BA" pozīcijām).

3.2.4. Saderība ar kārtējo daudzgadu finanšu shēmu

– ☐Priekšlikums/iniciatīva atbilst kārtējai daudzgadu finanšu shēmai.

– ☑Pieņemot priekšlikumu/iniciatīvu, jāpārplāno attiecīgā izdevumu kategorija daudzgadu finanšu shēmā.

Iekšējās drošības fondā paredzētā viedrobežu budžeta atlikuma pārdalīšana ir paredzēta, lai īstenotu funkcijas un pārmaiņas, kas paredzētas šajos divos priekšlikumos. IDF Robežu regula ir finanšu instruments, kurā ir iekļauts budžets viedrobežu tiesību aktu kopuma īstenošanai. Tās 5. pantā ir paredzēts, ka EUR 791 miljons tiek izmantoti ar programmu IT sistēmu izveidei, ar kurām palīdz pārvaldīt migrācijas plūsmas pāri ārējām robežām saskaņā ar 15. pantā paredzētajiem nosacījumiem. No minētās summas EUR 791 miljona apmēra EUR 480 miljoni ir rezervēti ieceļošanas/izceļošanas sistēmas izstrādei un EUR 210 miljoni - Eiropas ceļošanas informācijas un atļauju sistēmas (*ETIAS*) izveidei. Atlikusī daļa EUR 100 828 tiks daļēji izmantota, lai segtu izmaksas saistībā ar SIS II funkciju modernizāciju, kas paredzēta šajos divos priekšlikumos.

– ☐Pieņemot priekšlikumu/iniciatīvu, jāpiemēro elastības instruments vai jāpārskata daudzgadu finanšu shēma.

Aprakstīt, kas jādara, norādot attiecīgās izdevumu kategorijas, budžeta pozīcijas un summas.

3.2.5. Trešo personu iemaksas

– ☑Priekšlikums/iniciatīva neparedz trešo personu līdzfinansējumu

– Priekšlikums/iniciatīva paredz šādu līdzfinansējumu:

Apropriācijas EUR miljonos (trīs zīmes aiz komata)

	N gads	**N+1 gads**	**N+2 gads**	**N+3 gads**	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			Kopā
Norādīt līdzfinansējuma struktūru								
KOPĀ līdzfinansējuma apropriācijas								

3.3. Paredzamā ietekme uz ieņēmumiem

– ☐Priekšlikums/iniciatīva finansiāli neietekmē ieņēmumus

– ☑Priekšlikums/iniciatīva finansiāli ietekmē:

  – ☐pašu resursus

  – ☑dažādus ieņēmumus

EUR miljonos (trīs zīmes aiz komata)

Budžeta ieņēmumu pozīcija	Kārtējā finanšu gadā pieejamās apropriācijas	Priekšlikuma/iniciatīvas ietekme[100]						
		2018. gads	2019. gads	2020. gads	2021. gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
6313. pants — Šengenas asociēto valstu (CH, NO, LI, IS) iemaksas.		p.m	p.m	p.m	p.m			

Attiecībā uz dažādiem ieņēmumiem, kas ir "piešķirtie ieņēmumi", norādīt attiecīgo(-ās) izdevumu pozīciju(-as).

18.02.08 (Šengenas informācijas sistēma), 18.02.07 (*eu-LISA*)

Norādīt, ar kādu metodi aprēķināta ietekme uz ieņēmumiem.

Budžetā iekļauj ieguldījumu no valstīm, kas ir asociētas Šengenas *acquis* īstenošanai, piemērošanai un pilnveidošanai.

[100] Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t.i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 25 % apmērā.